

УТВЕРЖДЕН

ЛКНВ.11100-01 90 03-ЛУ

ОПЕРАЦИОННАЯ СИСТЕМА АЛЬТ 8 СП
(ОС АЛЬТ 8 СП)

Руководство администратора
ЛКНВ.11100-01 90 03

Листов 1228

Инд. № подл.	Подп. и дата	Взам. инв. №	Инд. № дубл.	Подп. и дата

2024

Литера О

АННОТАЦИЯ

Настоящий документ содержит инструкции по установке и эксплуатации программного изделия (ПИ) «Операционная система Альт 8 СП» ЛКНВ.11100-01, сокращенное наименование – ОС Альт 8 СП, **релиз 10** на процессорах архитектур **64 бит (x86_64), AArch64 (ARMv8)**.

Далее в документе будет использоваться альтернативное наименование ПИ: ОС Альт СП.

Версия: 2.1.

Документ предназначен для администратора ОС Альт СП и содержит общие сведения об ОС Альт СП, ее общей структуре, настройке, проверке, контрольных характеристиках развертывания и сообщениях администратору.

Также в документе приведены сведения, которые нужны для выполнения операций администрирования:

- установки и начального конфигурирования ОС Альт СП;
- конфигурирования параметров даты и времени, графической среды, средств ввода и вывода;
- конфигурирования сетей и сетевых служб;
- управления учетными записями и правами доступа пользователей;
- управления системными сервисами и служебными программами;
- настройки специализированного программного обеспечения;
- обновления программного обеспечения;
- просмотра системных журналов;
- управления автозапуском приложений;
- управления параметрами печати;
- работы с носителями информации;
- работы с руководствами, различными документами и дополнительными средствами.

СОДЕРЖАНИЕ

1. Общие сведения.....	18
1.1. Назначение и функции ОС Альт СП.....	18
1.2. Уровень подготовки администратора	19
2. Структура ОС Альт СП.....	20
2.1.1. Ядро ОС Альт СП.....	21
2.1.2. КСЗ.....	22
2.1.3. Системные библиотеки.....	25
2.1.4. Серверные программы и приложения.....	25
2.1.5. Прочие системные приложения.....	26
2.1.6. Программы веб-серверов.....	26
2.1.7. Интерактивные рабочие среды	27
2.1.8. Командные интерпретаторы	27
2.1.9. Графическая оболочка МАТЕ.....	27
2.1.10. Системы управления базами данных	27
2.1.11. Электронные справочники	27
3. Подготовительные процедуры.....	28
3.1. Настройка безопасной конфигурации компьютера.....	28
3.1.1. Процедура верификации	28
3.1.2. Настройка среды функционирования	28
3.2. Настройка опций безопасности	30
3.3. Описание механизмов устранения идентифицированных скрытых каналов.....	32
4. Функции и задачи администрирования ОС Альт СП.....	36
4.1. Функции администратора.....	36
4.2. Задачи администрирования	36
5. Установка ОС Альт СП.....	38
5.1. Запись установочного образа на USB-flash-накопитель	38
5.2. Начало установки: загрузка системы	40

5.3. Установка через VNC	44
5.4. Последовательность установки	47
5.4.1. Язык	48
5.4.2. Лицензионное соглашение	49
5.4.3. Дата и время.....	50
5.4.4. Подготовка диска	52
5.4.5. Перемонтирование	68
5.4.6. Установка системы.....	69
5.4.7. Сохранение настроек	71
5.4.8. Установка загрузчика.....	72
5.4.9. Настройка сети	75
5.4.10. Администратор системы	76
5.4.11. Системный пользователь.....	78
5.4.12. Установка пароля на LUKS-разделы	80
5.4.13. Завершение установки	81
5.5. Автоматическая установка системы (autoinstall)	81
5.5.1. Файлы автоустановки	82
5.5.2. Формат файла vm-profile.scn.....	82
5.5.3. Формат файла pkg-groups.tar.....	83
5.5.4. Формат файла autoinstall.scn	84
5.5.5. Формат файла install-scripts.tar	86
5.5.6. Запуск автоматической установки	87
5.6. Установка OEM-версии ОС Альт СП (рабочая станция).....	88
5.6.1. Установка в режиме OEM (предустановка)	90
5.6.2. Режим загрузки OEM.....	91
5.7. Обновление системы до актуального состояния	92
5.8. Установка графической оболочки на ОС Альт СП Сервер	92
5.9. Проблемы при установке системы	93
6. Начало использования ОС Альт СП.....	95
6.1. Запуск ОС.....	95

6.2. Получение доступа к шифруемым разделам.....	98
6.3. Вход в систему.....	99
6.3.1. Идентификация и аутентификация в графической оболочке МАТЕ.....	99
6.3.2. Идентификация и аутентификация в консольном режиме.....	103
6.3.3. Виртуальная консоль.....	103
6.4. Блокирование сеанса доступа.....	104
6.4.1. Блокирование сеанса доступа после установленного времени бездействия (неактивности) пользователя или по его запросу.....	104
6.4.2. Блокировка виртуальных текстовых консолей.....	105
6.4.3. Настройка блокировки возможности пользователя изменять настройки блокировки системы.....	105
6.5. Завершение сеанса пользователя.....	106
6.5.1. Графический режим.....	106
6.5.2. Консольный режим.....	107
6.5.3. Настройки завершения сеанса пользователя.....	107
6.6. Выключение/перезагрузка компьютера.....	108
6.6.1. Графический режим.....	108
6.6.2. Консольный режим.....	109
7. Настройки системы.....	110
7.1. Центр управления системой.....	110
7.1.1. Графический интерфейс.....	111
7.1.2. Веб-интерфейс ЦУС.....	112
7.1.3. Установка и удаление модулей ЦУС.....	114
7.1.4. Права доступа к модулям ЦУС.....	115
7.1.5. Получение справочной информации.....	117
7.2. Выбор программ, запускаемых автоматически при входе в систему.....	118
7.2.1. Вкладка автоматического запуска программ.....	118
7.2.2. Вкладка настроек сессии.....	119
7.3. Режим киоск по ограничению запуска программ.....	120

7.3.1. Настройка ограничения в ЦУС.....	120
7.3.2. Управление режимом киоск в консоли.....	121
7.4. Задание хешей паролей.....	121
7.4.1. Смена алгоритма в консоли	122
7.4.2. Смена алгоритма в ЦУС	122
7.5. Настройка фильтрации пакетов с помощью утилиты iptables	123
7.5.1. Устройство фильтра iptables	124
7.5.2. Встроенные таблицы фильтра iptables	125
7.5.3. Команды утилиты iptables	126
7.5.4. Ключи утилиты iptables	128
7.5.5. Основные действия над пакетами в фильтре iptables.....	129
7.5.6. Основные критерии пакетов в фильтре iptables.....	130
7.5.7. Модули iptables.....	132
7.5.8. Использование фильтра iptables	135
7.5.9. Примеры команд iptables	135
7.6. Настройка экспорта аудита на удаленный узел.....	139
7.7. Настройка системы сигнализации на основе icinga	141
7.7.1. Настройка сервера мониторинга	143
7.7.2. Настройка агентов.....	161
7.7.3. Управление конфигурацией.....	168
7.7.4. Работа с Icinga.....	217
7.8. ГОСТ в OpenSSL	219
7.8.1. Поддержка шифрования по ГОСТ в OpenSSL.....	219
7.8.2. Создание ключей.....	219
7.9. Утилита уничтожения информации при удалении – dm-secdel	220
8. Средства удаленного администрирования, организация сетевой инфраструктуры с помощью сервера	223
8.1. Вход в систему.....	223
8.2. Настройка подключения к Интернету.....	223
8.2.1. Конфигурирование сетевых интерфейсов.....	224

8.2.2. Объединение сетевых интерфейсов	227
8.2.3. Сетевые мосты	231
8.2.4. Настройка общего подключения к сети Интернет	233
8.2.5. Автоматическое присвоение IP-адресов (DHCP-сервер).....	238
8.3. Сетевая установка ОС на рабочие места	240
8.3.1. Подготовка сервера	240
8.3.2. Подготовка рабочих станций	243
8.4. Соединение удаленных офисов (OpenVPN-сервер)	243
8.4.1. Настройка OpenVPN-сервера.....	244
8.4.2. Настройка клиентов	250
8.5. Доступ к службам из сети Интернет	251
8.5.1. Внешние сети.....	251
8.5.2. Список блокируемых хостов.....	253
8.6. Статистика.....	253
8.6.1. Сетевой трафик.....	253
8.6.2. Прокси-сервер.....	255
8.7. Обслуживание системы	256
8.7.1. Мониторинг состояния системы.....	256
8.7.2. Системные службы	257
8.7.3. Обновление системы.....	258
8.7.4. Обновление систем, не имеющих выхода в Интернет	259
8.7.5. Локальные учетные записи	264
8.7.6. Администратор системы	265
8.7.7. Дата и время.....	266
8.7.8. Настройка прокси-сервера	267
8.7.9. Ограничение использования диска	268
8.7.10. Выключение и перезагрузка компьютера.....	269
8.7.11. FTP-сервер	270
8.7.12. Удостоверяющий центр.....	272
8.7.13. Резервное копирование.....	276

8.8. Сервер электронной почты (SMTP, POP3/IMAP).....	277
8.8.1. Сервер электронной почты	277
8.8.2. Сервер SMTP	278
8.8.3. Сервер POP3/IMAP	278
8.9. Сервер электронной почты postfix	278
8.9.1. Утилиты командной строки	279
8.9.2. Первичная настройка	281
8.9.3. Работа в режиме SMTP-сервера.....	282
8.9.4. SMTP-аутентификация	283
8.9.5. Триггеры ограничений.....	287
8.9.6. Алиасы и преобразование адресов	291
8.9.7. Настройка ограничений размера почтового ящика и отправляемого сообщения.....	292
8.10. Настройка удаленного подключения	292
8.10.1. OpenSSH, сервер протокола SSH (sshd).....	293
8.10.2. SSHD_CONFIG.....	306
8.10.3. USB/IP.....	317
8.11. Прокси-сервер (Squid).....	322
8.11.1. Настройка прозрачного доступа через прокси-сервер	323
8.11.2. Фильтрация доступа.....	323
8.11.3. Авторизация доступа	324
8.11.4. Кэширование данных.....	324
8.11.5. Настройка режима работы в качестве обратного прокси-сервера.....	325
8.11.6. Сбор статистики и ограничение полосы доступа	326
8.11.7. Кеширование DNS-запросов.....	326
9. Ограничение действий пользователя	327
9.1. Ограничение полномочий пользователей по использованию консолей	327
9.1.1. Настройка ограничения в ЦУС.....	327
9.1.2. Настройка ограничения в консоли	328

9.2. Ограничение неуспешных попыток входа в информационную систему	329
9.3. Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы	330
9.4. Блокировка макросов в приложениях	332
9.5. Настройка предупреждения пользователя при его входе в систему	333
9.6. Определение параметров уничтожения данных	334
9.7. Модуль AltНа.....	336
9.7.1. Запрет бита исполнения (SUID)	336
9.7.2. Блокировка интерпретаторов (запрет запуска скриптов)	337
9.7.3. Отключение возможности удаления открытых файлов.....	338
10. Доменная инфраструктура на базе Альт Домен	340
10.1. Основные сведения о логической модели «Альт Домен»	340
10.2. Разворачивание домена	341
10.2.1. Подготовка системы к установке сервера «Альт Домен»	341
10.2.2. Создание первого контроллера домена	345
10.2.3. Присоединение к домену в роли контроллера домена.....	365
10.2.4. Контроллер домена на чтение (RODC).....	372
10.2.5. Редактирование существующего домена	378
10.2.6. Отладочная информация	383
10.2.7. Удаление контроллера домена.....	384
10.3. Клиенты «Альт Домена»	391
10.3.1. SSSD vs Winbind.....	391
10.3.2. Подготовка системы к вводу в домен	395
10.3.3. Присоединение к домену в роли участника	399
10.3.4. Отладочная информация	408
10.3.5. Удаление клиента домена.....	409
10.3.6. Повторная регистрация клиента	410
10.3.7. Настройка аутентификации доменных пользователей на DC.....	411
10.3.8. Настройка обновления паролей аккаунтов машин.....	418

10.4. Инструменты управления объектами домена и групповыми политиками	424
10.4.1. Групповые политики.....	424
10.4.2. Установка административных шаблонов и административных инструментов	427
10.4.3. Включение механизма применения конфигурации на клиентских машинах.....	436
10.4.4. Модуль клиентской машины для применения конфигурации	439
10.4.5. Модуль удаленного управления базой данных конфигурации (ADMC)	456
10.4.6. Модуль редактирования настроек клиентской конфигурации (GPUИ)	531
10.4.7. Расширение возможностей ГП	705
10.4.8. Решение проблем	745
10.5. Доверительные отношения (Трасты)	758
10.5.1. Настройка доверия	758
10.5.2. Настройка DNS	761
10.5.3. Создание двухстороннего транзитивного подключения	767
10.5.4. Управление пользователями и группами	780
10.5.5. Использование трастов на LINUX-клиентах.....	784
10.5.6. Удаление доверия.....	786
10.6. Администрирование домена	789
10.6.1. Управление пользователями и группами	789
10.6.2. Администрирование DNS.....	801
10.6.3. Администрирование сайтов и подсетей.....	830
10.6.4. Управление парольными политиками	833
10.6.5. Резервное копирование и восстановление домена	840
10.6.6. Роли FSMO.....	857
10.6.7. Репликация.....	865
10.6.8. Настройка Samba для привязки к определенным интерфейсам.....	877

10.6.9. Создание keytab-файла	878
10.6.10. Аутентификация других сервисов в домене	882
10.6.11. Distributed File System.....	891
10.6.12. Настройка SSSD	894
10.6.13. Монтирование общих ресурсов samba.....	902
10.6.14. Журналирование в Samba.....	907
10.6.15. Усиление безопасности DC.....	927
10.6.16. Инструменты командной строки	930
10.6.17. Конфигурационные файлы.....	952
11. SOGo	961
11.1. Установка.....	961
11.2. Подготовка среды.....	961
11.3. Включение веб-интерфейса	964
11.4. Настройка электронной почты.....	965
11.4.1. Настройка Postfix	966
11.4.2. Настройка Dovecot	968
11.4.3. Безопасность	970
11.4.4. Проверка конфигурации.....	971
11.4.5. Настройка автоответчика, переадресации и фильтрации	971
12. FreeIPA.....	976
12.1. Установка сервера FreeIPA	976
12.2. Установка сервера FreeIPA в режиме CA-less	979
12.3. Добавление новых пользователей домена.....	984
12.4. Ввод рабочей станции в домен FreeIPA – установка клиента и подключение к серверу.....	986
12.4.1. Установка FreeIPA клиента.....	986
12.4.2. Настройка сети. FreeIPA.....	986
12.4.3. Подключение к серверу в ЦУС.....	988
12.4.4. Подключение к серверу в консоли.....	990
12.4.5. Вход пользователя.....	991

12.4.6. Удаление клиента FreeIPA	992
12.5. Настройка репликации.....	993
12.5.1. Настройка реплики на существующем клиенте.....	994
12.5.2. Установка реплики на машине, которая еще не зарегистрирована в домене FreeIPA	996
12.5.3. Проверка репликации	998
12.6. Настройка доверительных отношений с Active Directory.....	999
12.6.1. Настройка DNS.....	999
12.6.2. Предварительная настройка IPA-сервера	1001
12.6.3. Проверка конфигурации DNS	1002
12.6.4. Настройка доверия	1003
12.6.5. Проверка конфигурации Kerberos	1005
12.6.6. Проверка пользователей доверенного домена	1005
13. Настройка служб DNS (Bind).....	1007
13.1. Общие сведения.....	1007
13.2. Уменьшение времени ответа на DNS-запрос абонентов внутренней сети	1008
13.3. Именованье компьютеров в интранет-сети.....	1008
13.4. Примеры использования DNS-сервера Bind	1008
14. Система мониторинга Zabbix	1015
14.1. Установка сервера PostgreSQL	1015
14.2. Установка Apache2.....	1016
14.3. Установка PHP.....	1016
14.4. Настройка и запуск Zabbix-сервера.....	1016
14.5. Установка веб-интерфейса Zabbix.....	1017
14.6. Установка Zabbix-агента (клиента)	1021
14.7. Добавление нового хоста на Zabbix-сервере	1021
14.8. Авторегистрация узлов	1023
15. Отказоустойчивый кластер (High Availability) на основе Pacemaker	1026
15.1. Настройка узлов кластера.....	1027

15.2. Установка кластерного ПО и создание кластера	1030
15.3. Настройка основных параметров кластера.....	1032
15.3.1. Кворум	1032
15.3.2. Настройка STONITH.....	1032
15.3.3. Настройка ресурсов.....	1033
16. Postgresql	1035
16.1. Состав	1035
16.2. Настройка.....	1035
16.3. Использование postgresql	1036
16.3.1. Конфигурирование сервера.....	1036
16.3.2. Конфигурирование ролей.....	1037
16.3.3. Создание администратора БД и БД.....	1038
16.3.4. Работа роли администратора БД	1039
16.4. Настройка кластера postgresql.....	1039
17. Функциональные возможности ОС	1044
17.1. Управление системными сервисами, основные команды.....	1044
17.1.1. Сервисы	1044
17.1.2. Команды	1045
17.2. Администрирование многопользовательской и многозадачной среды .	1048
17.2.1. Команда who	1048
17.2.2. Команда ps	1050
17.2.3. Команда ntop	1053
17.2.4. Команда nice	1054
17.2.5. Команда renice	1055
17.2.6. Команда kill и killall.....	1056
17.3. Основные утилиты для операций с файлами и каталогами.....	1058
17.3.1. Команда ls	1058
17.3.2. Команда cp	1062
17.3.3. Команда rsync	1063
17.3.4. Команда mv.....	1064

17.3.5. Команда dd	1065
17.3.6. Команда s_rm	1065
17.3.7. Команда s_fill	1066
17.3.8. Команда cd	1066
17.3.9. Команда pwd	1067
17.3.10. Команда mkdir	1067
17.3.11. Команда rmdir	1067
17.3.12. Команда mount	1068
17.4. Создание, просмотр и редактирование файлов	1068
17.4.1. Команда cat	1068
17.4.2. Команда less	1069
17.4.3. Команда echo	1070
17.4.4. Команда grep	1070
17.4.5. Команда touch	1070
17.4.6. Команда mknod	1071
17.5. Поиск файлов	1072
17.5.1. Команда find	1072
17.5.2. Команда whereis	1074
17.6. Средства архивирования файлов	1075
17.6.1. Команда tar	1075
17.6.2. Команда cpio	1076
17.7. Средства редактирования файлов	1078
17.7.1. Текстовый редактор Vi	1078
17.7.2. Редактор Vim	1081
17.8. Средства настройки отложенного исполнения команд	1086
17.8.1. Служба crond	1086
17.8.2. Команда at	1091
17.8.3. Команда batch	1093
17.9. Control	1093
17.10. Защищенный интерпретатор команд SSH	1094

17.11. Средство управления процессами xinetd	1095
17.12. Работа со смарт-картами	1099
17.12.1. Двухфакторная аутентификация	1099
17.13. Поддержка файловых систем.....	1101
17.14. Поддержка сетевых протоколов	1103
17.14.1. SMB.....	1103
17.14.2. NFS.....	1107
17.14.3. FTP	1109
17.14.4. NTP	1116
17.14.5. HTTP(S).....	1117
17.15. Управление печатью	1118
17.15.1. Устройство CUPS	1119
17.15.2. Установка принтера	1128
17.15.3. Настройка сервера печати для сети.....	1131
17.15.4. Команды управления печатью.....	1132
17.16. Организация терминального доступа XRDP	1136
17.16.1. Базовая настройка сервера терминалов	1136
17.16.2. Настройка сервера.....	1136
17.16.3. Настройки доступа пользователей	1137
17.16.4. Подключение звука	1138
17.16.5. Подключение USB-устройств.....	1138
17.16.6. Настройка клиента для подключения к серверу терминалов.....	1139
17.16.7. Управление XRDP	1144
17.17. Timeshift	1144
17.17.1. Настройка резервного копирования.....	1146
17.17.2. Создание снимков	1154
17.17.3. Восстановление системы.....	1154
17.17.4. Работа с Timeshift в командной строке.....	1157
17.18. Информация о системе и об аппаратной части компьютера	1159
17.18.1. Команда inxi.....	1159

17.18.2. Команда glxinfo	1165
17.19. Xpra	1165
17.19.1. Установка	1166
17.19.2. Режимы работы	1166
17.19.3. Использование	1169
17.19.4. Клиент HTML5	1177
17.19.5. Графический интерфейс	1179
17.20. Установка корневого сертификата	1181
17.21. Выявление уязвимостей в образах контейнеров (trivy)	1182
17.21.1. Использование	1182
17.21.2. Примеры	1183
17.21.3. Локальная база данных Trivy	1184
18. Управление программными пакетами	1185
18.1. Источники программ (репозитории)	1186
18.1.1. Репозитории для АРТ	1186
18.1.2. Добавление репозитория с использованием терминала	1189
18.1.3. Программа управления пакетами Synaptic	1191
18.2. Обновление информации о репозиториях в АРТ	1192
18.3. Поиск пакетов (apt-cache)	1192
18.4. Управление установкой (инсталляцией) компонентов программного обеспечения	1193
18.4.1. Команда integrity-applier	1194
18.5. Установка или обновление пакета командой apt	1195
18.6. Удаление установленного пакета командой apt	1197
18.7. Альтернативная установка дополнительного ПО	1197
18.7.1. Программа управления пакетами Synaptic	1198
18.8. Обновление всех установленных пакетов apt-get	1199
18.9. Обновление всех установленных пакетов Synaptic	1199
18.10. Обновление ядра и модулей ядра	1200
18.10.1. В консоли	1200

18.10.2. Графический инструмент обновления ядра	1201
18.11. Обновление изолированного окружения (chrooted environment).....	1205
18.12. Проверка подлинности пакетов	1206
18.13. Получение уведомлений о выходе обновлений	1206
18.14. Обновление систем, не имеющих выхода в Интернет	1206
18.15. Единая команда управления пакетами (rpm)	1206
19. Ограничение действий пользователя	1208
19.1. Определение параметров уничтожения данных	1208
20. Контрольные характеристики развернутой ОС Альт СП	1210
21. Основы администрирования Linux	1211
21.1. Общие принципы работы ОС	1211
21.1.1. Процессы и файлы	1211
21.1.2. Командные оболочки (интерпретаторы)	1216
21.1.3. Командная оболочка Bash	1216
21.1.4. Стыкование команд в системе Linux	1218
21.2. Режим суперпользователя	1220
21.2.1. Пользователи ОС	1220
21.2.2. Назначение режима суперпользователя	1221
21.2.3. Получение прав суперпользователя	1221
21.2.4. Переход в режим суперпользователя	1221
21.3. Управление пользователями	1222
21.4. Система инициализации systemd и sysvinit	1222
21.4.1. Запуск операционной системы	1222
21.4.2. Примеры команд управления службами, журнал в systemd.....	1223
21.4.3. Журнал в systemd	1224
22. Сообщения администратору	1226
Перечень сокращений	1227

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение и функции ОС Альт СП

ОС Альт СП представляет собой совокупность интегрированных программ, созданных на основе операционной системы (ОС) Linux.

ОС Альт СП предназначена для группового и корпоративного использования, автоматизации информационных, конструкторских и производственных процессов предприятий (организаций, учреждений) всех возможных типов и направлений.

ОС Альт СП поддерживает клиент-серверную архитектуру и может обслуживать процессы как в пределах одной компьютерной системы, так и процессы на других персональных электронных вычислительных машинах (далее – ПЭВМ) через каналы передачи данных или сетевые соединения.

ОС Альт СП обладает следующими функциональными характеристиками:

- обеспечивает возможность обработки, хранения и передачи информации в защищенной программной среде;
- обеспечивает возможность запуска пользовательского программного обеспечения (далее – ПО) в сертифицированном окружении;
- обеспечивает возможность функционирования в многозадачном режиме (одновременное выполнение множества процессов);
- обеспечивает возможность масштабирования системы: возможна эксплуатация ОС как на одной ПЭВМ, так и в информационных системах различной архитектуры;
- обеспечивает многопользовательский режим эксплуатации;
- обеспечивает поддержку мультипроцессорных систем;
- обеспечивает сетевую обработку данных, в том числе разграничение доступа к сетевым пакетам.

Для поддержки выполнения описанных функций в ОС Альт СП реализованы следующие возможности:

- управление процессами и информационными ресурсами;
- управление системными ресурсами;
- управление памятью;
- управление файлами и внешними устройствами;
- управление доступом к обрабатываемой информации;
- защита хранимых, обрабатываемых и передаваемых информационных ресурсов комплексом средств защиты (далее – КСЗ) ОС;
- администрирование;
- поддержка интерфейса прикладного программирования;
- поддержка пользовательского интерфейса.

1.2. Уровень подготовки администратора

Администратор ОС Альт СП должен иметь базовые знания в областях:

- принципы построения и функционирования современных вычислительных систем, механизмов защиты информации;
- работа с ОС семейства Linux;
- администрирование общесистемного и прикладного ПО;
- настройка средств защиты, используемых в составе ОС Альт СП;
- конфигурирование проводных подключений.

2. СТРУКТУРА ОС АЛЬТ СП

ОС Альт СП состоит из набора компонентов, предназначенных для реализации функциональных задач пользователями (должностными лицами для выполнения определенных должностными инструкциями повседневных действий). ПИ ОС Альт СП поставляется в виде дистрибутива и комплекта эксплуатационной документации.

Структура ОС Альт СП представлена на рис. 1.

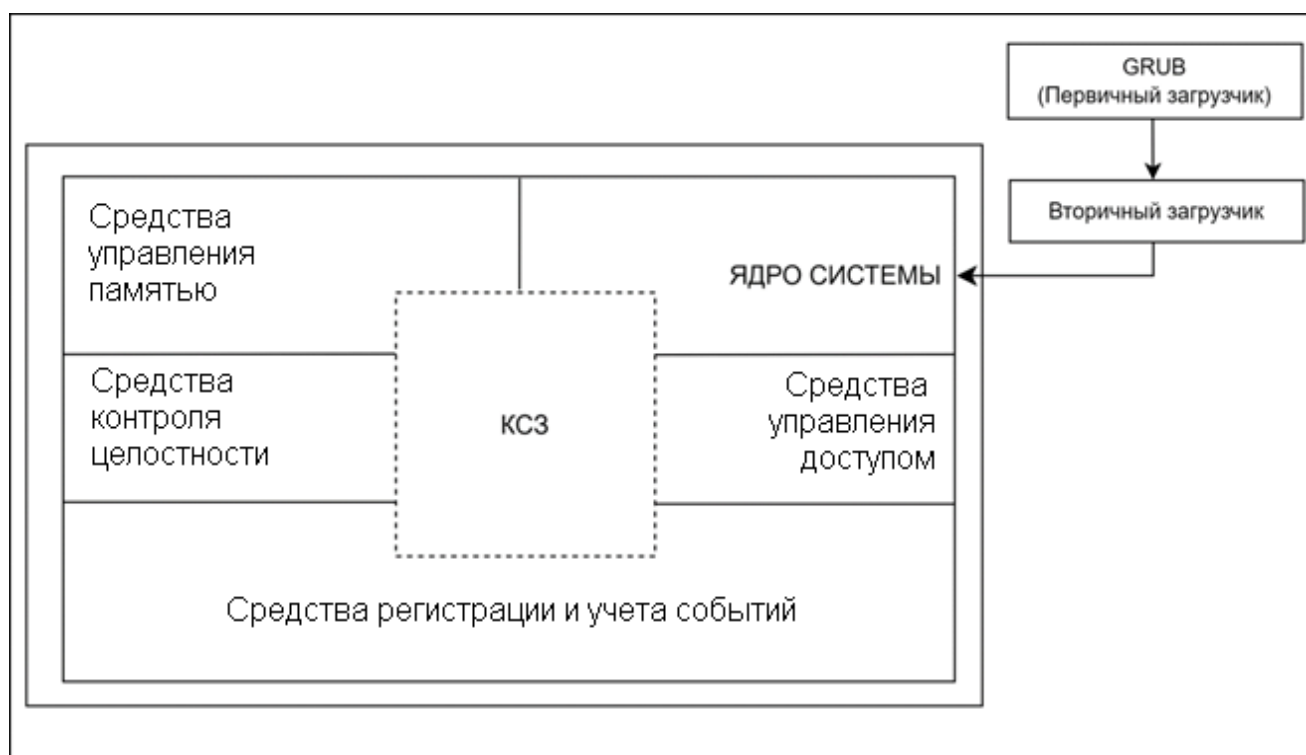


Рис. 1 – Структура ОС Альт СП

В состав ОС Альт СП входят следующие компоненты:

- ядро системы;
- средства управления доступом;
- средства регистрации и учета событий;
- средства контроля целостности;
- средства управления памятью.

В структуре компонентов ОС Альт СП выделены следующие функциональные элементы:

- ядро ОС;
- системные библиотеки;
- утилиты и драйверы;
- комплекс средств защиты информации;
- системные приложения;
- системы мониторинга и управления;
- интерактивные рабочие среды;
- серверные программы и приложения;
- графическая оболочка;
- командные интерпретаторы;
- прикладное программное обеспечение общего назначения;
- офисные приложения;
- программные средства виртуализации;
- программные средства контейнеризации;
- системы управления базами данных;
- программный комплекс Альт Домен.

Первичный и вторичный загрузчики ОС обращаются напрямую к ядру ОС, вызывая запуск системных процессов и приложений.

Взаимодействие и обмен информацией в ОС Альт СП контролируются КСЗ, предназначенным для защиты ОС от несанкционированного доступа к обрабатываемой (хранящейся) информации на ПЭВМ.

2.1.1. Ядро ОС Альт СП

Ядро ОС Альт СП управляет доступом к оперативной памяти, сети, дисковым и прочим внешним устройствам. Оно запускает и регистрирует процессы, управляет разделением времени между ними, реализует разграничение прав и определяет политику безопасности, обойти которую, не обращаясь к нему, нельзя.

Ядро работает в режиме «супервизора», позволяющем ему иметь доступ сразу ко всей оперативной памяти и аппаратной таблице задач. Процессы запускаются в «режиме пользователя»: каждый жестко привязан ядром к одной записи таблицы задач, в которой, в числе прочих данных, указано, к какой именно части оперативной памяти этот процесс имеет доступ. Ядро постоянно находится в памяти, выполняя системные вызовы – запросы от процессов на выполнение этих подпрограмм.

2.1.2. КСЗ

КСЗ представляет собой набор специальных программных пакетов, в том числе из состава ядра ОС Альт СП, предназначенных для реализации механизмов безопасности и контроля функционирования ОС Альт СП в целом. Состав и версии пакетов КСЗ уточняйте в зависимости от архитектуры процессора.

* – группа пакетов.

КСЗ включает в себя следующие программные пакеты:

- `acl` – утилиты, предназначенные для администрирования списков контроля доступа Access Control Lists, которые используются для более точного задания прав доступа к файлам и директориям;
- `alterator*` – группа пакетов различных модулей системных настроек интерфейса Центра управления системой (ЦУС), предназначены для выполнения наиболее востребованных административных задач;
- `apt` – средства управления пакетами АРТ, установка, обновление, разрешение зависимостей RPM пакетов;
- `audit` – утилиты для хранения и поиска записей аудита, генерируемых подсистемой аудита;
- `bash` – командная оболочка Bourne-Again Shell;
- `control` – содержит общие интерфейсы управления системным оборудованием, предоставляемые другими пакетами;
- `control++` – утилита конфигурирования системы, которая позволяет администратору изменять ограничения системы, устанавливать права доступа;

- coreutils – набор утилит для управления файлами и изменения текстовых файлов;
- corosync – реализует систему взаимодействия для отказоустойчивых кластеров (Сервер 64 бит (x86_64), AArch64 (ARMv8));
- dm-secdel – утилита уничтожения информации, реализует безопасное удаление;
- grub* – модули загрузчика ОС;
- icinga2 – система мониторинга служб и сетевой активности;
- ima-evm* – подсистема контроля целостности GNU/Linux, использует технологии IMA и EVM;
- iptables – используется для настройки, обслуживания и проверки находящихся в ядре Linux таблиц правил фильтрации пакетов IP;
- kernel-image* – ядро ОС Linux, управляет аппаратными ресурсами компьютера и обеспечивает взаимодействие между аппаратным обеспечением и программами. Отвечает за управление процессами, памятью, устройствами, системные вызовы;
- kernel-modules* – пакеты аппаратных драйверов и библиотек в ядре ОС;
- kubernetes – система с открытым исходным кодом для управления контейнерными приложениями на нескольких хостах; предоставляет базовые механизмы для развертывания, обслуживания и масштабирования приложений;
- libvirt* – набор инструментов для управления виртуализацией;
- lightdm* – менеджер дисплеев, предоставляет графический интерфейс;
- mate-screensaver – хранитель и блокировщик экрана;
- mount – утилита для монтирования файловых систем;
- nagwad – сервис, генерирующий уведомления от icinga, основанные на записях из журнала аудита;
- ntpdate – устанавливает дату и время с помощью NTP. Используется для синхронизации времени компьютерного клиента или сервера с другим

- сервером или источником эталонного времени, обеспечивает временную точность работ;
- `openvpn` – VPN с использованием SSL, реализует подключение для удаленных пользователей, телекоммуникации для дома и офиса, безопасные подключения для беспроводных сетей;
 - `ossec` – программный комплекс проверки целостности, предназначенный для обнаружения различий между двумя состояниями системы, а также для поиска потенциально опасных файлов;
 - `racemaker` – менеджер управления ресурсами масштабируемого и высоко доступного кластера (Сервер 64 бит (x86_64), AArch64 (ARMv8));
 - `libpam0`, `pam*`, `pam0*` – инструменты системы безопасности, позволяющие администраторам устанавливать политику аутентификации без необходимости повторной компиляции программ проверки подлинности;
 - `passwd` – утилита для установки/смены паролей с использованием PAM;
 - `passwdqc` – набор инструментов для контроля сложности паролей и парольных фраз, включающий PAM-модуль, программы и библиотеку;
 - `podman` – модули управления контейнерами, образы контейнеров;
 - `polkit` – это набор инструментов для определения и обработки разрешений. Он используется для того, чтобы позволить непривилегированным процессам контактировать с привилегированными процессами;
 - `postgresql*` – система управления базами данных PostgreSQL;
 - `qemu` – быстрый эмулятор процессора, использующий динамическую трансляцию для достижения хорошей скорости эмуляции;
 - `rpm` – менеджер пакетов, используемый для сборки, установки, инспекции, проверки, обновления и удаления отдельных программных пакетов;
 - `rsync` – утилита синхронизации файлов по сети, используется в качестве эффективного процесса зеркалирования, т. к. пересылает только различия между файлами, а не файлы целиком;
 - `secure_delete` – набор утилит для безопасного удаления файлов, безопасной очистки от остатков данных неиспользуемого пространства дисков,

- безопасной очистки разделов подкачки и безопасной очистки неиспользуемой памяти;
- setup – начальный набор конфигурационных файлов;
 - sh – командная оболочка Bourne shell;
 - shadow – усиливает безопасность системных паролей;
 - su – утилита запуска командного интерпретатора от имени другого пользователя;
 - sudo – программа, позволяющая делегировать те или иные привилегированные ресурсы пользователям с ведением протокола работы;
 - systemd*– менеджер системы и служб в ОС, реализует запуск демонов и отслеживает процессы;
 - util-linux – коллекция основных системных утилит;
 - vim-console – экранный редактор;
 - vlock – программа блокировки сеансов в консоли.

2.1.3. Системные библиотеки

Системные библиотеки – наборы программ (пакетов программ), выполняющие различные функциональные задачи и предназначенные для динамического подключения к работающим программам, которым требуется выполнение этих задач.

2.1.4. Серверные программы и приложения

Серверные программы и приложения предоставляют пользователю специализированные услуги (почтовые службы, хранилище файлов, веб-сервер, система управления базой данных, обеспечение документооборота, хранилище данных пользователей и так далее) в локальной или глобальной сети и обеспечивают их выполнение.

В состав ОС Альт СП включены следующие серверные программы и приложения:

- приложения, обеспечивающие поддержку сетевого протокола DHCP (Dynamic Host Configuration Protocol);

- приложения, обеспечивающие поддержку протокола аутентификации LDAP (Lightweight Directory Access Protocol);
- приложения, обеспечивающие поддержку протоколов FTP, SFTP, SSHD;
- системы управления базами данных;
- программы, обеспечивающие работу SMB-сервера (сервер файлового обмена);
- программы почтового сервера postfix;
- программы прокси-сервера Squid;
- программы веб-сервера apache2;
- программы DNS-сервера.

2.1.5. Прочие системные приложения

Прочие системные приложения – приложения (программы), оказывающие пользователю дополнительные системные услуги при работе с ОС.

В состав ОС Альт СП включены следующие дополнительные системные приложения:

- архиваторы;
- для управления RPM-пакетами;
- резервного копирования;
- мониторинга системы;
- для работы с файлами;
- для настройки системы;
- для настройки параметров загрузки;
- для настройки оборудования;
- для настройки сети;
- для доступа к виртуальным рабочим столам (см. документ «Руководство администратора. Виртуализация и контейнеризация. ЛКНВ.11100 01 92 02»).

2.1.6. Программы веб-серверов

Программы веб-серверов участвуют в организации доступа пользователей к сети Интернет. Доступ организуется с помощью клиент-серверной архитектуры.

Клиент, которым обычно является веб-браузер, передает программе веб-сервера запросы на получение ресурсов. В качестве ресурсов могут выступать HTML-страницы, изображения, файлы, медиа-потoki или другие данные, которые требуются клиенту. В ответ веб-сервер передает клиенту запрошенные данные. Обмен происходит по протоколу HTTP.

В состав ОС Альт СП включены программы веб-сервера Apache.

2.1.7. Интерактивные рабочие среды

Интерактивные рабочие среды – программы (пакеты программ), предназначенные для работы пользователя в ОС Альт СП и предоставляющие ему удобный интерфейс для общения с ней.

2.1.8. Командные интерпретаторы

Командные интерпретаторы – специальные программы (терминалы), предназначенные для выполнения различных команд пользователей при работе с ОС Альт СП.

2.1.9. Графическая оболочка МАТЕ

Графическая оболочка МАТЕ – набор программ и технологий, предназначенных для управления ОС Альт СП и предоставляющих пользователю графический интерфейс для работы.

2.1.10. Системы управления базами данных

Системы управления базами данных (далее – СУБД) (см. раздел 16) – приложения, предназначенные для работы с данными, представленными в виде набора записей. СУБД осуществляет поиск, обработку и структурирование данных.

2.1.11. Электронные справочники

Электронные справочники – наборы внутрисистемных справочных страниц, описывающих работу команд и приложений, которые выполнены в виде примеров HOWTOs и справки man.

3. ПОДГОТОВИТЕЛЬНЫЕ ПРОЦЕДУРЫ

3.1. Настройка безопасной конфигурации компьютера

3.1.1. Процедура верификации

Проверка поставленного потребителю дистрибутива производится путем подсчета контрольной суммы с использованием программы фиксации и контроля исходного состояния программного комплекса «ФИКС» (версия 2.0.2)/программы фиксации и контроля целостности информации «ФИКС-UNIX 1.0» по алгоритму «Уровень-3» (при наличии)¹ и сравнения ее с контрольной суммой, указанной в документе «Формуляр. ЛКНВ.11100-01 30 01» и на этикетке ПИ для соответствующей архитектуры.

Администратор имеет возможность верифицировать версию ОС Альт СП, выполнив команду:

```
# cat /root/.install-log/diskinfo
```

3.1.2. Настройка среды функционирования

Для среды функционирования ОС Альт СП (средств вычислительной техники (СВТ)) сформулированы следующие рекомендации:

- обновление установленной системы до ОС Альт СП релиз 10 не допускается. Установка должна производиться с удалением всех предыдущих данных со всех разделов диска;
- не допускается использовать аппаратные платформы, включающие в себя базовые системы ввода-вывода (BIOS) или унифицированные расширяемые интерфейсы встроенного ПО (UEFI), содержащие уязвимости, без применения обновлений с закрытием уязвимостей, предоставленных разработчиком данной аппаратной платформы для BIOS или UEFI;
- отключать в BIOS-е Intel SGX;

¹ Или с использованием аналогичного ПО, осуществляющего подсчет контрольных сумм по алгоритму ФИКС режим «Уровень-3».

- на серверах отключать системы контроля и управления типа ILO, RSA, iDRAC, ThinkServer EasyManage, AMT, iMana;
- для Intel платформ нужно устранить уязвимости Intel-SA-00086 в Intel Management Engine;
- установка, конфигурирование и управление ОС Альт СП должны выполняться в соответствии с эксплуатационной документацией;
- должна быть обеспечена защита от осуществления действий, направленных на нарушение физической целостности СВТ, на котором функционирует ОС Альт СП;
- должна быть обеспечена доверенная загрузка ОС (блокирование попыток несанкционированной загрузки, контроль доступа субъектов доступа к процессу загрузки, контроль целостности компонентов загружаемой операционной среды);
- должны быть обеспечены ресурсы для выполнения функциональных возможностей безопасности ОС, хранения резервных копий, создаваемых ОС, а также защищенное хранение данных ОС и защищаемой информации;
- должно быть обеспечено ограничение на установку ПО и его компонентов, не задействованных в технологическом процессе обработки информации;
- должен обеспечиваться доверенный маршрут между ОС и пользователями ОС (администраторами, пользователями);
- должен обеспечиваться доверенный канал передачи данных между ОС и средствами вычислительной техники, на которых происходит обработка информации, а также с которых происходит их администрирование;
- должна быть обеспечена невозможность отключения (обхода) компонентов ОС;
- должны быть реализованы меры, препятствующие несанкционированному копированию информации, содержащейся в ОС, на съемные машинные носители информации (или за пределы ИС). В том числе должен осуществляться контроль вноса (выноса) в (из) контролируемую зону (контролируемой зоны) съемных машинных носителей информации;

- должна осуществляться проверка целостности внешних модулей уровня ядра, получаемых от заявителя (разработчика, производителя), перед их установкой в ОС;
- должно быть обеспечено выделение вычислительных ресурсов для процессов в соответствии с их приоритетами;
- персонал, ответственный за функционирование ОС Альт СП, должен обеспечивать функционирование ОС Альт СП, в точности руководствуясь эксплуатационной документацией;
- лица, ответственные за эксплуатацию ОС Альт СП, должны обеспечить, чтобы аутентификационная информация для каждой учетной записи пользователя ОС содержалась в тайне и была недоступна лицам, не уполномоченным использовать данную учетную запись;
- должна обеспечиваться возможность генерации аутентификационной информации соответствующей метрике качества.

3.2. Настройка опций безопасности

Во время установки ОС Альт СП в соответствии с принятыми парольными ограничениями на объекте эксплуатации:

- задать пользователя с паролем, отвечающим требованиям безопасности;
- задать пароль администратора, отвечающий требованиям безопасности;
- установить пароль на загрузчик (при наличии).

Перед началом эксплуатации ОС Альт СП рекомендуется администратору обеспечить выполнение следующих условий:

- 1) настроить параметры входа пользователя (порядок действий приведен в документе «Руководство по комплексу средств защиты. ЛКНВ.11100-01 99 03» – далее Руководство по КСЗ):
 - время засыпания (блокирование сеанса доступа см. в п. 6.4);
- 2) настроить параметры пароля пользователя (порядок действий приведен в Руководстве по КСЗ подразделы «Настройка парольных ограничений», «Управление сроком действия пароля»):
 - сложность пароля;
 - время действия;

- 3) настроить средства контроля целостности (порядок действий приведен в Руководстве по КСЗ в подразделе «Средства контроля целостности»);
- 4) настроить параметры запрета удаления файлов (порядок действий приведен п. 9.7 «Модуль AltNa»);
- 5) настроить сервисы в соответствии с функциональным назначением объекта автоматизации (управление сервисами см. в п. 17.1.1);
- 6) настроить аудит:
 - создать правила аудита (примеры использования аудита приведены в Руководстве по КСЗ подраздел «Использование аудита»);
 - настроить экспорт аудита на другой компьютер (порядок действий приведен п. 7.6);
- 7) настроить подключение оповещений администратора (порядок действий приведен п. 7.8);
- 8) механизм замкнутой программной среды должен быть настроен для работы в штатном режиме пользователя (порядок действий приведен в Руководстве по КСЗ в подразделе «Подсистема IMA/EVM»);
- 9) с использованием средств управления дискреционными правами разграничения доступа запретить пользователям, не обладающим привилегиями администратора:
 - доступ к библиотеке `libpcprofile.so`;
 - запуск (использование) средств создания символических ссылок;
- 10) с использованием средств управления запуском сервисов должна быть отключена служба `grm` для поддержки «мыши» в консольном режиме;
- 11) для защиты от атаки подбора пароля (brute force):
 - внести изменения в файл `/etc/pam.d/sshd` – добавить строку:
`auth required pam_faillock.so authfail deny=3 unlock_time=19`
- 12) для суперпользователя (`root`) заблокировать возможность его удаленного входа в ОС посредством включения PAM-модуля `pam_securetty` в файл сценария `/etc/pam.d/system-auth-common`. Для этого в «Primary block» в указанном файле первой строкой добавить:
`auth required pam_securetty.so`

3.3. Описание механизмов устранения идентифицированных скрытых каналов

Далее приведены дополнительные рекомендации по настройке механизмов защиты ОС Альт СП для устранения возможных скрытых каналов передачи информации.

Механизмы защиты направлены на ограничение, мониторинг, полное или частичное устранение идентифицированных скрытых каналов, которые могут возникнуть в информационных (автоматизированных) системах вследствие использования в них ОС Альт СП.

1) Исключить возможность работы с общими каталогами с правом записи для пользователей, имеющих разные полномочия доступа.

2) Для противодействия атакам на каналы передачи по времени и памяти администратору безопасности нужно исключить наличие в системе общих для пользователей файловых ресурсов, где размещаются файлы с разными правами дискреционного разграничения доступа, в частности, исключить размещение в каталогах файлов, доступ к которым полностью закрыт для конкретных пользователей данного каталога. Также можно монтировать файловую систему без учета времени доступа:

```
mount LABEL=mydisk -o noatime
```

3) На уровне ядра запретить процессам создавать слушающие сокеты, кроме тех, что им действительно нужны, в том числе запрещать слушать на фиксированном порту, а также контролировать частоту создания сокета.

4) Монтировать подсистему /proc с флагом hidepid=2 или 1. При этом имена процессов других пользователей и другие данные таких процессов будут недоступны вызывающему непривилегированному пользователю.

5) Организовать маскирующие процессы, имитирующие постоянную загрузку процессора. Использовать механизмы ограничения CPU для процессов, гарантирующих время выполнения, одинаковое для всех процессов, таких как cgroups.

6) Для предотвращения Timestamp Evaluation (вычисления временных меток) – отключить отметки времени TCP в ОС Альт СП. Для этого выполните команду:

```
# echo 0 > /proc/sys/net/ipv4/tcp_timestamps
```


и, чтобы изменения стали постоянными добавьте следующую строку в файл /etc/sysctl.conf:

```
net.ipv4.tcp_timestamps = 0
```

также можно настроить правила iptables:

```
iptables -A INPUT -p icmp --icmp-type timestamp-request -j DROP
iptables -A OUTPUT -p icmp --icmp-type timestamp-reply -j DROP
```

7) Для предотвращения ISN Evaluation (использование порядковых номеров для индексации передаваемых TCP-данных) – использовать TCP/IP прокси (socks).

8) Для предотвращения TCP URG Pointer (указателя TCP URG) – настроить правила iptables:

```
iptables -N BADFLAGS
iptables -A BADFLAGS -j LOG --log-prefix "BADFLAGS: "
iptables -A BADFLAGS -j DROP
iptables -N TCP_FLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ACK,FIN FIN -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ACK,PSH PSH -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ACK,URG URG -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags FIN,RST FIN,RST -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags SYN,FIN SYN,FIN -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags SYN,RST SYN,RST -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ALL ALL -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ALL NONE -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ALL FIN,PSH,URG -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ALL SYN,FIN,PSH,URG -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j BADFLAGS
```

9) Для предотвращения IP ToS Evaluation (оценки IP-ToS) – настроить способ обслуживания для telnet, ftp-control и ftp-data – выполнить команды:

```
# iptables -A PREROUTING -t mangle -p tcp --sport telnet \
-j TOS --set-tos Minimize-Delay
# iptables -A PREROUTING -t mangle -p tcp --sport ftp \
-j TOS --set-tos Minimize-Delay
# iptables -A PREROUTING -t mangle -p tcp --sport ftp-data \
-j TOS --set-tos Maximize-Throughput
```

Эти правила прописываются на удаленном хосте и воздействуют на входящие по отношению к компьютеру пакеты. Для пакетов, отправляемых в обратном направлении, эти флаги устанавливаются автоматически. Настроить их можно, прописав следующие правила:

```
# iptables -A OUTPUT -t mangle -p tcp --dport telnet \
-j TOS --set-tos Minimize-Delay
# iptables -A OUTPUT -t mangle -p tcp --dport ftp \
-j TOS --set-tos Minimize-Delay
# iptables -A OUTPUT -t mangle -p tcp --dport ftp-data \
-j TOS --set-tos Maximize-Throughput
```

Для противодействия данной атаке нужно в командной строке прописать следующие правила:

```
# Разрешить главные типы протокола ICMP
iptables -A OUTPUT -p icmp --icmp-type 0 -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 3 -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 4 -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 11 -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 12 -j ACCEPT
```

Типы ICMP-сообщений:

- 0 – echo reply (echo-ответ, пинг);
- 3 – destination unreachable (адресат недостижим);
- 4 – source quench (подавление источника, просьба посылать пакеты медленнее);
- 5 – redirect (редирект);
- 8 – echo request (echo-запрос, ping);
- 9 – router advertisement (объявление маршрутизатора);
- 10 – router solicitation (ходатайство маршрутизатора);
- 11 – time-to-live exceeded (истечение срока жизни пакета);
- 12 – IP header bad (неправильный IP заголовок пакета);
- 13 – timestamp request (запрос значения счетчика времени);
- 14 – timestamp reply (ответ на запрос значения счетчика времени);
- 15 – information request (запрос информации);
- 16 – information reply (ответ на запрос информации);
- 17 – address mask request (запрос маски сети);
- 18 – address mask reply (ответ на запрос маски сети).

10) Для предотвращения Initial Sequence Number hijacking and spoofing (перехвата и подмены изначальных порядковых номеров при индексации TCP-соединений) – настроить правила iptables:

```
# Защита от подмены
iptables -I INPUT -m conntrack --ctstate NEW,INVALID -p tcp \
  --tcp-flags SYN,ACK SYN,ACK -j REJECT --reject-with tcp-reset
# Защита от SYN-флуда
iptables -A INPUT -p tcp --syn -m limit --limit 10/s \
  --limit-burst 50 -j ACCEPT
iptables -A INPUT -p udp -m limit --limit 10/s --limit-burst 50 -j \
  ACCEPT
```

ЛКНВ.11100-01 90 03

```
iptables -A INPUT -p icmp -m limit --limit 10/s --limit-burst 50 \  
-j ACCEPT  
iptables -A INPUT -j DROP  
# Отбрасывать ошибочные пакеты  
iptables -A INPUT -m state --state INVALID -j DROP  
iptables -I INPUT -m conntrack --ctstate INVALID -j DROP  
# Отбрасывать фрагментированные пакеты  
iptables -A INPUT -f -j DROP  
# Защита от попытки открыть входящее соединение TCP не через SYN  
iptables -I INPUT -m conntrack --ctstate NEW -p tcp ! --syn -j DROP  
# Защита от Ping of death  
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit  
10/s --limit-burst 50 -j ACCEPT  
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP  
# Защита от некорректных ICMP  
iptables -I INPUT -p icmp -f -j DROP  
# Отбросить ошибочные пакеты  
iptables -A FORWARD -m state --state INVALID -j DROP  
iptables -I FORWARD -m conntrack --ctstate INVALID -j DROP  
# Отбросить фрагментированные пакеты  
iptables -A FORWARD -f -j DROP  
# Сбрасывать фрагментированные пакеты  
iptables -A OUTPUT -f -j DROP
```

Дополнительно требуется внести правки в /etc/sysctl.conf:

```
# vim /etc/sysctl.conf  
  
# Отбросить ICMP-редиректы (против атак типа MITM)  
net.ipv4.conf.all.accept_redirects=0  
net.ipv6.conf.all.accept_redirects=0  
# Включить механизм TCP syncookies  
net.ipv4.tcp_syncookies=1  
# Различные улучшения (защита от подмены  
# увеличение очереди «полуоткрытых» TCP-соединений и далее):  
net.ipv4.tcp_timestamps=0  
net.ipv4.conf.all.rp_filter=1  
net.ipv4.tcp_max_syn_backlog=1280  
kernel.core_uses_pid=1
```

4. ФУНКЦИИ И ЗАДАЧИ АДМИНИСТРИРОВАНИЯ ОС АЛЬТ СП

4.1. Функции администратора

Основными функциями администратора при эксплуатации ОС Альт СП являются:

- ввод в эксплуатацию и эксплуатация в соответствии с указаниями, приведенными в документе «Формуляр. ЛКНВ.11100-01 30 01»;
- соблюдение подготовительных процедур (см. раздел 3);
- установка и настройка ОС Альт СП;
- управление и поддержка функционирования ПЭВМ.

4.2. Задачи администрирования

В состав основных задач администрирования входят следующие:

- установка ОС Альт СП и назначение параметров системы;
- создание загрузочных носителей информации;
- конфигурирование параметров даты и времени, графической среды, средств ввода и вывода;
- настройка и управление системными сервисами и служебными программами;
- настройка и управление работой системы управления пакетами Advanced Packaging Tool (далее – АРТ);
- обновление ОС и прикладного ПО из ее состава;
- настройка и управление учетными записями и правами доступа пользователей;
- конфигурирование сети `/etc/net` и проверка ее работоспособности;
- настройка FTP-серверов;
- настройка служб DNS;
- настройка серверов электронной почты postfix;
- настройка и управление кэширующими прокси-серверами;
- настройка серверного и клиентского ПО Samba для осуществления связи UNIX-машин с сетями Microsoft и LanManager;

- настройка и управление печатью;
- настройка и управление базами данных.

5. УСТАНОВКА ОС АЛЬТ СП

Обычно для установки дистрибутива используется установочный загрузочный компакт-диск дистрибутива. Если установка производится с компакт-диска, можно сразу перейти к п. 5.2 и п. 5.4.

Для начала процесса установки ОС Альт СП нужно:

- выбрать способ первоначальной загрузки компьютера;
- выбрать источник установки.

В случае загрузки с установочного компакт-диска эти две возможности предоставляются самим диском: он является загрузочным и содержит все требуемые для установки файлы. Однако вполне допустим и такой вариант: первоначальная загрузка происходит со специально подготовленного USB-flash-накопителя, а установочные файлы берутся с FTP-сервера сети.

Установка с загрузочного компакт-диска – это один из возможных способов установки системы. Он является самым распространенным способом установки системы, но не работает, например, в случае отсутствия на компьютере CD/DVD-привода. Для таких случаев поддерживаются альтернативные методы установки (см. п. 5.1).

5.1. Запись установочного образа на USB-flash-накопитель

⚠ Запись образа дистрибутива на USB-flash-накопитель приведет к изменению таблицы разделов на носителе, таким образом, если USB-flash-накопитель выполнил функцию загрузочного\установочного устройства и требуется вернуть ему функцию переносного накопителя данных, то нужно удалить все имеющиеся разделы на USB-flash-накопителе и создать нужное их количество заново.

⚠ Для восстановления совместимости USB-flash-накопителя с ОС семейства Windows может понадобиться также пересоздание таблицы разделов (например, при помощи parted). Нужно удалить таблицу GPT и создать таблицу типа msdos. Кроме того, должен быть только один раздел с FAT или NTFS.

Для создания загрузочного USB-flash-накопителя требуется файл ISO-образа установочного носителя информации с дистрибутивом.

ISO-образы установочных носителей информации являются гибридными (Hybrid ISO/IMG), что позволяет записывать их на USB-flash-накопитель.

В ОС Linux для записи образа на USB-flash-накопитель можно воспользоваться любой программой с графическим интерфейсом, например:

- ALT Media Writer (altmediawriter);
- SUSE Studio Imagewriter.

Для записи установочного образа можно также воспользоваться утилитой командной строки `dd`, выполнив с правами пользователя `root` следующие команды:

```
# dd oflag=direct if=<файл-образа.iso> of=/dev/sdX bs=1M;sync
```

где:

- `<файл-образа.iso>` – ISO-образ установочного диска с дистрибутивом;
- `/dev/sdX` – устройство, соответствующее USB-flash-накопителю.

Для удобства отображения прогресса записи можно установить пакет `pv` и запустить команду:

```
# pv <файл-образа.iso> | dd oflag=direct of=/dev/sdX bs=1M;sync
```

Точное обозначение устройства можно узнать, выполнив команду `dmesg`, после подключения USB-flash-накопителя к компьютеру. Например:

```
# dmesg | grep disk
```

```
[ 1.171036] sd 0:0:0:0: [sda] Attached SCSI disk
```

```
[ 4.755468] sd 1:0:0:0: [sdb] Attached SCSI disk
```

```
[53271.629338] sd 5:0:0:0: [sdc] Attached SCSI removable disk
```

Здесь USB-flash-накопитель имеет имя устройства `sdc`.

Просмотреть список доступных устройств также можно командой `lsblk` или (если такой команды нет): `blkid`.

⚠ Будьте внимательны при указании имени USB-устройства – запись образа по ошибке на жесткий диск приведет к потере данных на нем.

⚠ Не добавляйте номер раздела, образ пишется на USB-flash-накопитель с самого начала!

⚠ Пока образ не запишется до конца нельзя извлекать USB-flash-накопитель. Примеры даны с дополнительной командой sync, которая вызывает сброс кэша на носителях, в том числе и для только что записанного USB-flash-накопителя, так что после завершения sync USB-flash-накопитель можно извлечь.

В среде ОС Windows для создания загрузочного USB-flash-накопителя рекомендуется использовать специализированные программные средства, например: ALT Media Writer, Win32 Disk Imager и другие.

Созданный, описанным выше способом, USB-flash-накопитель является одновременно и загрузочным, и установочным. В результате, установка дистрибутива может быть произведена исключительно с использованием USB-flash-накопителя.

5.2. Начало установки: загрузка системы

Для загрузки компьютера с целью установки системы нужно воспользоваться носителем, содержащим начальный загрузчик. Таким носителем может быть, как сам загрузочный компакт-диск дистрибутива, так и, например, USB-flash-накопитель, который можно сделать загрузочным (см. п. 5.1).

Примечания:

1. Перед установкой системы нужно выставить точное время в базовой системе ввода-вывода (БСВВ).

2. Может потребоваться включить в БСВВ опцию загрузки с CD/DVD-привода. Способ входа в меню БСВВ и информация о расположении настроек определяется производителем используемого оборудования. За информацией можно обратиться к документации на оборудование.

После загрузки компьютера с установочного компакт-диска или специально подготовленного USB-flash-накопителя (см. п. 5.1) выводится меню, в котором возможно перечисление нескольких вариантов загрузки, зависит от особенностей архитектуры процессора, причем установка системы – это только одна из возможностей.

Загрузчик рабочей станции (рис. 2) включает следующие пункты:

- «Установить ALT SP Workstation 10.2» – установка ОС;

- «Установить через VNC ALT SP Workstation 10.2 (измените пароль и соединение здесь)» – установка по VNC с соединением в сторону устанавливаемой машины (см. п. 5.3);
- «Спасательный LiveCD» – восстановление уже установленной, но так или иначе поврежденной ОС Linux путем запуска небольшого образа ОС в оперативной памяти. Восстановление системы потребует некоторой квалификации. Этот пункт также может быть использован для сбора информации об оборудовании компьютера, которую можно отправить разработчикам, если ОС Альт СП устанавливается и работает неправильно. Загрузка восстановительного режима заканчивается приглашением командной строки: [root@localhost /]#;
- «Change language (press F2)» («Изменить язык (нажмите F2)») – позволяет выбрать язык интерфейса загрузчика и программы установки (нажатие клавиши <F2> вызывает такое же действие);
- «UEFI Firmware Settings» – позволяет получить доступ к настройкам UEFI.

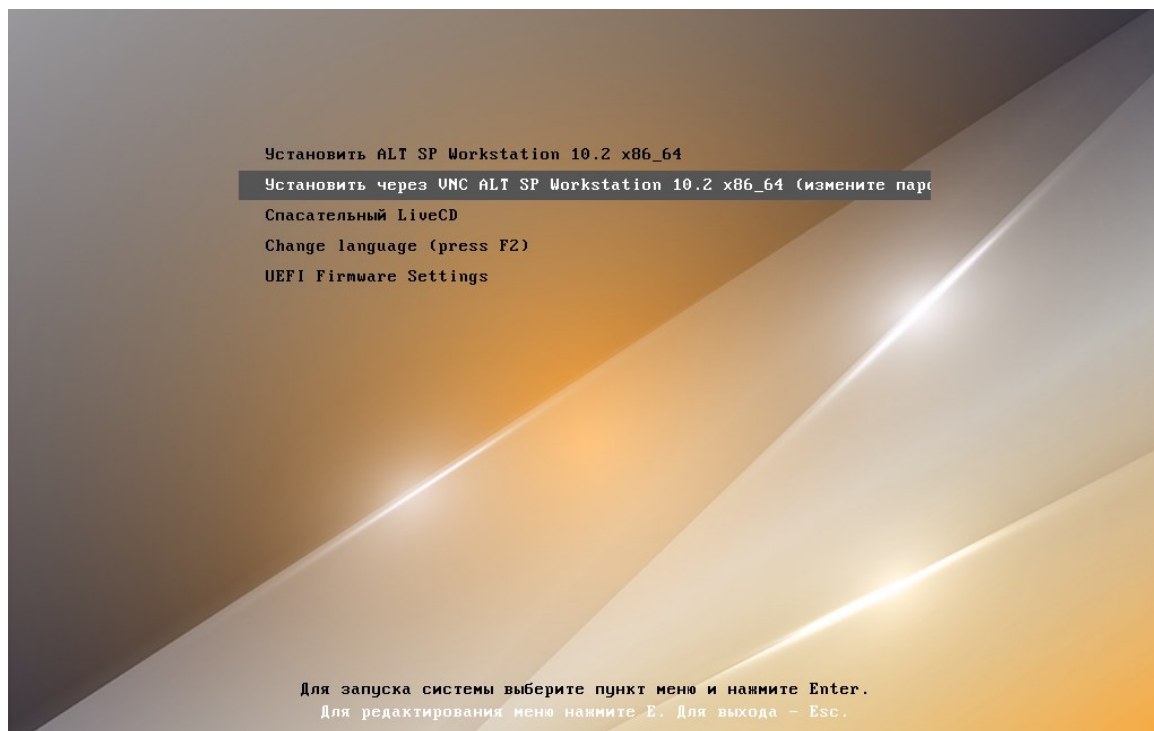


Рис. 2 – Загрузка с установочного диска рабочей станции

Примечание. На данном этапе установки не поддерживается «мышь», поэтому для выбора различных вариантов и опций установки следует воспользоваться клавиатурой.

Примечание. Начальный загрузчик рабочей станции в режиме Legacy показан на рис. 3. Пункт «Загрузка с жесткого диска» позволяет запустить уже установленную на жестком диске операционную систему.

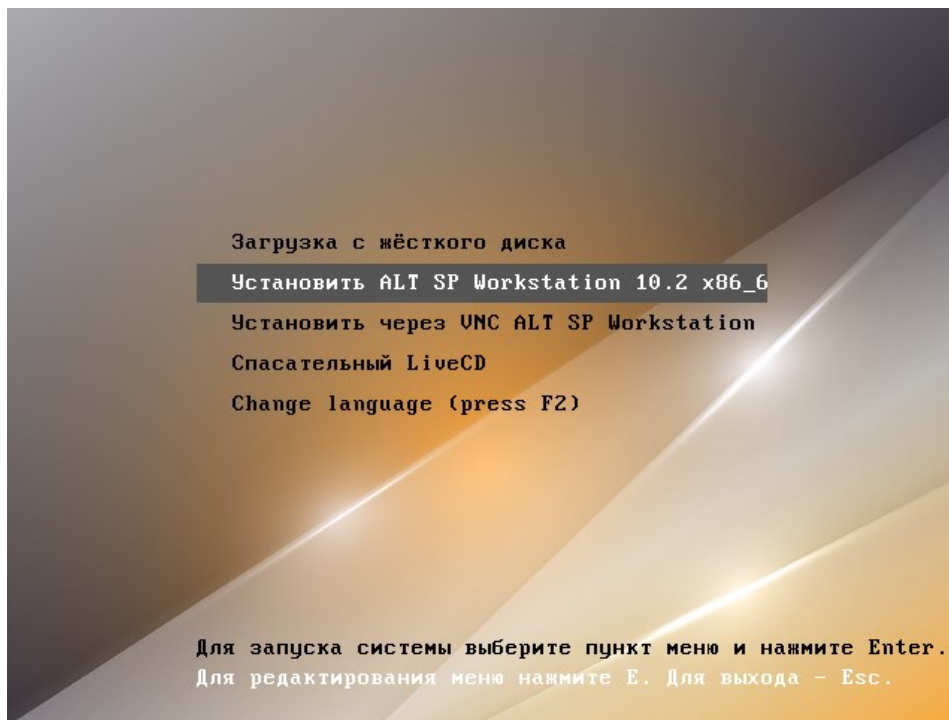


Рис. 3 – Пример загрузки с установочного диска в режиме Legacy

Загрузчик сервера (рис. 4) включает следующие пункты:

- «Install ALT SP Server 10.2» – установка ОС;
- «VNC install ALT SP Server 10.2 (edit to set password and connect here)» – установка по VNC с соединением в сторону устанавливаемой машины (см. п. 5.3);
- «Rescue LiveCD» – восстановление уже установленной, но так или иначе поврежденной ОС Linux путем запуска небольшого образа ОС в оперативной памяти. Загрузка восстановительного режима заканчивается приглашением командной строки: `[root@localhost /]#`;
- «UEFI Firmware Settings» – позволяет получить доступ к настройкам UEFI.

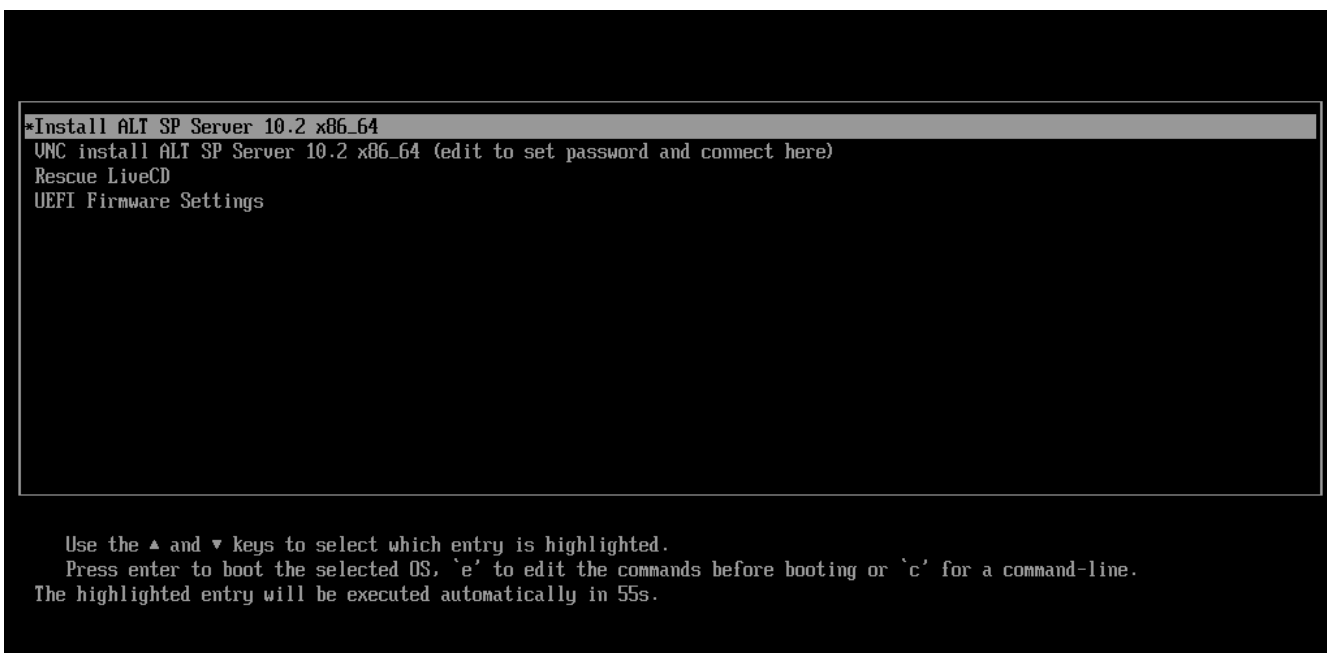


Рис. 4 – Загрузка с установочного диска сервера

Для редактирования параметров текущего пункта загрузки нажмите клавишу <E>.

Примечание. Начальный загрузчик сервера в режиме Legacy показан на рис. 5.

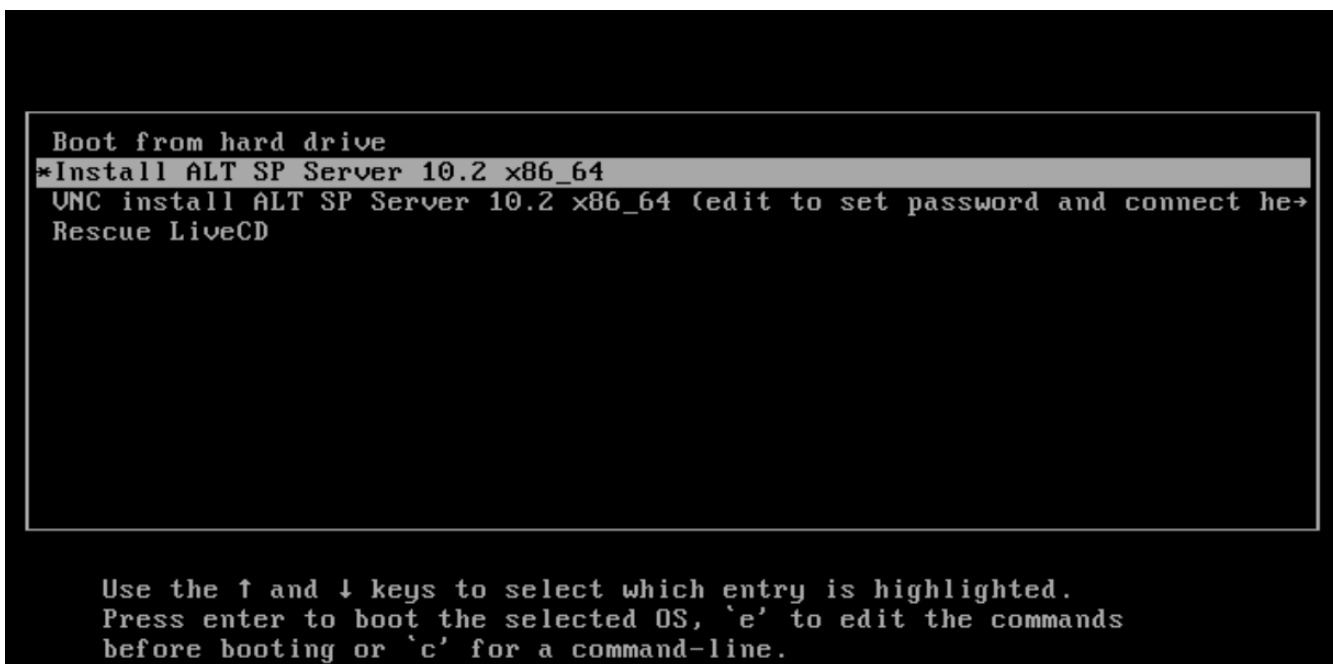


Рис. 5 – Пример загрузки сервера в режиме Legacy

Сочетание клавиш <Ctrl>+<Alt>+<F1> – выдает технические сведения о выполнении процесса установки ОС Альт СП.

Чтобы начать процесс установки, нужно клавишами перемещения курсора вверх <↑>, вниз <↓> выбрать пункт меню «Установить ALT SP Workstation 10.2» и нажать клавишу <Enter>.

Начальный этап установки не требует вмешательства пользователя: происходит автоматическое определение оборудования и запуск компонентов программы установки. Сообщения о том, что происходит на этом этапе, можно просмотреть, нажав клавишу <ESC>.

Примечание. В начальном загрузчике установлено небольшое время ожидания: если в этот момент не предпринимать никаких действий, то будет загружена та система, которая уже установлена на жестком диске. Если пропустили нужный момент, перезагрузите компьютер и вовремя выберите пункт «Установка».

5.3. Установка через VNC

Для управления сетевой установкой следует подключить машину к сети и обеспечить ей получение адреса по DHCP, затем выбрать пункт в меню установки «Установить через VNC ALT SP Server/Workstation (измените пароль и соединение здесь)» (см. рис. 2).

После запуска установки по VNC будет запущен сервер VNC (рис. 6) и машина будет ожидать подключения к нему, стандартный пароль для подключения «VNCPWD».

Примечание. Параметры установки по VNC передаются как параметры ядра. Нажатие клавиши <E>, при выбранном пункте «Установить через VNC ALT SP Server/Workstation (измените пароль и соединение здесь)» (рис. 2), позволяет задать пароль VNC (рис. 7).

```
init-bottom: Root fs is squashfs
init-bottom: Remounting / with Overlayfs
init-bottom: Root FS overlaid with Overlayfs
Spawning init ... done.
Starting systemd-udevd service: [ DONE ]
Populating /dev: [ DONE ]
Running initinstall script [00-create-missing-symlinks-in-dev.sh] [ DONE ]
Running initinstall script [01-apt-cache-limit.sh] [ DONE ]
Running initinstall script [01-multipath.sh] [ DONE ]
Running initinstall script [05-efi.sh] [ DONE ]
Running initinstall script [10-disk.sh] [ DONE ]
Running initinstall script [10-network.sh] [ DONE ]
Running initinstall script [10-serial.sh] [ DONE ]
Running initinstall script [10-vm-profile.sh] [ DONE ]
Running initinstall script [10-ut.sh] [ DONE ]
Running initinstall script [15-expert.sh] [ DONE ]
Running initinstall script [20-bend-license-ru-step.sh] [ DONE ]
Running initinstall script [20-nodesign.sh] [ DONE ]
Running initinstall script [20-pts.sh] [ DONE ]
Running initinstall script [25-setup-dhcp.sh] [ DONE ]
Running initinstall script [26-metadata-autoinstall.sh] [ DONE ]
Running initinstall script [27-metadata-install-scripts.sh] [ DONE ]
Running initinstall script [30-ntp-client.sh] [ DONE ]
Running initinstall script [30-turn-grub-password-on.sh] [ DONE ]
Running initinstall script [30-ntp-client.sh] [ DONE ]
Running initinstall script [30-turn-grub-password-on.sh] [ DONE ]
Running initinstall script [40-xorg.sh] [ DONE ]
Running initinstall script [50-removable] [ DONE ]
Running initinstall script [80-stop-md-dm.sh] [ DONE ]
Running initinstall script [85-start-multipath.sh] [ DONE ]
Running initinstall script [90-alteratord.sh] [ DONE ]
Running initinstall script [90-date.sh] [ DONE ]
Running initinstall script [90-pkg.sh] [ DONE ]
Running initinstall script [95-add-remount-step.sh] [ DONE ]
Running initinstall script [98-oem.sh] [ DONE ]
stored passwd in file: /tmp/uncpasswd
Waiting for network...
** IP(s): 192.168.0.193
** UNC cmdline: uncpasswd=UNCPWD

The UNC desktop is: localhost.localdomain:0
PORT=5900
```

Рис. 6 – Запуск сервера VNC

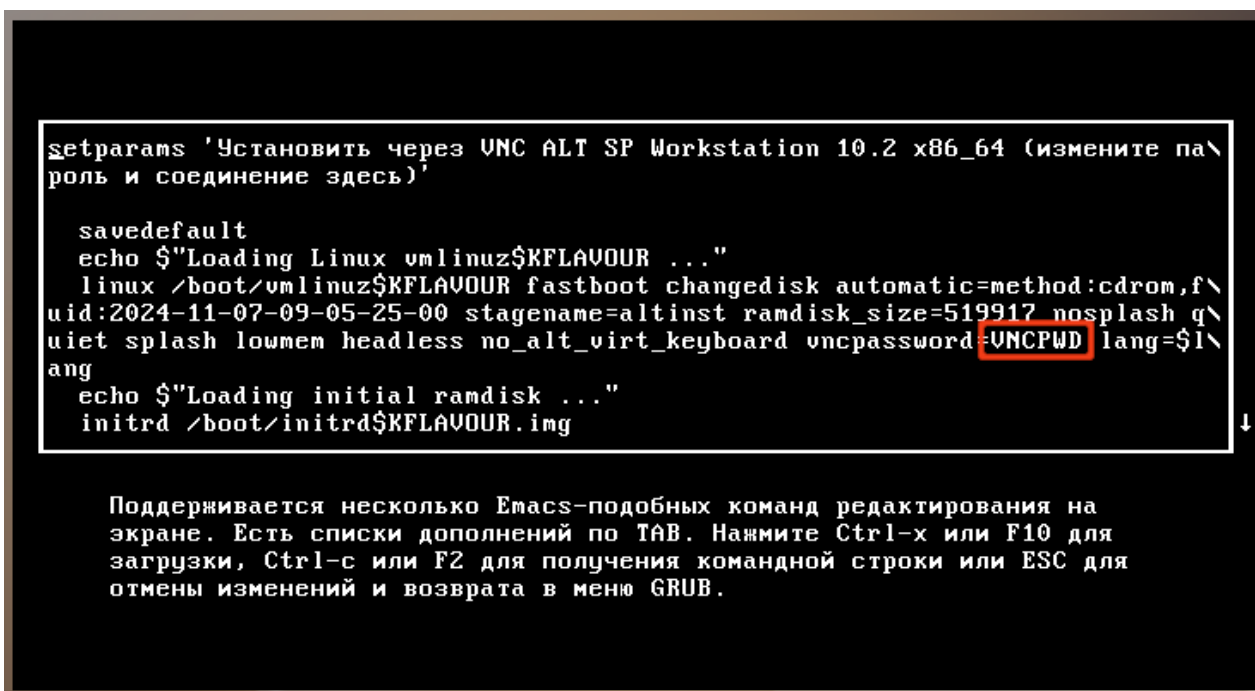


Рис. 7 – Параметры установки по VNC

Далее требуется выполнить подключение к данному VNC-серверу и продолжить установку ОС (рис. 8).

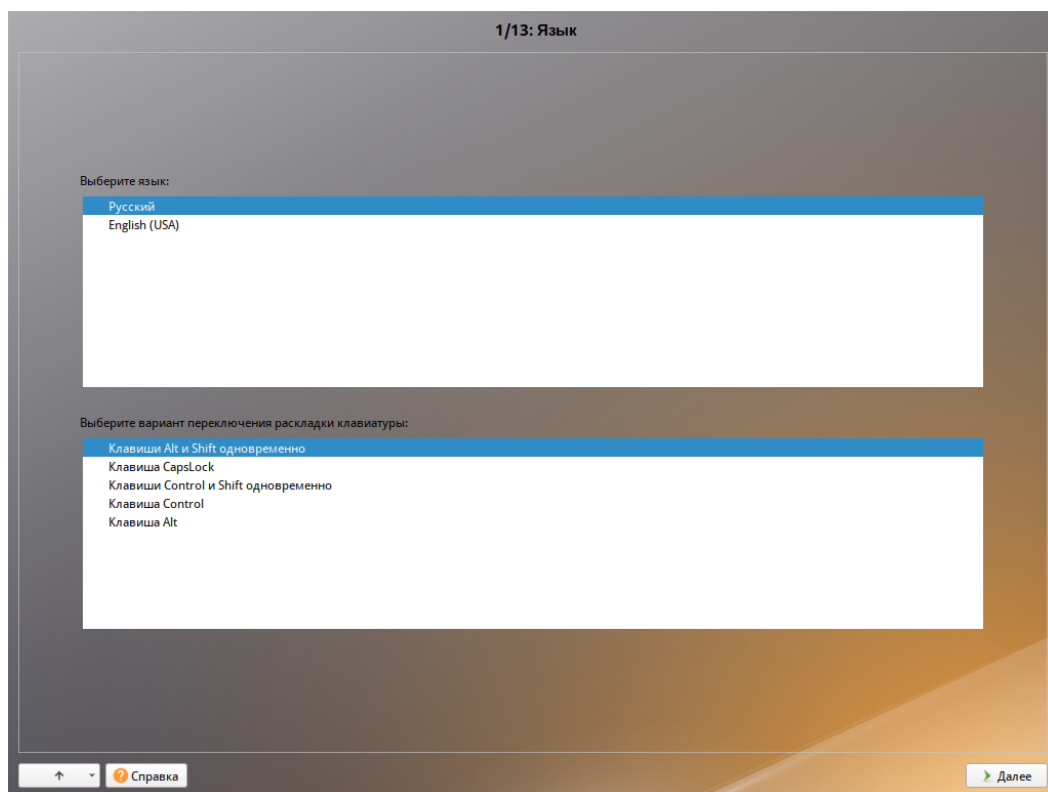


Рис. 8 – Подключение к VNC-серверу для дальнейшей установки ОС

5.4. Последовательность установки

До того как будет произведена установка базовой системы на жесткий диск, программа установки работает с образом системы, загруженным в оперативную память компьютера.

Если инициализация оборудования завершилась успешно, будет запущен графический интерфейс программы-установщика.

Процесс установки разделен на шаги; каждый шаг посвящен настройке или установке определенного свойства системы. Шаги нужно проходить последовательно, переход к следующему шагу происходит по нажатию кнопки «Далее». При помощи кнопки «Назад» можно вернуться к уже пройденному шагу и изменить настройки. Однако на этом этапе установки возможность перехода к предыдущему шагу ограничена теми шагами, где нет зависимости от данных, введенных ранее.

В случае необходимости отмены установки, следует нажать кнопку <Reset> на корпусе системного блока компьютера.

Примечание. Совершенно безопасно выполнить отмену установки только до шага «Подготовка диска» (см. п. 5.4.4), поскольку до этого момента не производится никаких изменений на жестком диске. Если прервать установку между шагами «Подготовка диска» и «Установка загрузчика» (см. п. 5.4.8), существует вероятность, что после этого с жесткого диска ОС не сможет загрузиться.

Технические сведения о ходе установки можно посмотреть, нажав клавиши <Ctrl>+<Alt>+<F1>, вернуться к программе установки – <Ctrl>+<Alt>+<F7>. По нажатию клавиш <Ctrl>+<Alt>+<F2> откроется отладочная виртуальная консоль.

Каждый шаг сопровождается краткой справкой, которую можно вызвать, нажав <F1>.

Во время установки системы выполняются следующие шаги:

- язык (см. п. 5.4.1);
- лицензионное соглашение (см. п. 5.4.2);
- дата и время (см. п. 5.4.3);
- подготовка диска (см. п. 5.4.4);
- перемонтирование (см. п. 5.4.5);

- установка системы (см. п. 5.4.6);
- сохранение настроек (см. 5.4.7);
- установка загрузчика (см. п. 5.4.8);
- настройка сети (см. п. 5.4.9);
- администратор системы (см. п. 5.4.10);
- системный пользователь (см. п. 5.4.11);
- в случае создания LUKS разделов – этап установки пароля на LUKS разделы (см. п. 5.4.12);
- завершение установки (см. п. 5.4.13).

П р и м е ч а н и е . Некоторые шаги при установке могут отсутствовать в связи с особенностями архитектуры процессора.

5.4.1. Язык

Установка начинается с выбора основного языка – языка интерфейса программы установки и устанавливаемой системы (рис. 9).

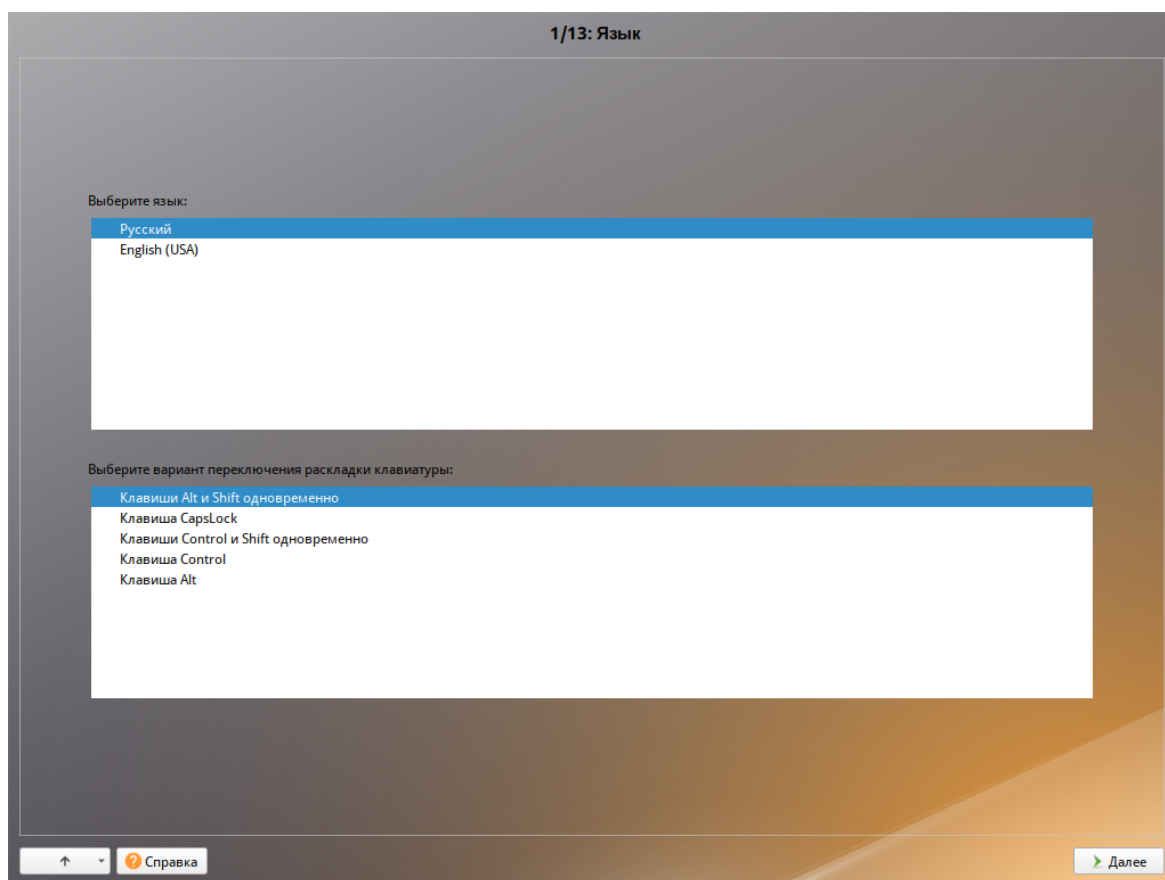


Рис. 9 – Установка. Выбор языка

На данном этапе также выбирается вариант переключения раскладки клавиатуры. Раскладка клавиатуры – это привязка букв, цифр и специальных символов к клавишам на клавиатуре. Переключение между раскладками осуществляется при помощи специально зарезервированных для этого клавиш.

Для настройки варианта переключения раскладки клавиатуры в пункте «Выберите вариант переключения раскладки клавиатуры» нужно установить одно из следующих значений (доступно при выборе русского языка, в качестве основного):

- клавиши <Alt> и <Shift> одновременно;
- клавиша <CapsLock>;
- клавиши <Control> и <Shift> одновременно;
- клавиша <Control>;
- клавиша <Alt>.

Если выбранный основной язык имеет всего одну раскладку (например, при выборе английского языка в качестве основного), эта единственная раскладка будет принята автоматически.

После завершения настройки основного языка и варианта переключения раскладки клавиатуры нужно нажать на кнопку «Далее».

5.4.2. Лицензионное соглашение

После окна выбора языковых параметров ОС Альт СП программа установки переходит к окну «Лицензионное соглашение» (рис. 10).

Перед продолжением установки следует внимательно прочитать условия, регулирующие права владельца экземпляра дистрибутива ОС Альт СП на использование дистрибутива, а также включенных в состав дистрибутива отдельных программ для ЭВМ в установленных условиях пределах.

Для подтверждения согласия следует отметить пункт «Да, я согласен с условиями» и нажать на кнопку «Далее».

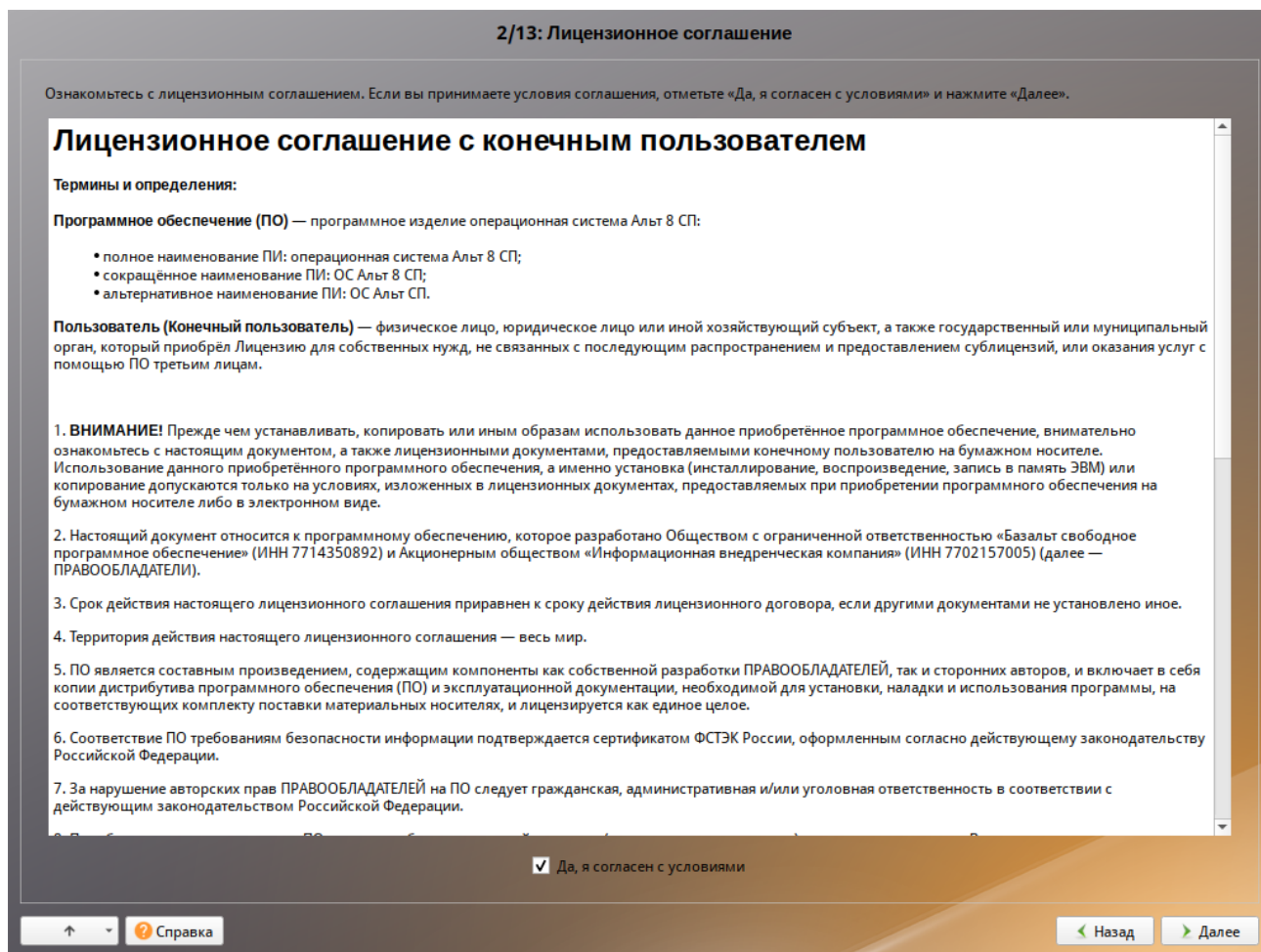


Рис. 10 – Установка. Лицензионное соглашение

5.4.3. Дата и время

После окна «Лицензионное соглашение» ОС Альт СП программа установки переходит к окну «Дата и время». На данном этапе выполняется выбор региона и города, по которым будет определен часовой пояс и установлены системные часы (рис. 11).

Для указания часового пояса в соответствующих списках выберите регион, а затем город. Поиск по списку можно ускорить, набирая на клавиатуре первые буквы искомого слова.

Пункт «Хранить время в BIOS по Гринвичу» выставляет настройки даты и времени в соответствии с часовыми поясами, установленными по Гринвичу, и добавляет к местному времени часовую поправку для выбранного региона.

После выбора часового пояса будут предложены системные дата и время по умолчанию.

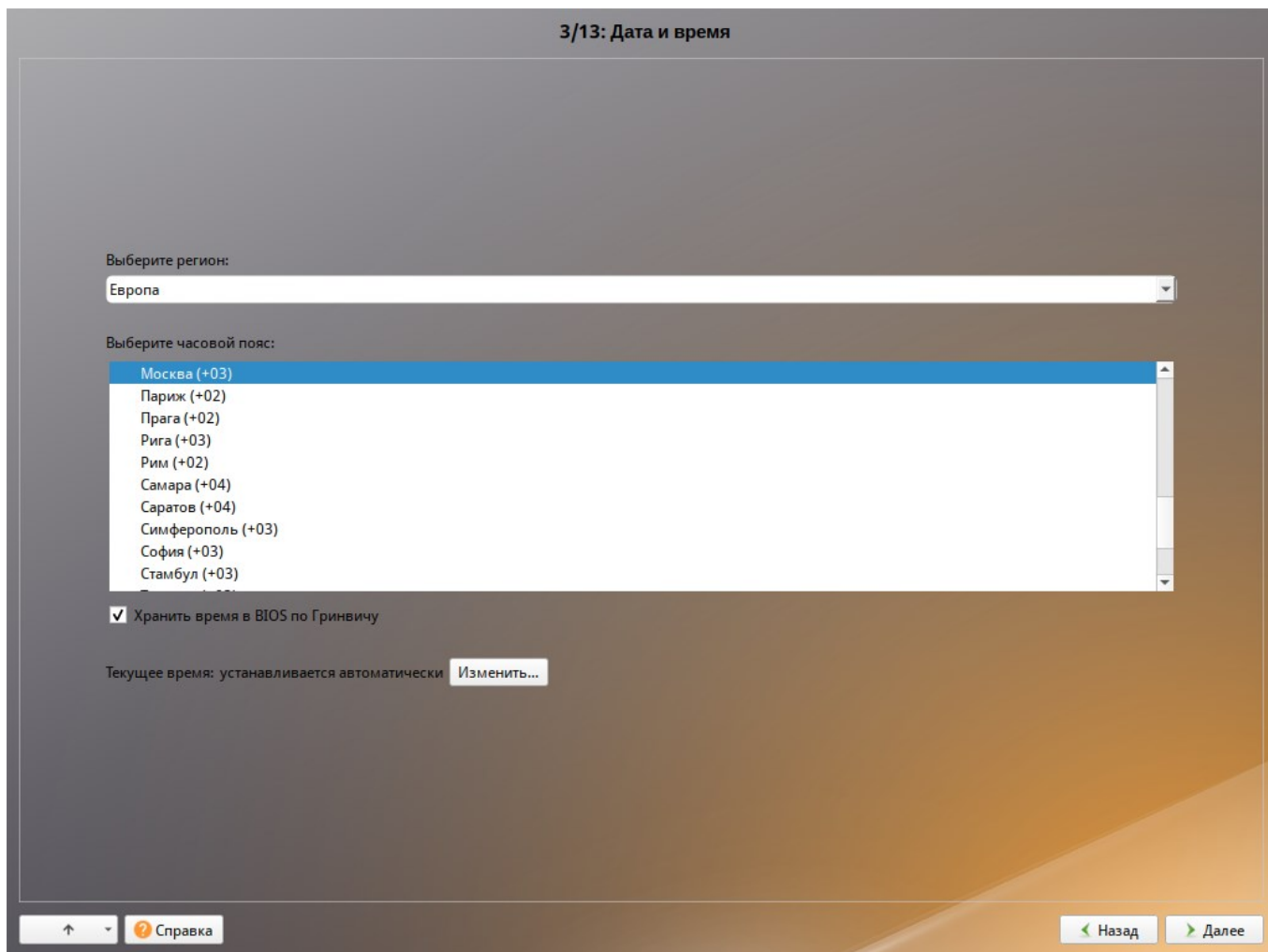


Рис. 11 – Установка. Выбор часового пояса

Для ручной установки текущих даты и времени нужно нажать на кнопку «Изменить...». Откроется окно ручной настройки системных параметров даты и времени (рис. 12).

По умолчанию для синхронизации системных часов (NTP) с удаленным сервером по сети Интернет отмечен пункт «Получать точное время с NTP-сервера» и указан NTP-сервер `pool.ntp.org`.

Если выбрана опция «Получать точное время с NTP-сервера», то компьютер может и сам быть сервером точного времени. Для работы компьютера в качестве сервера точного времени внутри локальной сети нужно отметить пункт «Работать как NTP-сервер».

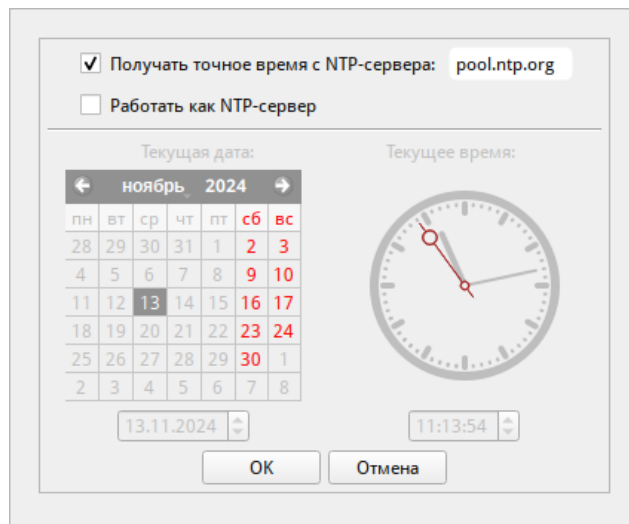


Рис. 12 – Установка. Настройка времени

Для сохранения настроек и продолжения установки системы в окне ручной установки даты и времени следует нажать на кнопку «ОК» и затем в окне «Дата и время» нажать на кнопку «Далее».

5.4.4. Подготовка диска

На этом этапе программа установки подготавливает площадку для установки ОС Альт СП, в первую очередь – выделяется свободное место на диске.

Переход к этому шагу может занять некоторое время – период ожидания может быть разным и зависит от производительности компьютера, объема жесткого диска, количества разделов на нем и других параметров.

5.4.4.1. Выбор профиля разбиения диска

После завершения первичной конфигурации загрузочного носителя откроется окно «Подготовка диска» (рис. 13). В списке разделов перечислены уже существующие на жестких дисках разделы (в том числе здесь могут оказаться съемные USB-носители, подключенные к компьютеру в момент установки).

В списке «Выберите профиль» перечислены доступные профили разбиения диска. Профиль – это шаблон распределения места на диске для установки ОС. Можно выбрать один из профилей:

- установка сервера/рабочей станции;
- вручную.

Первый профиль предполагает автоматическое разбиение диска.

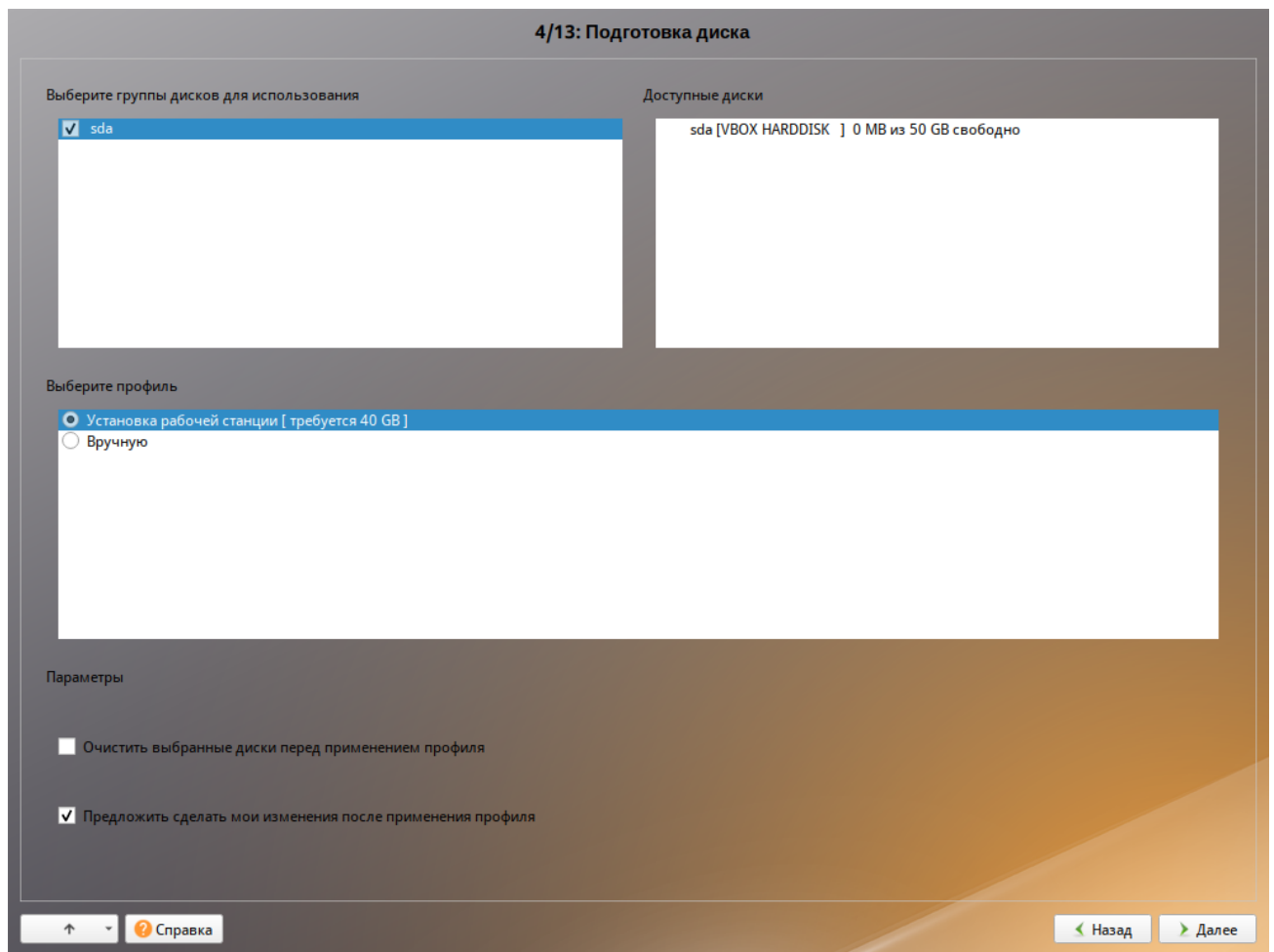


Рис. 13 – Установка. Установка рабочей станции

5.4.4.2. Автоматические профили разбиения диска

Если происходит установка рабочей станции, то при выборе профиля «Установка рабочей станции» будут выделены отдельные разделы для EFI, для корневой файловой системы и для /home (рис. 14).



Рис. 14 – Установка. Профиль «Установка рабочей станции»

Если происходит установка сервера, то при выборе «Установка сервера» профиля будут выделены отдельные разделы для EFI и для корневой файловой системы. Если размер диска больше 120 Гбайт (рис. 15), будет также создан раздел `/var` (23,8 Гбайт для корневой файловой системы, остальное под `/var`).



Рис. 15 – Установка. Профиль «Установка сервера»

Примечание. Если происходит установка ОС с UEFI, то при разбиении диска будет автоматически выделен раздел `/boot/efi` размером 512 Мбайт.

Если результат разбиения дисков по каким-то причинам не устраивает, сейчас можно его отредактировать.

От возможности редактировать результат разбиения можно отказаться, сняв выделение с пункта «Предложить сделать мои изменения после применения профиля». В этом случае никакой информации о распределении дискового пространства на экране отображаться не будет. После осуществления физических изменений на жестком диске начнется установка базовой системы. Этот вариант подойдет для установки на чистый диск.

Рядом с названием профиля указан минимальный объем свободного места на диске, требуемый для установки в соответствии с данным профилем:

- профиль «Установка рабочей станции»: 40 Гбайт для legacy и 40,5 Гбайт для UEFI;
- профиль «Установка сервера»: 24 Гбайт для legacy и 24,5 Гбайт для UEFI.

Если при применении профиля автоматического разбиения диска доступного места на диске окажется недостаточно, то на монитор будет выведено сообщение об ошибке: «Невозможно применить профиль, недостаточно места на диске». В этом случае можно воспользоваться методом ручной разметки: профиль «Вручную» или установить отметку на пункте «Очистить выбранные диски перед применением профиля».

Примечание. При отмеченном пункте «Очистить выбранные диски перед применением профиля» будут удалены все данные с выбранных дисков (включая внешние USB-носители) без возможности восстановления. Рекомендуется использовать эту возможность при полной уверенности в том, что диски не содержат никаких ценных данных.

5.4.4.3. Ручной профиль разбиения диска

При необходимости освободить часть дискового пространства следует воспользоваться профилем разбиения «Вручную». В этом случае можно удалить некоторые из существующих разделов или содержащиеся в них файловые системы. После этого можно создать разделы самостоятельно или вернуться к шагу выбора профиля и применить автоматический профиль. Выбор этой возможности требует знаний об устройстве диска и технологиях его разбиения.

По нажатию «Далее» будет произведена запись новой таблицы разделов на диск и форматирование разделов. Разделы, только что созданные на диске программой установки, пока не содержат данных и поэтому форматируются без предупреждения. Уже существовавшие, но измененные разделы, которые будут отформатированы, помечаются специальным значком в колонке «Файловая система» слева от названия. При уверенности в том, что подготовка диска завершена, подтвердите переход к следующему шагу нажатием кнопки «Далее».

Не следует форматировать разделы с теми данными, которые нужно сохранить, например, со старыми пользовательскими данными (/home). С другой стороны отформатировать можно любые разделы, которые нужно «очистить» (т. е. удалить все данные).

Для того чтобы система правильно работала (в частности могла загрузиться) с UEFI, при ручном разбиении диска следует обязательно сделать точку монтирования /boot/efi, в которую нужно смонтировать vfat раздел с загрузочными записями. Если такого раздела нет, то его надо создать вручную. При разбивке жесткого диска в автоматическом режиме такой раздел создает сам установщик.

Особенности разбиения диска в UEFI-режиме:

- требуется создать новый или подключить существующий FAT32-раздел с GPT-типом ESP (efi system partition) размером 100 – 500 Мбайт (будет смонтирован в /boot/efi);
- может понадобиться раздел типа «bios boot partition» минимального размера, никуда не подключенный и предназначенный для встраивания grub2-efi;
- остальные разделы – и файловая система, и swap – имеют GPT-тип «basic data»; актуальный тип раздела задается отдельно.

5.4.4.4. Дополнительные возможности разбиения диска

Ручной профиль разбиения диска позволяет установить ОС на программный RAID-массив, разместить разделы в томах LVM и использовать маскирование на разделах. Данные возможности требуют от пользователя понимания принципов функционирования указанных технологий.

5.4.4.4.1. Создание программного RAID-массива

Избыточный массив независимых дисков RAID (redundant array of independent disks) – технология виртуализации данных, которая объединяет несколько НЖМД в логический элемент для избыточности и повышения производительности.

Для создания программного RAID-массива потребуется минимум два жестких диска.

Программа установки поддерживает создание программных RAID-массивов следующих типов:

- RAID 1;
- RAID 0;
- RAID 4/5/6;
- RAID 10.

Процесс подготовки к установке на RAID условно можно разбить на следующие шаги:

- создание разделов на жестких дисках;
- создание RAID-массивов на разделах жесткого диска;
- создание файловых систем на RAID-массиве.

Примечание. Для создания программного RAID-массива может потребоваться предварительно удалить существующую таблицу разделов с жесткого диска.

Примечание. Системный раздел EFI должен быть физическим разделом в основной таблице разделов диска.

Для настройки параметров нового раздела из состава RAID-массива нужно выбрать неразмеченный диск в окне профиля разбивки пространства «Вручную» и нажать на кнопку «Создать раздел».

Для создания программного массива на GPT-разделах в открывшемся окне (рис. 16) нужно настроить следующие параметры:

- «Размер» – в поле нужно указать размер будущего раздела в Мбайт;
- «Смещение» – в поле нужно указать смещение начала данных на диске в Мбайт;
- «Тип раздела» – в выпадающем поле нужно выбрать значение «basic data» для последующего включения раздела в RAID-массивы;

- «Создать том» – следует снять отметку с этого пункта (не создавать том).

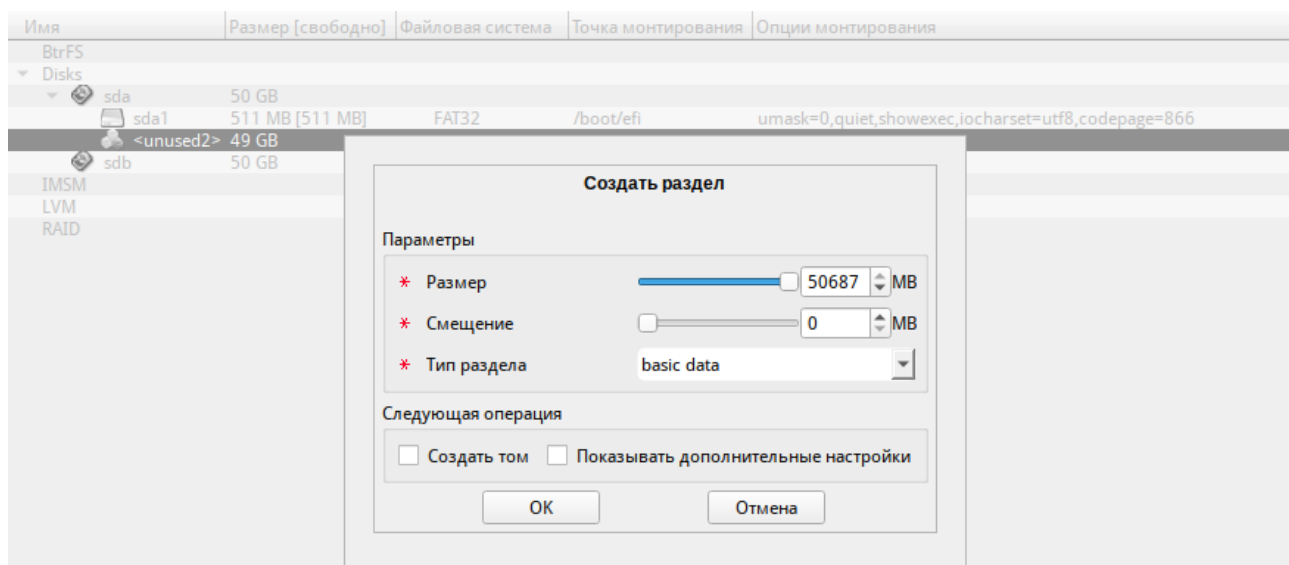


Рис. 16 – Создание раздела программного массива в режиме UEFI

Примечание. В режиме Legacy при создании разделов на жестких дисках для последующего включения их в RAID-массивы следует указать «Тип раздела» для них равным «Linux RAID» (рис. 17).

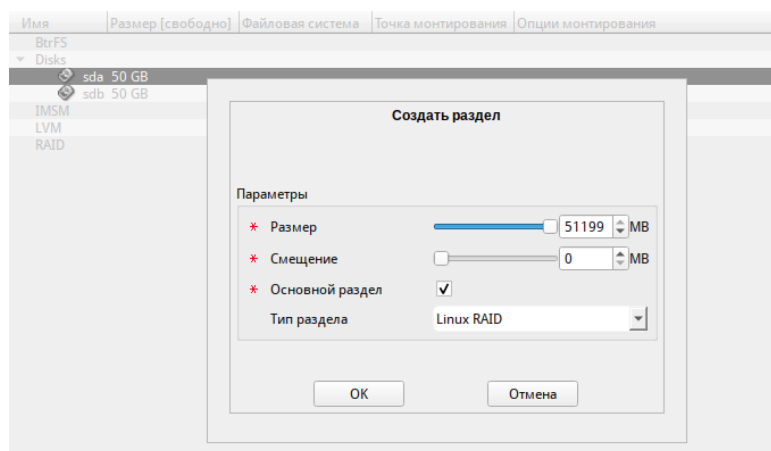


Рис. 17 – Создание раздела Linux RAID в режиме Legacy

На втором диске создать два раздела с типом «basic data» без создания на них томов. При этом разделы на разных дисках должны совпадать по размеру.

Примечание. При создании разделов следует учесть, что объем результирующего массива может зависеть от размера, включенных в него разделов жесткого диска. Например, при создании RAID 1 результирующий размер массива будет равен размеру минимального участника.

После создания разделов на дисках можно переходить к организации самих RAID-массивов. Для этого в списке следует выбрать пункт «RAID», после чего нажать на кнопку «Создать RAID». Далее мастер предложит выбрать тип массива и указать его участников (рис. 18, рис. 19).

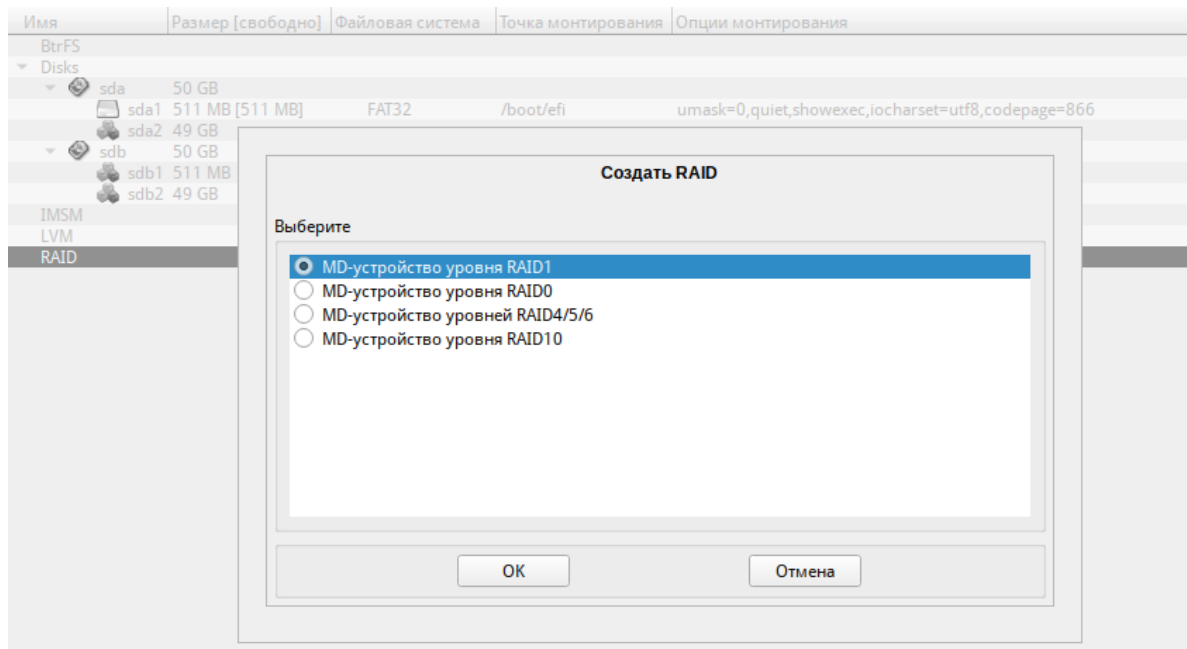


Рис. 18 – Установка. Выбор типа RAID-массива

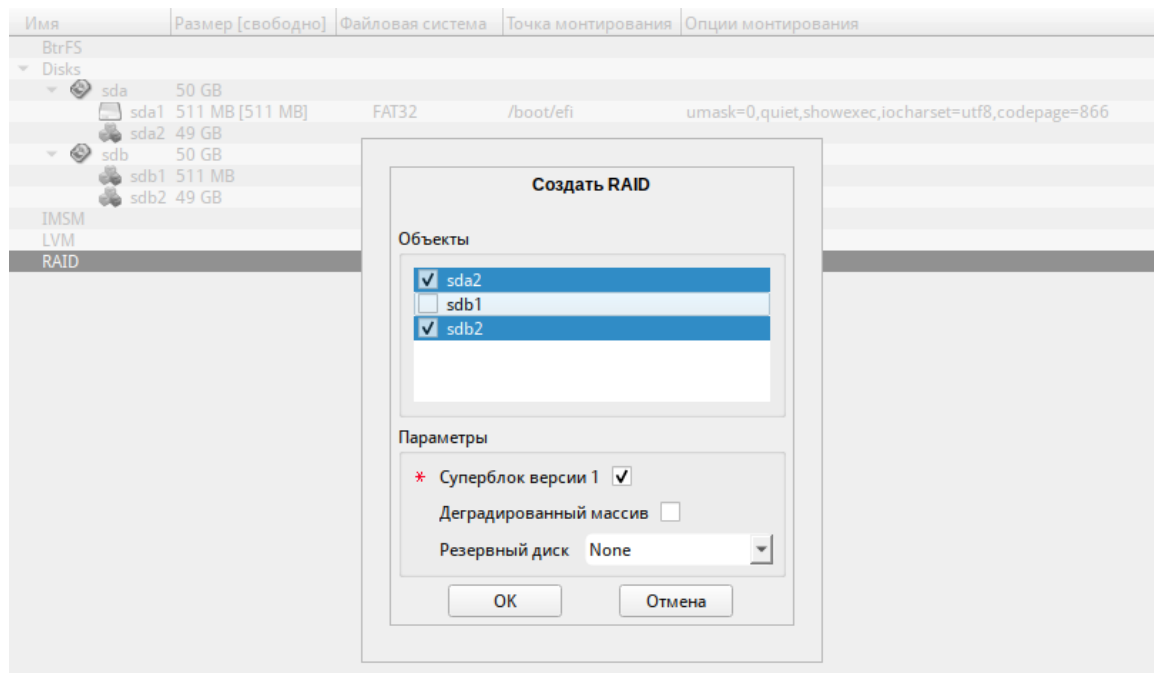


Рис. 19 – Установка. Выбор участников RAID-массива

Примечание. По умолчанию выбираются все разделы, поэтому необходимо снять отметку с раздела sdb1.

После того, как RAID-массив создан, его можно использовать как обычный раздел на жестких дисках, то есть на нем можно создавать файловые системы или же, например, включать в LVM-тома.

Примечание. После установки системы можно будет создать еще один RAID-массив и добавить в него загрузочный раздел (/boot/efi).

5.4.4.4.2. Создание LVM-томов

Менеджер логических дисков LVM (Logical Volume Manager) – средство гибкого управления дисковым пространством, позволяющее создавать поверх физических разделов (либо неразбитых дисков) логические тома, которые в самой системе будут видны как обычные блочные устройства с данными (обычные разделы).

Процесс подготовки к установке на LVM можно разбить на следующие шаги:

- создание разделов на жестких дисках;
- создание группы томов LVM;
- создание томов LVM;
- создание файловых систем на томах LVM.

Примечание. Для создания группы томов LVM может потребоваться предварительно удалить таблицу разделов с жесткого диска.

Примечание. Системный раздел EFI должен быть физическим разделом в основной таблице разделов диска.

Для настройки параметров нового раздела нужно выбрать неразмеченный диск в окне профиля разбивки пространства «Вручную» и нажать на кнопку «Создать раздел». В открывшемся окне (см. рис. 16) нужно настроить следующие параметры:

- «Размер» – в поле нужно указать размер будущего раздела в Мбайт;
- «Смещение» – в поле нужно указать смещение начала данных на диске в Мбайт;
- «Тип раздела» – в выпадающем поле нужно выбрать значение «basic data» для последующего включения раздела в LVM-тома;

- «Создать том» – нужно снять отметку с этого пункта (не создавать том).

Примечание. В режиме Legacy при создании разделов на жестких дисках для последующего включения их в LVM-тома следует указать «Тип раздела» для них, равным «Linux LVM» (рис. 20).

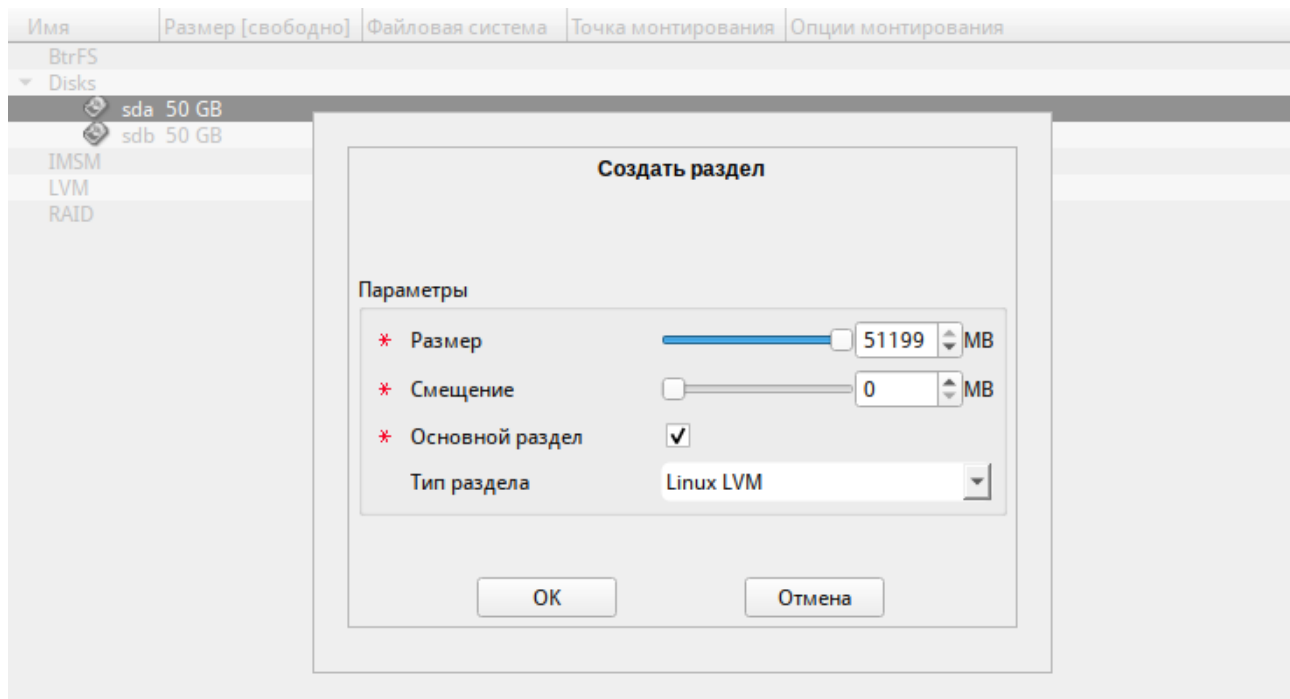


Рис. 20 – Создание раздела Linux LVM в режиме Legacy

После создания разделов на дисках можно переходить к созданию группы томов LVM. Для этого в списке следует выбрать «LVM», после чего нажать кнопку «Создать группу томов».

В открывшемся окне (рис. 21) необходимо выбрать физические разделы, которые будут входить в группу томов, указать название группы и выбрать размер экстенда.

Примечание. Размер экстенда представляет собой наименьший объем пространства, который может быть выделен тому. Размер экстенда по умолчанию 65536 (65536*512 байт = 32 Мбайт, где 512 байт – размер сектора).

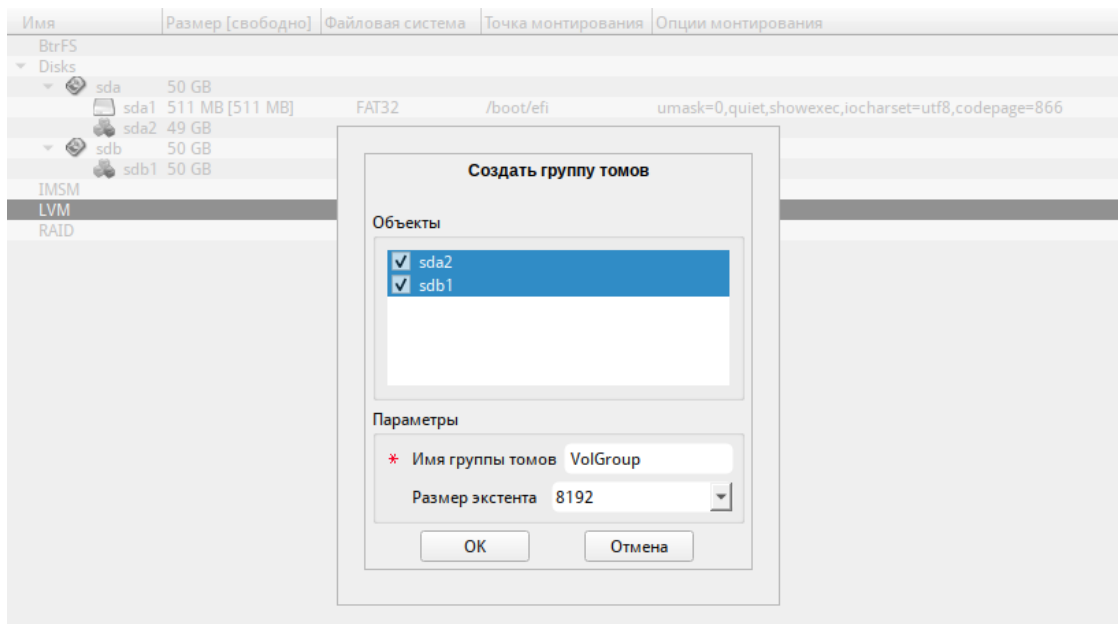


Рис. 21 – Установка. Подготовка диска. Создание группы томов LVM

После того, как группа томов LVM создана, ее можно использовать как обычный жесткий диск, то есть внутри группы томов можно создавать тома (аналог раздела на физическом жестком диске) и файловые системы внутри томов (рис. 22).

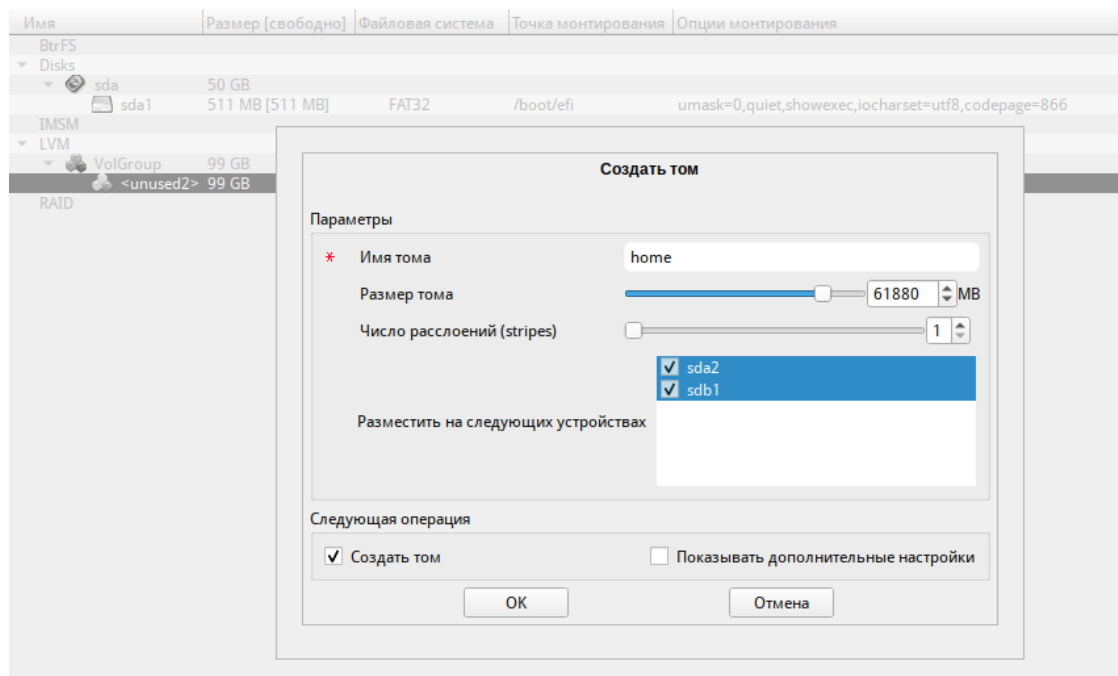


Рис. 22 – Установка. Подготовка диска. Создание тома

5.4.4.4.3. Создание шифруемых разделов

Программа установки ОС Альт СП позволяет создавать шифруемые разделы с использованием встроенных средств маскирования.

Для создания шифруемого раздела и выполнения дальнейшей разметки нужно выбрать требуемый диск и нажать на кнопку «Создать шифруемый раздел».

В открывшемся окне доступны следующие настройки (рис. 23):

- «Размер» – общий размер шифруемого тома;
- «Смещение» – настройка осуществляется с помощью ползунка либо путем ввода значения с клавиатуры (в поле нужно указать смещение начала данных на диске в Мбайт);
- «Основной раздел» – нужно отметить пункт, если раздел является основным для установки ОС;
- «Тип раздела» – в выпадающем поле нужно выбрать значение «Linux»;
- «Создать шифруемый том» – отметить пункт для автоматического перехода к настройке файловой системы на данном разделе;
- «Показывать дополнительные настройки» – отметить пункт для отображения дополнительных настроек при последующей работе с разделом.

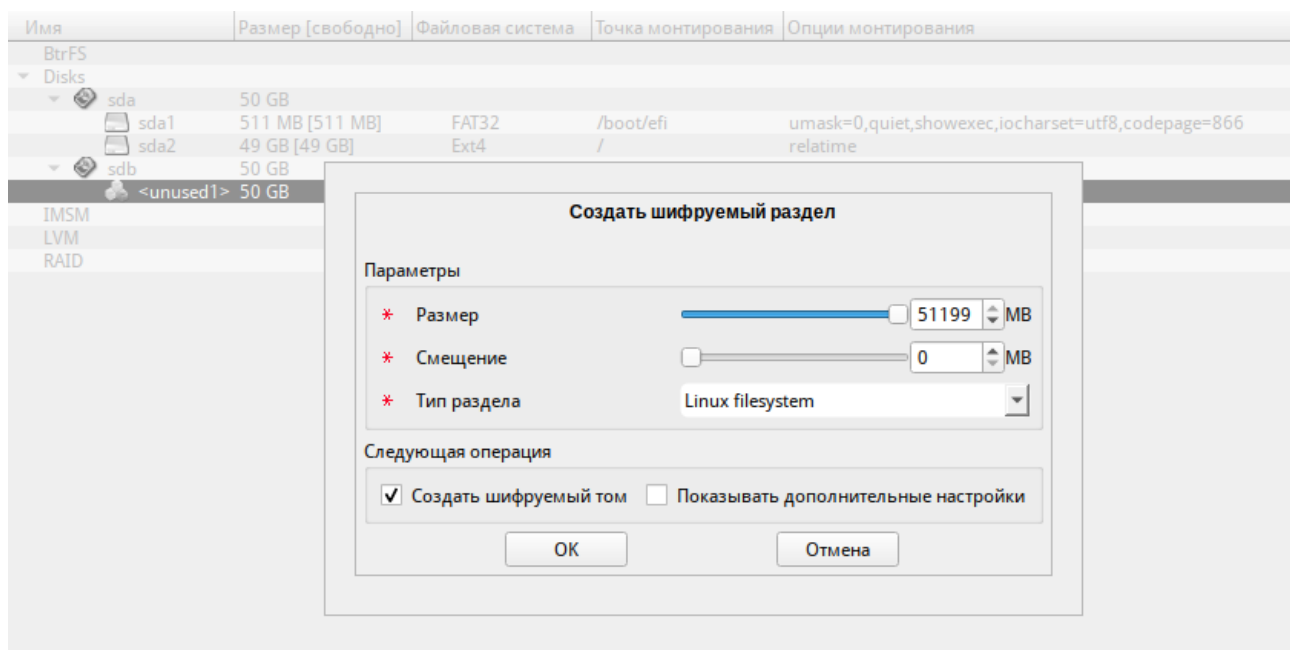


Рис. 23 – Установка. Создание кодируемого раздела

После создания шифруемого раздела мастер, как и при создании обычного раздела, предложит создать на нем файловую систему и при необходимости потребует указать точку монтирования.

⚠ Установка загрузчика на шифруемый раздел не поддерживается.

5.4.4.4. Создание подтомов Btrfs

Btrfs – файловая система, которая может работать с очень большими файлами, имеется поддержка снимков файловой системы (снапшотов), сжатие и подтома.

Подтом (subvolume) не является блочным устройством, но в каждом томе Btrfs создается один подтом верхнего уровня (subvolid=5), в этом подтоме могут создаваться другие подтома и снапшоты. Подтома (подразделы, subvolumes) создаются ниже вершины дерева Btrfs по мере необходимости, например, для / и /home создаются подтома с именами @ и @home. Для монтирования подтомов нужны определенные параметры вместо корня системы Btrfs по умолчанию:

- подтом @ монтируется в / с помощью опции `subvol=@`;
- подтом @home (если он используется) монтируется с помощью параметра монтирования `subvol=@home`.

В данном разделе рассмотрен вариант подготовки раздела Btrfs с разбивкой на подтома @ и @home.

Программа установки позволяет создать подтома (subvolume), указав разные точки монтирования.

Процесс подготовки к установке на подтома условно можно разбить на следующие шаги:

- создание разделов на жестких дисках;
- создание подтомов на разделах жесткого диска.

Для настройки параметров нового раздела нужно выбрать незамеченный диск в окне профиля разбивки пространства «Вручную» и нажать кнопку «Создать раздел».

При создании раздела на жестком диске следует указать «Тип раздела» равным «Linux filesystem» или «basic data» (рис. 24).

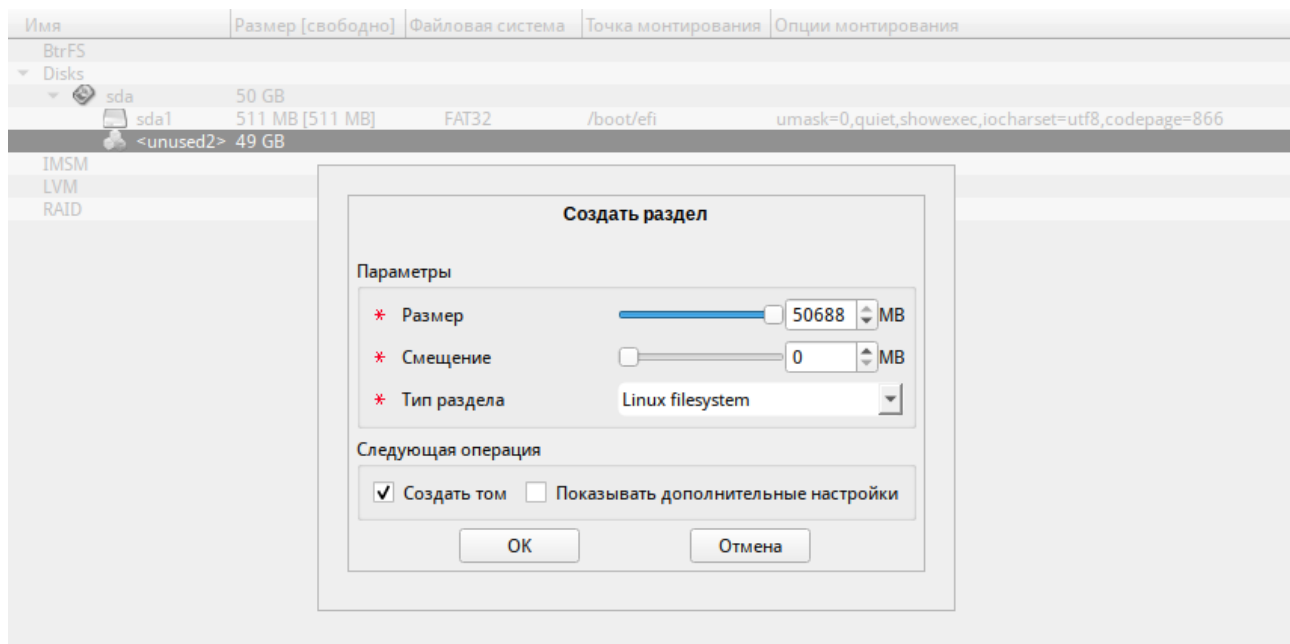


Рис. 24 – Создание раздела с ФС VtrFS в режиме UEFI

Примечание. В режиме Legacy при создании раздела на жестком диске следует указать «Тип раздела» равным «Linux» (рис. 25).

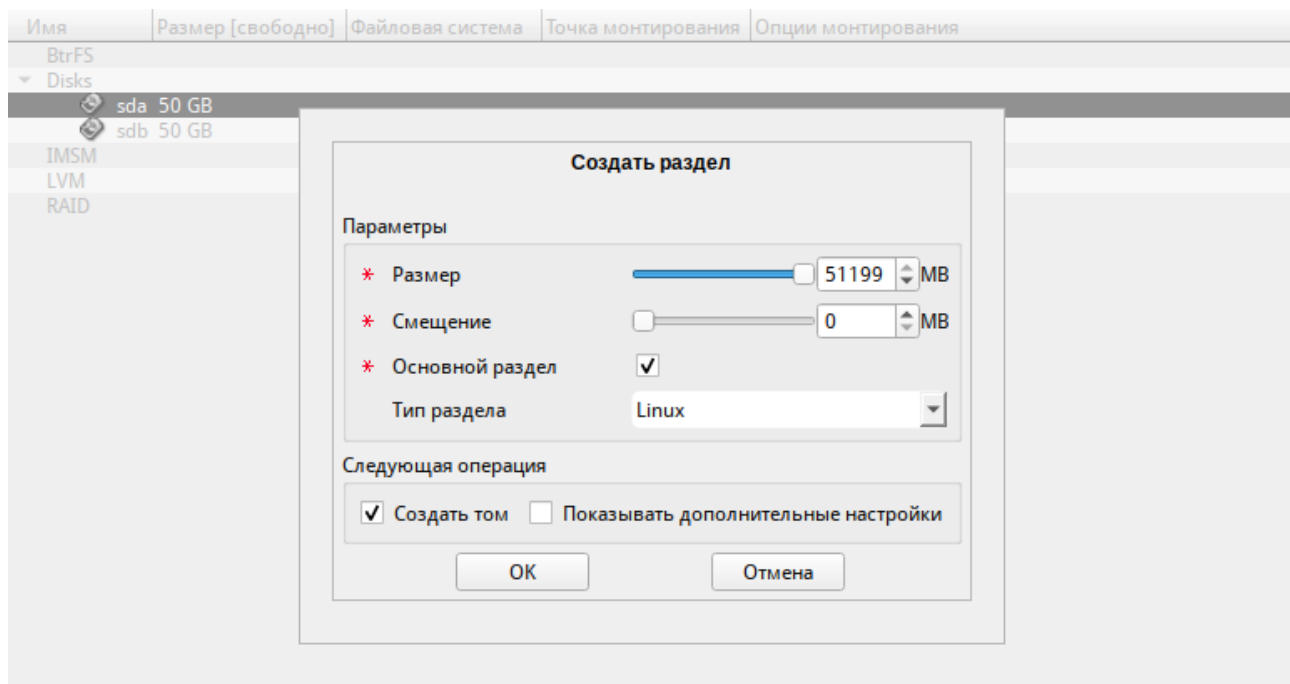


Рис. 25 – Создание раздела с ФС VtrFS в режиме Legacy

На следующем шаге выбрать файловую систему VtrFS (рис. 26).

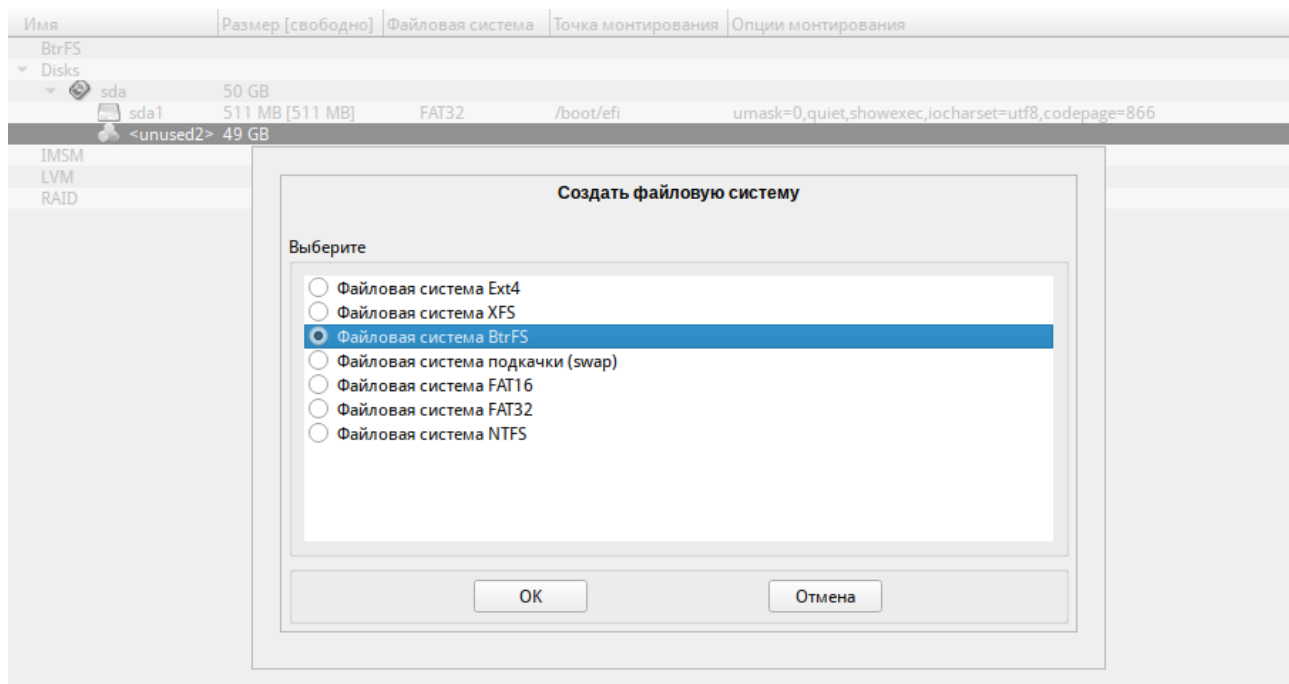


Рис. 26 – Создание раздела с ФС VtrFS

В окне «Изменить точку монтирования» (рис. 27) нажать кнопку «Отмена» (не указывать точку монтирования для раздела).

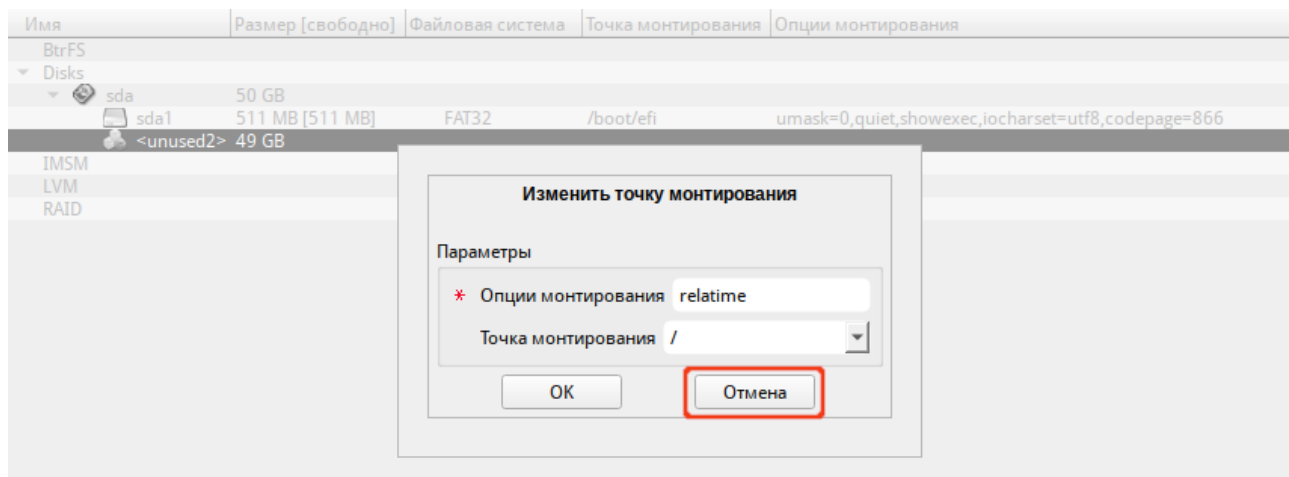


Рис. 27 – Окно «Изменить точку монтирования»

После создания раздела можно переходить к созданию подтомов. Для этого в списке следует выбрать раздел с файловой системой VtrFS, после чего нажать на кнопку «Создать подтом».

В открывшемся окне следует указать имя подтома или путь до него. На рис. 28 показано создание подтома @home. Данное действие следует повторить для создания подтома @.

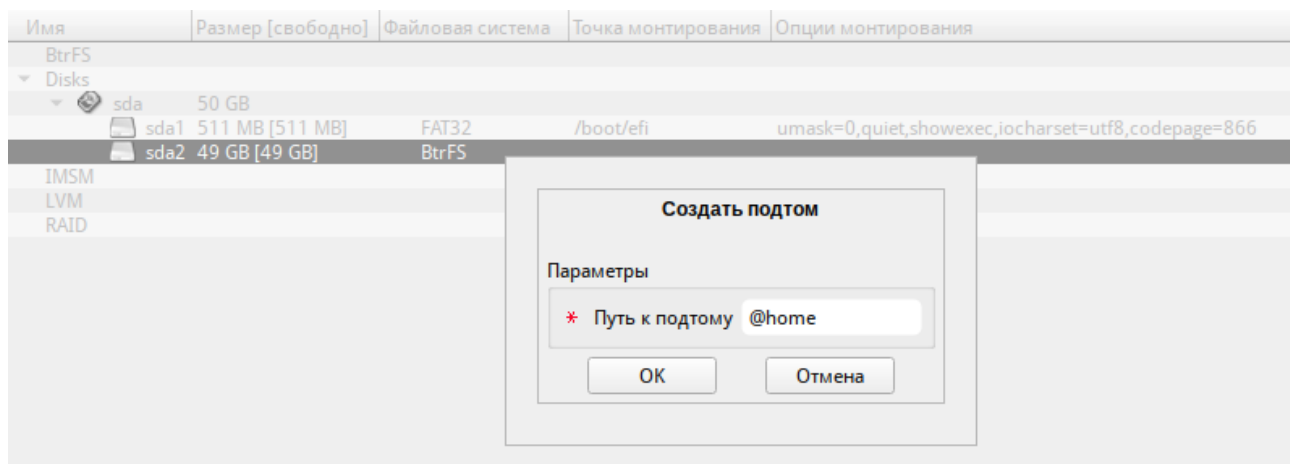


Рис. 28 – Создание подтома

После создания подтомов нужно указать точки монтирования для каждого тома. Для этого выбрать подтом и нажать кнопку «Изменить точку монтирования» (рис. 29).

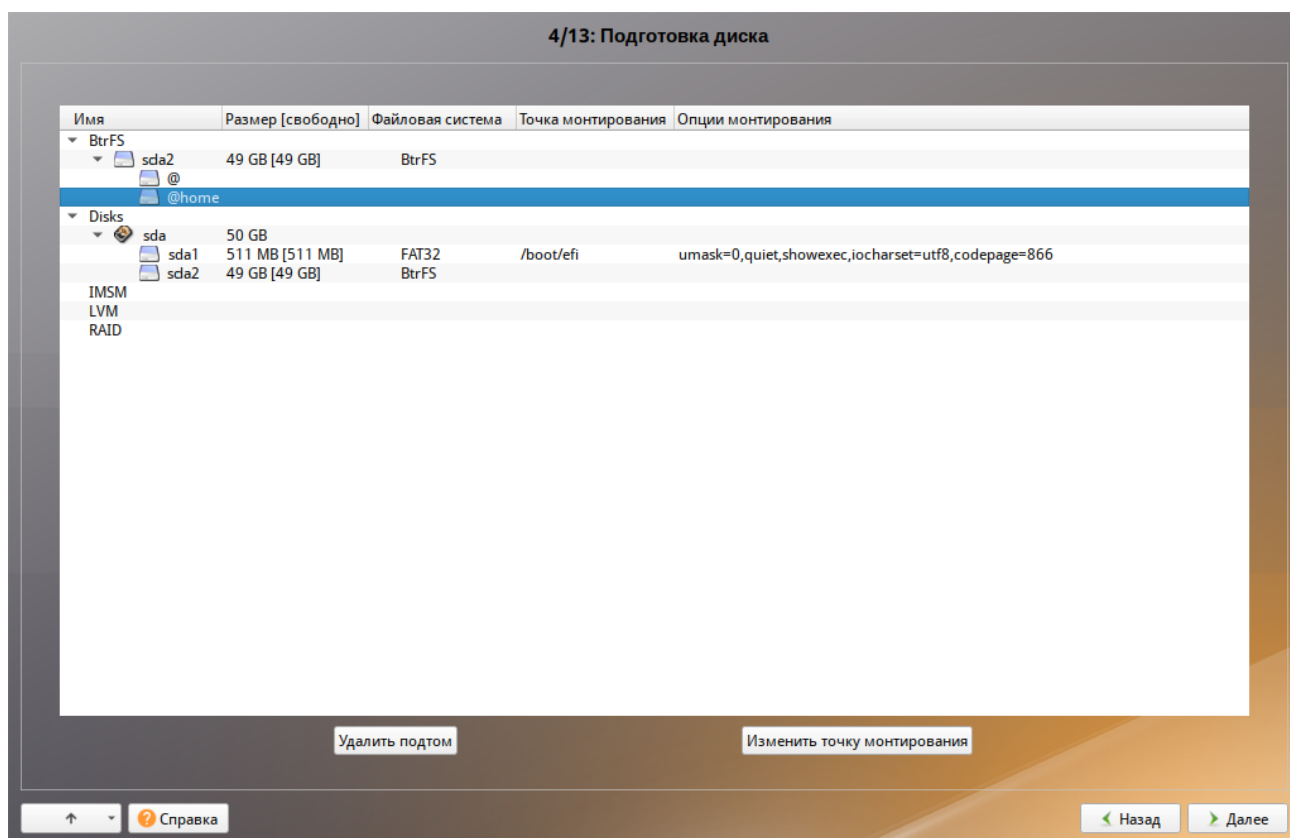


Рис. 29 – Созданные подтома

В открывшемся окне указать точку монтирования (рис. 30).

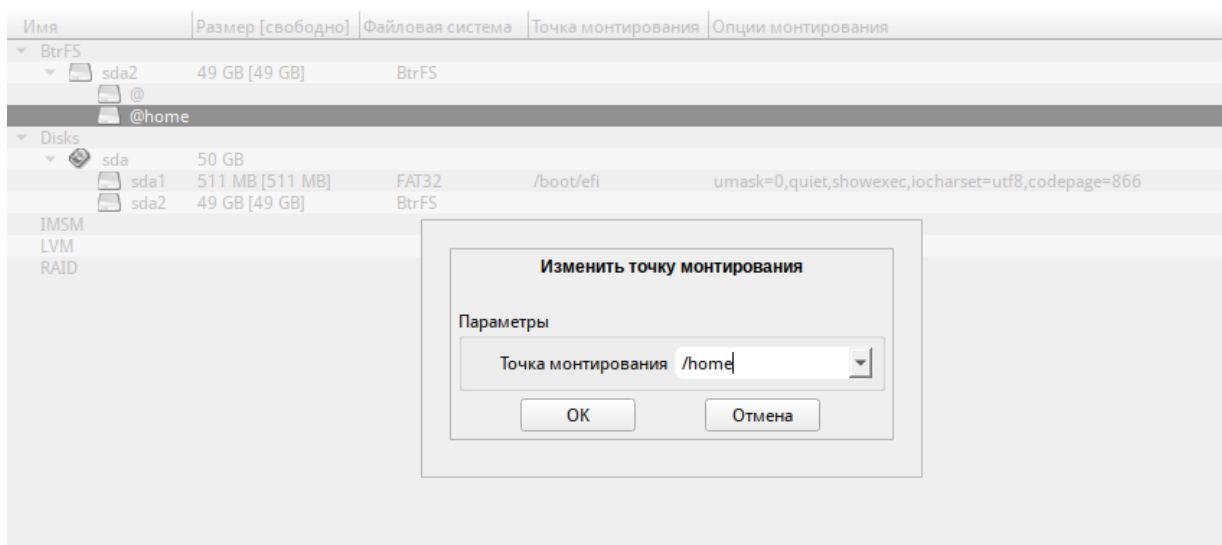


Рис. 30 – Точка монтирования для подтома @home

После указания точек монтирования для подтомов можно установить систему как обычно.

5.4.5. Перемонтирование

По завершении этапа подготовки диска начинается шаг перемонтирования. Он проходит автоматически и не требует вмешательства пользователя. На экране отображается индикатор выполнения (рис. 31).

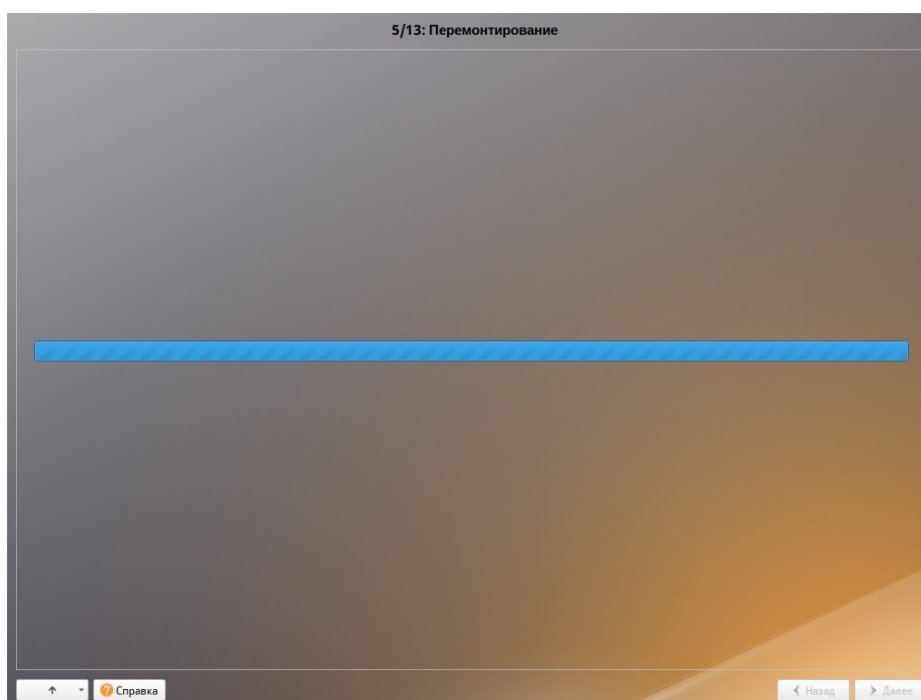


Рис. 31 – Перемонтирование

После сохранения настроек осуществляется автоматический переход к следующему шагу.

5.4.6. Установка системы

На данном этапе происходят распаковка ядра и установка набора программ, которые требуются для работы ОС Альт СП.

Программа установки предлагает выбрать дополнительные пакеты программ, которые будут включены в состав ОС Альт СП и установлены вместе с ней на диск (рис. 32, рис. 33).

Под списком групп на экране отображается информация об объеме дискового пространства, которое будет занято после установки пакетов, входящих в выбранные группы.

При выборе группы пакетов будет показан список программных пакетов, входящих в состав этой группы.

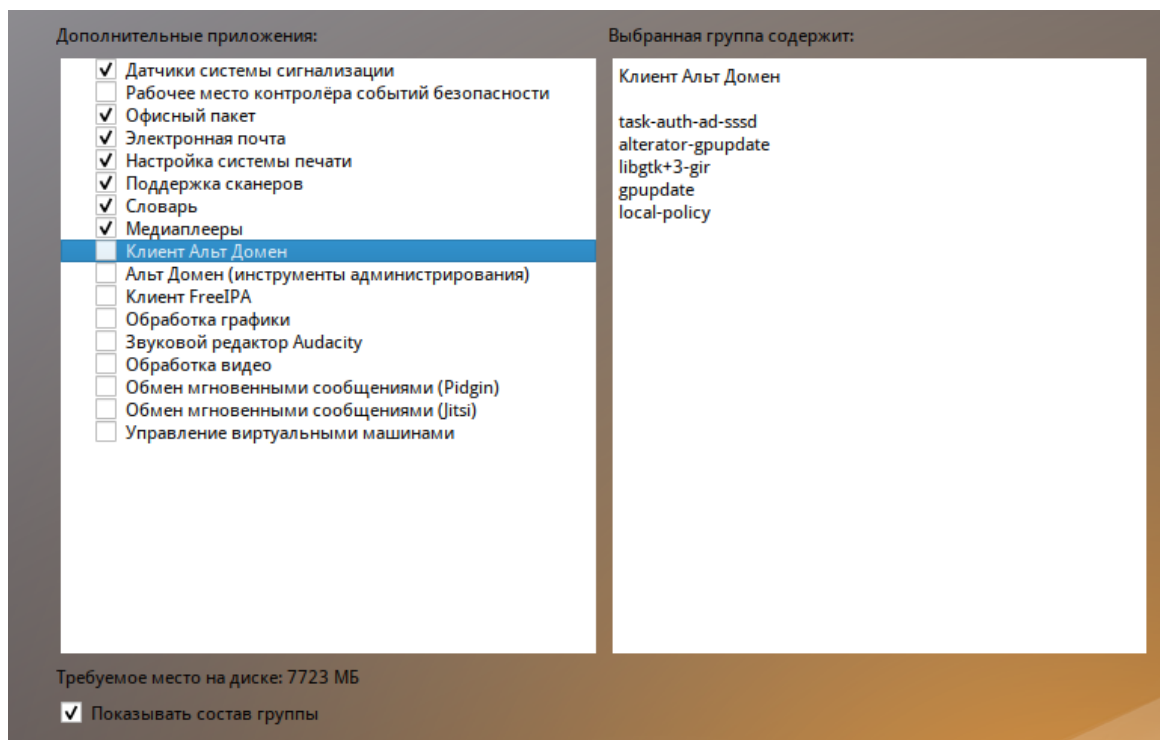


Рис. 32 – Установка рабочей станции. Выбор групп пакетов

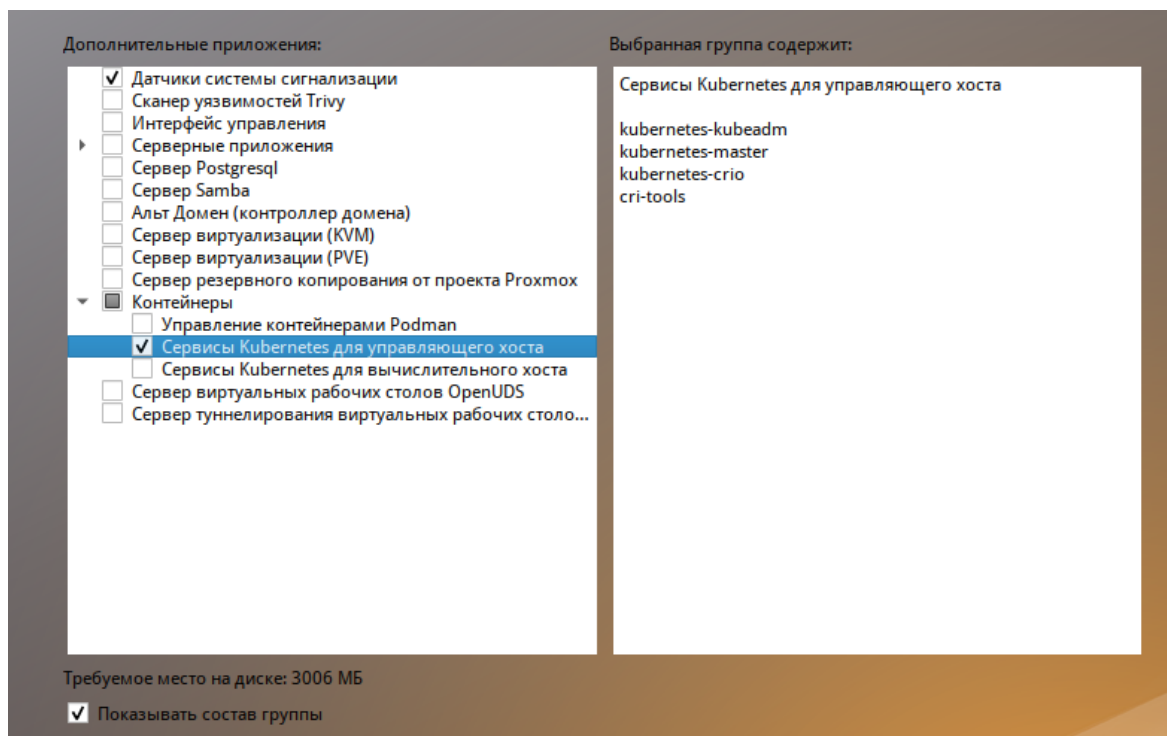


Рис. 33 – Установка сервера. Выбор групп пакетов

Выбрав группы пакетов, следует нажать «Далее», после чего начнется установка пакетов (рис. 34).



Рис. 34 – Установка. Установка пакетов

Установка пакетов происходит автоматически в два этапа:

- получение пакетов;
- установка пакетов.

Получение пакетов осуществляется с источника, выбранного на этапе начальной загрузки. При сетевой установке (по протоколу FTP или НТТР) время выполнения этого шага будет зависеть от скорости соединения.

5.4.7. Сохранение настроек

Начиная с данного этапа, программа установки работает с файлами только что установленной базовой системы. Все последующие изменения можно будет совершить после завершения установки посредством редактирования соответствующих конфигурационных файлов или при помощи модулей управления, включенных в дистрибутив.

После завершения установки базовой системы выполняется шаг сохранения настроек (рис. 35). Он проходит автоматически и не требует вмешательства пользователя, на экране отображается индикатор выполнения.

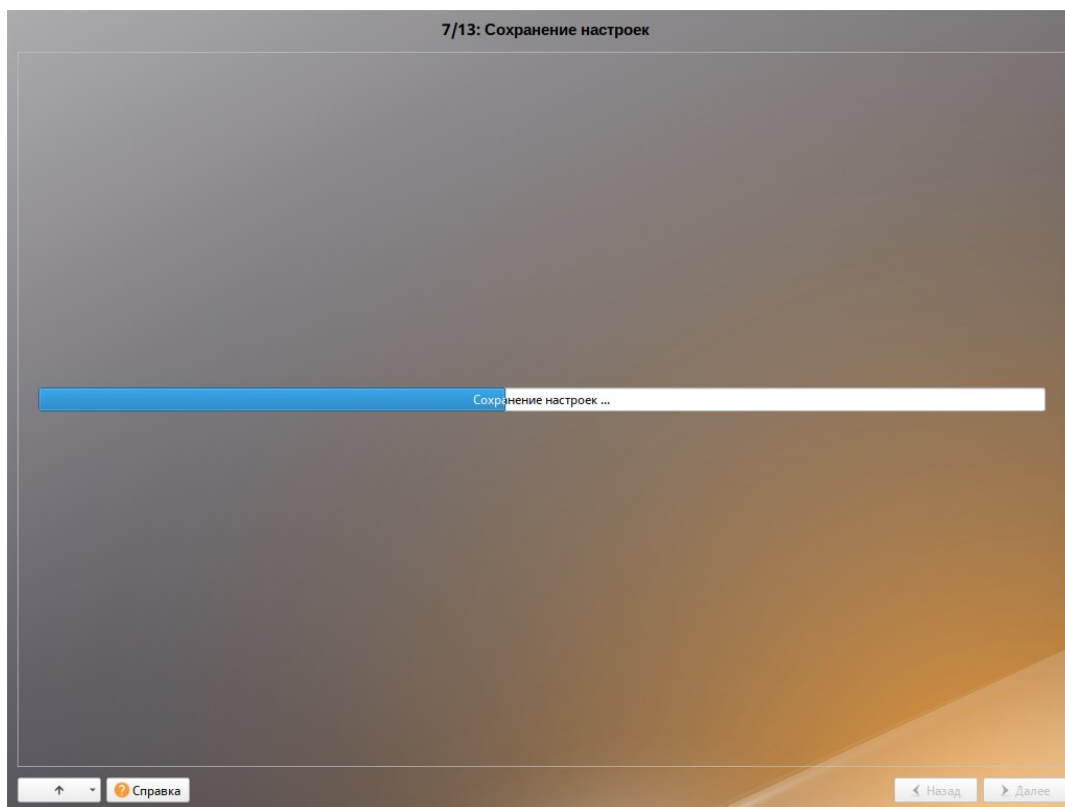


Рис. 35 – Установка. Сохранение настроек

На данном этапе производится перенос настроек, выполненных на первых шагах установки, в установленную базовую систему. Также производится запись информации о соответствии разделов жесткого диска смонтированным на них файловым системам (заполняется конфигурационный файл `/etc/fstab`).

В список доступных источников программных пакетов добавляется репозиторий, находящийся на установочном лазерном диске – выполняется команда `apt-cdrom add`, осуществляющая запись в конфигурационный файл `/etc/apt/sources.list`.

После сохранения настроек осуществляется автоматический переход к следующему шагу.

5.4.8. Установка загрузчика

Загрузчик ОС – программа, которая позволяет загружать ОС.

Программа установки автоматически определяет, в каком разделе НЖМД следует располагать загрузчик для возможности корректного запуска ОС. При установке на EFI модуль установки загрузчика предложит установить загрузчик в специальный раздел EFI (рис. 36).

Варианты установки загрузчика при установке в режиме EFI:

- «EFI (рекомендуемый)» – при установке загрузчика в NVRAM будет добавлена запись, без которой большинство компьютеров не смогут загрузиться во вновь установленную ОС;
- «EFI (сначала очистить NVRAM)» – перед добавлением записи в NVRAM ее содержимое будет сохранено в `/root/.install-log`, после чего из нее будут удалены все загрузочные записи, что приведет к восстановлению полностью заполненной NVRAM и гарантирует загрузку вновь установленной ОС;
- «EFI (запретить запись в NVRAM)» – этот вариант следует выбрать, только если инсталлятор не может создать запись в NVRAM или если заведомо известно, что запись в NVRAM может вывести компьютер из строя (вероятно, запись в NVRAM придется создать после установки ОС средствами BIOS Setup);

- «EFI (для съёмных устройств)» – этот вариант следует выбрать, только если ОС устанавливается на съёмный накопитель. Этот вариант также можно использовать вместо варианта EFI (запретить запись в NVRAM) при условии, что это будет единственная ОС на данном накопителе. Создавать запись в NVRAM не потребуется.

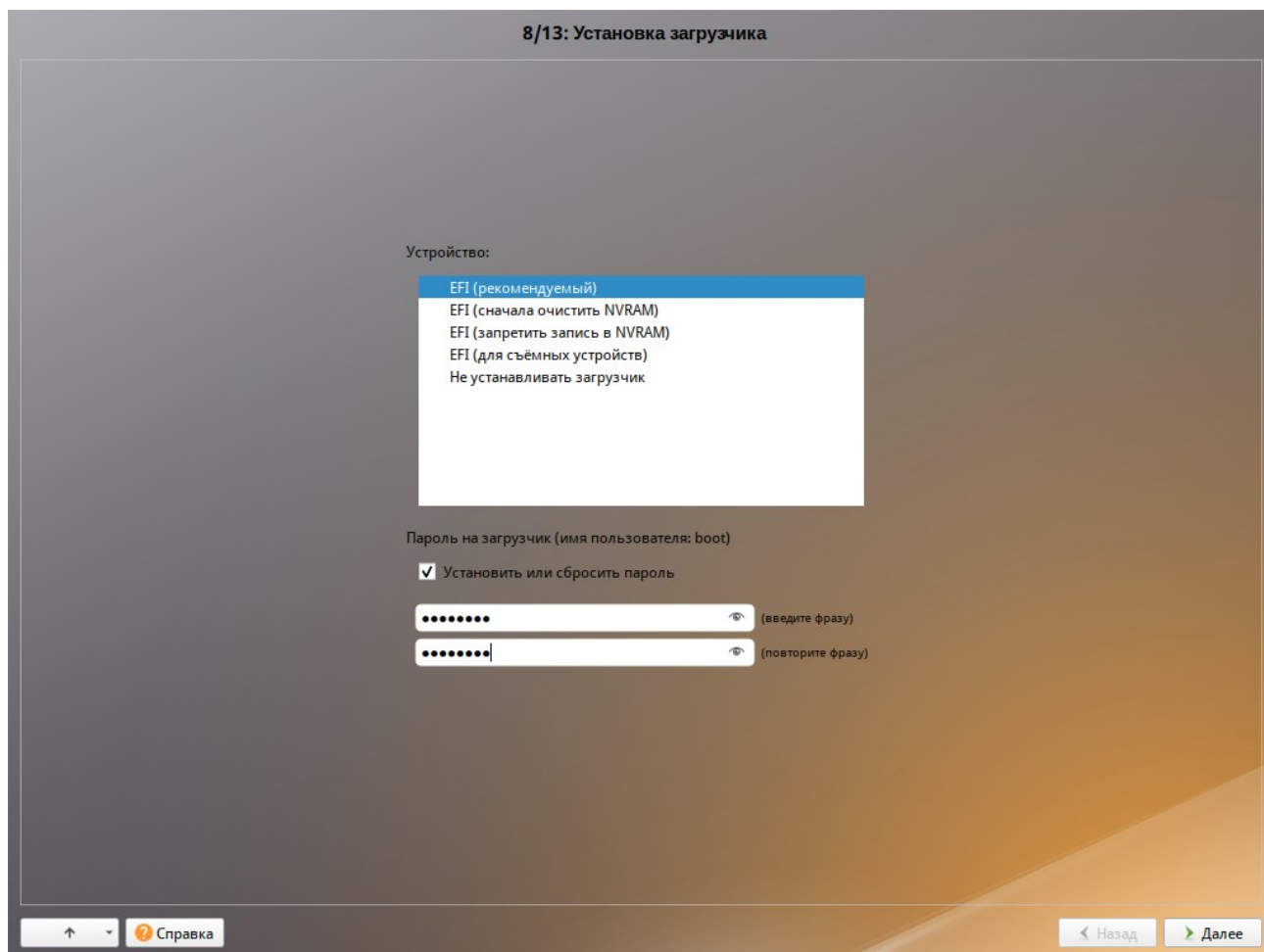


Рис. 36 – Установка. Установка загрузчика в режиме EFI

Примечание. Установка загрузчика при установке в режиме Legacy показана на рис. 37.

Положение загрузчика, в случае необходимости, можно изменить в выпадающем списке «Устройство», выбрав другой раздел.

Для ограничения доступа к опциям загрузки устанавливается пароль на загрузчик. Чтобы исключить опечатки при вводе пароля, пароль вводится дважды.

Примечание. При необходимости изменения опций загрузки при старте компьютера потребуется ввести имя пользователя «boot» и заданный на этом шаге пароль.

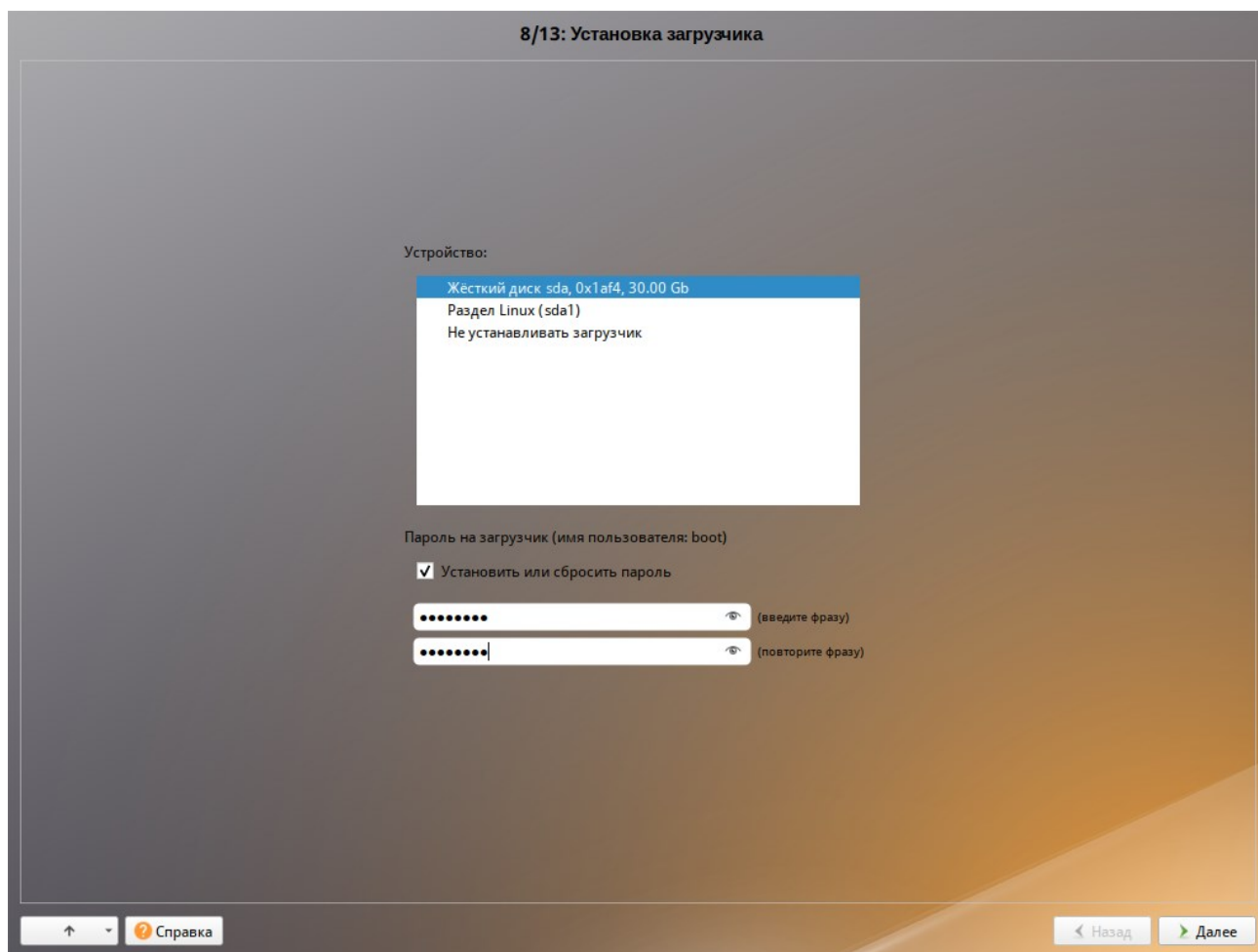


Рис. 37 – Установка загрузчика

ВАЖНО

При установке на EFI выберите в качестве устройства для установки «EFI». Рекомендуется выбрать автоматическое разбиение на этапе разметки диска для создания разделов для загрузки с EFI.

Для подтверждения выбора и продолжения работы программы установки нужно нажать на кнопку «Далее».

5.4.9. Настройка сети

На этом этапе в окне «Настройка сети» нужно задать параметры работы сетевой карты и настройки сети (рис. 38):

- «Имя компьютера» – сетевое имя компьютера (это общий сетевой параметр, не привязанный к какому-либо конкретному интерфейсу);
- «Интерфейсы» – список доступных сетевых интерфейсов;
- «Версия протокола IP» – версия используемого протокола IP (IPv4, IPv6);
- «Конфигурация» – способ назначения IP-адресов (службы DHCP, Zeroconf либо вручную);
- «IP-адреса» – пул назначенных IP-адресов из поля «Добавить ↑ IP», выбранные адреса можно удалить нажатием кнопки «Удалить»;
- «Добавить ↑ IP» – позволяет ввести IP-адрес вручную и выбрать в выпадающем поле предпочтительную маску сети. Для переноса адреса в пул поля «IP-адреса» необходимо нажать кнопку «Добавить»;
- «Шлюз по умолчанию» – адрес шлюза, который будет использоваться сетью по умолчанию;
- «DNS-серверы» – список предпочтительных DNS-серверов, которые будут получать информацию о доменах, выполнять маршрутизацию почты и управлять обслуживающими узлами для протоколов в домене;
- «Домены поиска» – список предпочтительных доменов, по которым будет выполняться поиск.

Конкретные значения будут зависеть от используемого сетевого окружения. Ручного введения настроек можно избежать, если в сети уже есть настроенный DHCP-сервер. В этом случае все нужные сетевые настройки будут получены автоматически.

В окне (рис. 39), открываемом при нажатии кнопки «Дополнительно», можно выбрать сетевую подсистему (NetworkManager, Etcnet) для интерфейса, а также указать должен ли запускаться данный интерфейс при загрузке системы.

Для сохранения настроек сети и продолжения работы программы установки нужно нажать на кнопку «Далее».

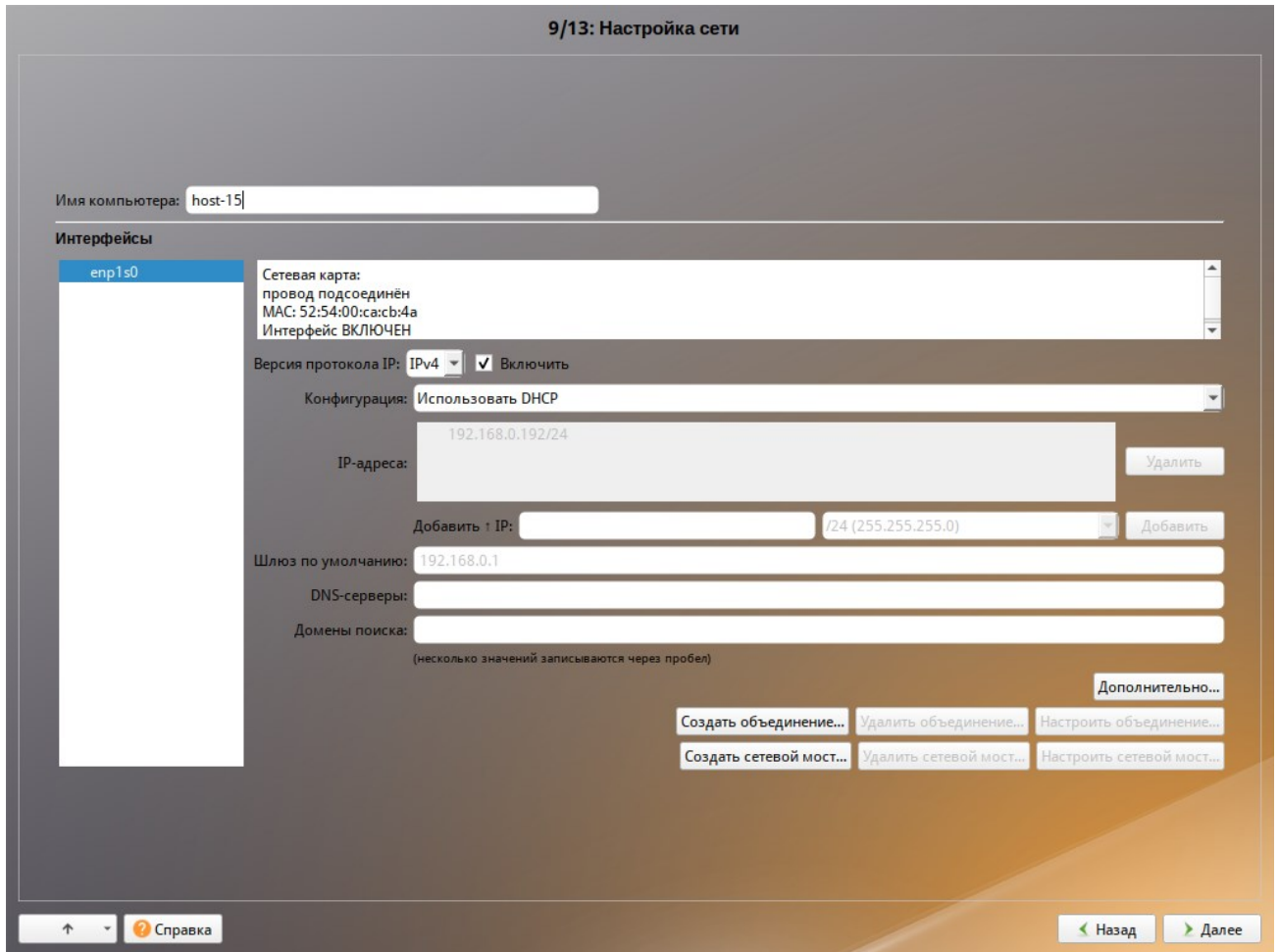


Рис. 38 – Установка. Настройка сети

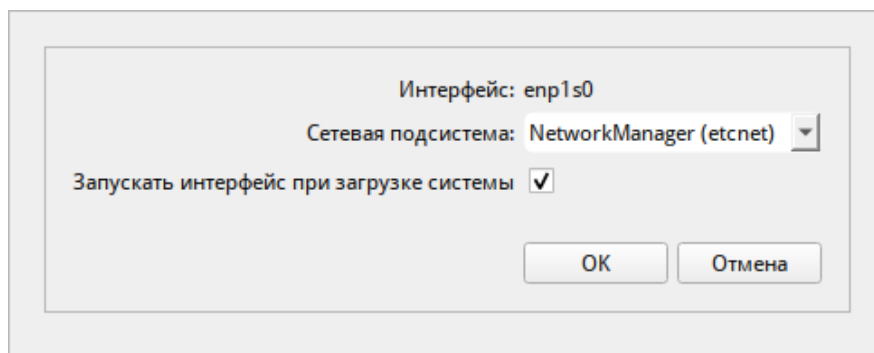


Рис. 39 – Установка. Настройка сетевой подсистемы

5.4.10. Администратор системы

На данном этапе загрузчик создает учетную запись администратора (рис. 40). В открывшемся окне нужно ввести пароль учетной записи администратора (root). Чтобы исключить опечатки при вводе пароля, пароль учетной записи вводится дважды.

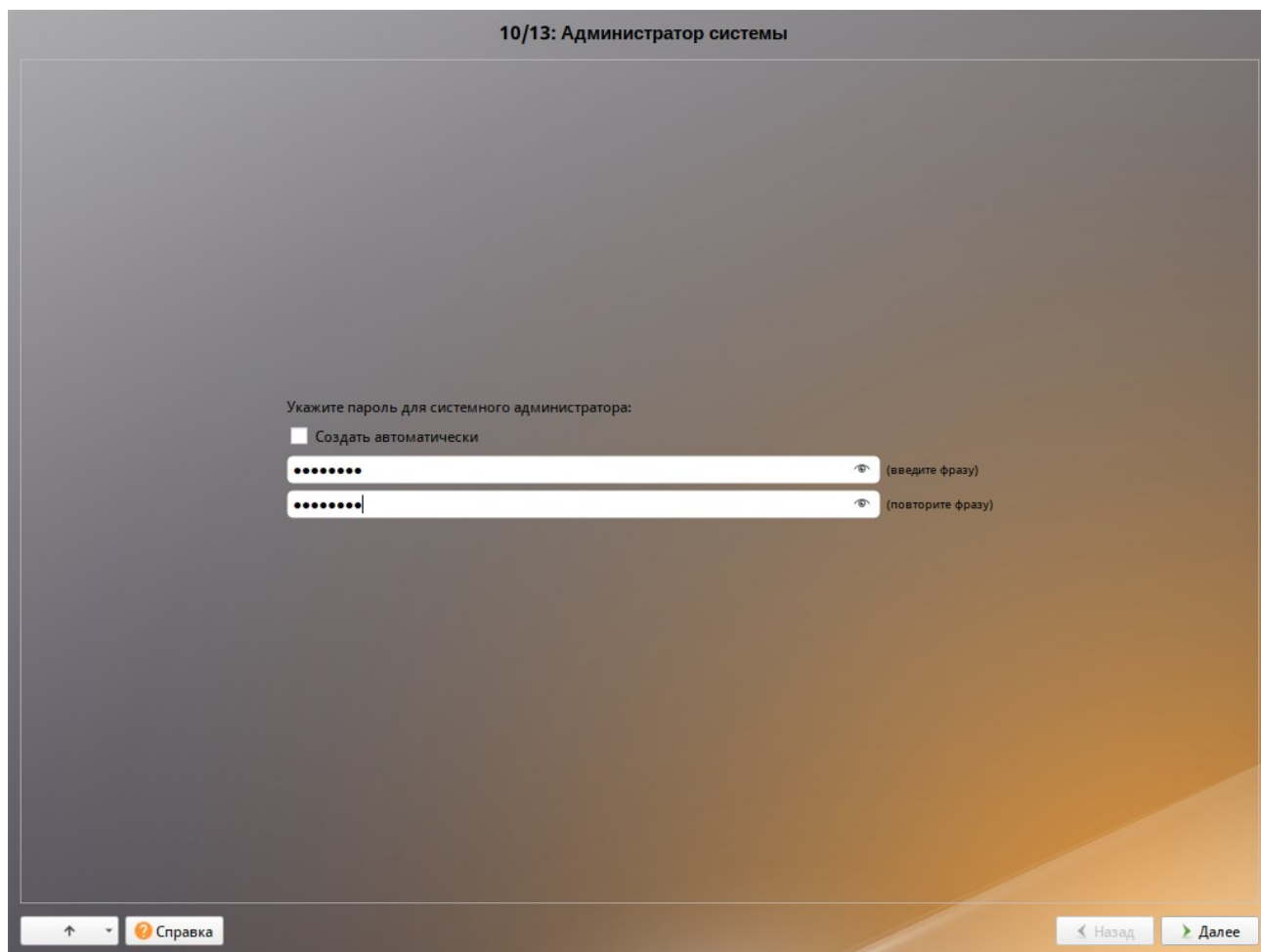


Рис. 40 – Установка. Задание пароля администратора

Для автоматической генерации пароля нужно отметить пункт «Создать автоматически». Система предложит пароль, сгенерированный автоматическим образом в соответствии с требованиями по стойкости паролей.

В любой системе Linux всегда присутствует один специальный пользователь-администратор системы, он же суперпользователь. Для него зарезервировано стандартное системное имя – root.

Администратор системы отличается от всех прочих пользователей тем, что ему позволено производить любые, в том числе критичные изменения в системе. Поэтому выбор пароля администратора системы – очень важный момент для безопасности. Любой, кто сможет ввести его правильно (узнать или подобрать), получит неограниченный доступ к системе. Даже собственные неосторожные действия от имени root могут иметь катастрофические последствия для всей системы.

ВАЖНО

Запомните пароль root – его нужно будет вводить для получения права изменять настройки системы с помощью стандартных средств настройки ОС. Более подробную информацию о режиме суперпользователя см. в п. 21.2.

Подтверждение введенного (или сгенерированного) пароля учетной записи администратора (root) и продолжение работы программы установки выполняется нажатием кнопки «Далее».

5.4.11. Системный пользователь

На данном этапе программа установки создает учетную запись системного пользователя (пользователя) ОС Альт СП.

Помимо администратора (root) в систему нужно добавить, по меньшей мере, одного обычного системного пользователя. Работа от имени администратора системы считается опасной, поэтому повседневную работу в Linux следует выполнять от имени ограниченного в полномочиях системного пользователя.

При добавлении системного пользователя предлагается в окне «Системный пользователь» заполнить следующие поля (рис. 41):

- «Имя» – имя учетной записи пользователя ОС Альт СП (слово, состоящее только из строчных латинских букв, цифр и символа подчеркивания «_», причем цифра и символ «_» не могут стоять в начале слова, есть также возможность использовать «-»). Начинаться имя должно со строчной латинской буквы);
- «Комментарий» – комментарий к имени учетной записи (обычно тут указывается реальные имя и фамилия пользователя);
- «Пароль» – пароль учетной записи пользователя (чтобы исключить опечатки при вводе пароля, пароль пользователя вводится дважды).

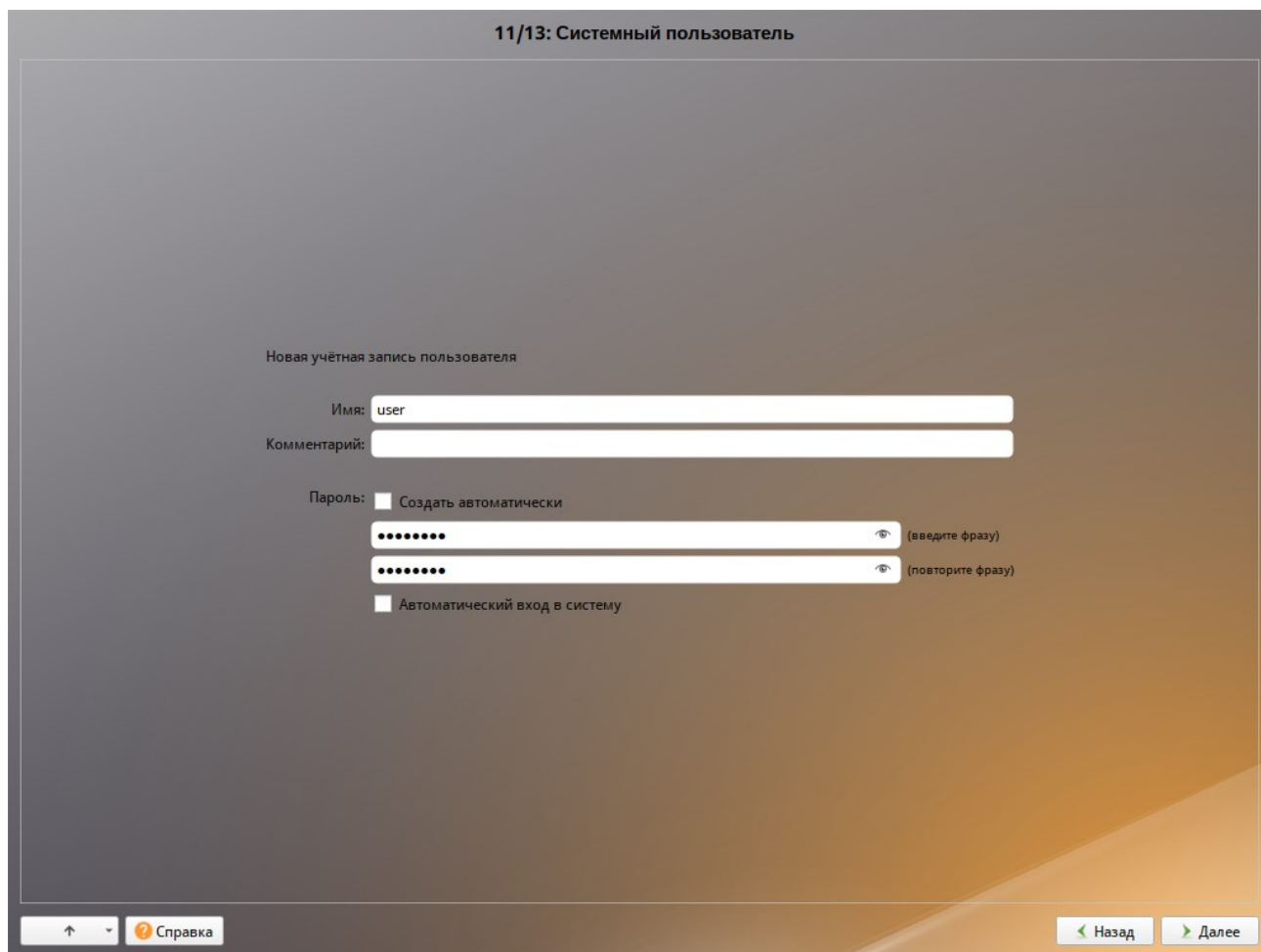


Рис. 41 – Установка. Создание пользователя

Для автоматической генерации пароля нужно отметить пункт «Создать автоматически». Система предложит пароль, сгенерированный автоматическим образом в соответствии с требованиями по стойкости паролей.

В процессе установки предлагается создать только одну учетную запись пользователя – чтобы от его имени администратор мог выполнять задачи, которые не требуют привилегий администратора (root). Учетные записи для всех прочих пользователей системы можно будет создать в любой момент после ее установки.

Подтверждение введенного (или сгенерированного) пароля учетной записи системного пользователя и продолжение работы программы установки выполняется нажатием кнопки «Далее».

5.4.12. Установка пароля на LUKS-разделы

Если на этапе подготовки диска был создан LUKS-раздел, на данном этапе нужно ввести пароль для обращения к этому разделу (рис. 42).

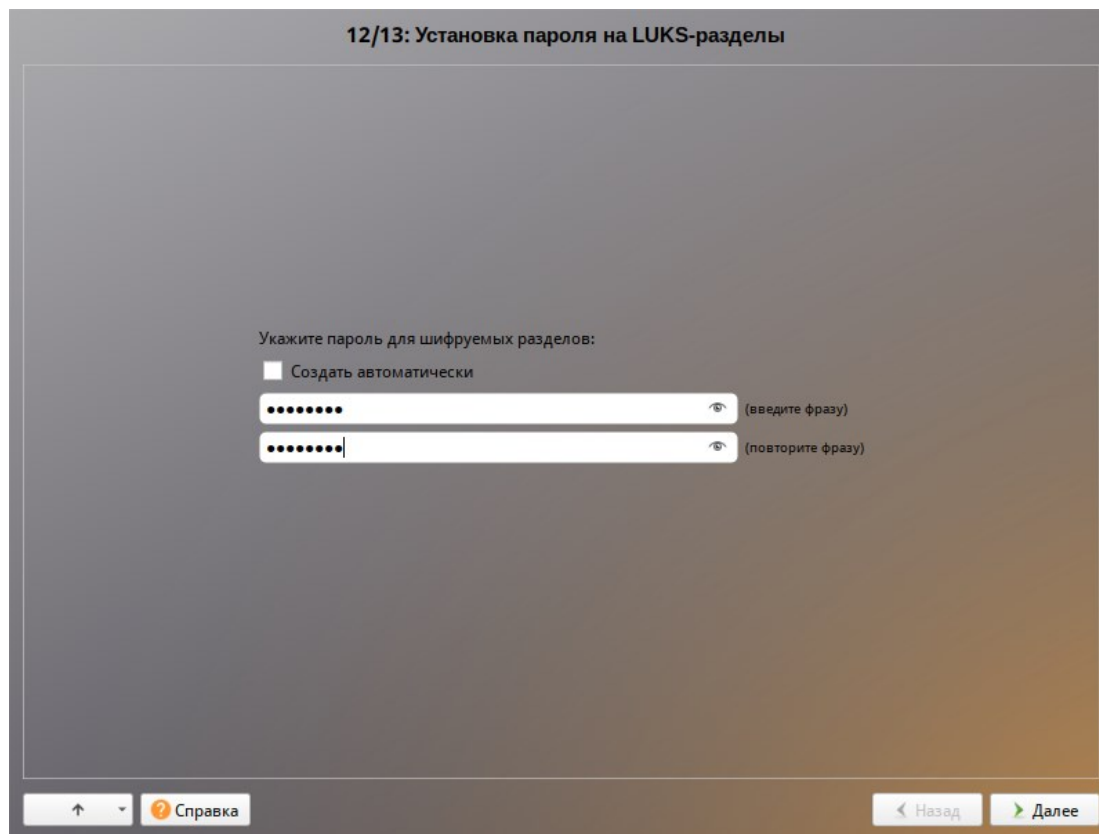


Рис. 42 – Установка пароля на LUKS-разделы

Установленный пароль потребуется вводить для получения доступа к информации на данных разделах. Например, если был зашифрован `/home`, то во время загрузки системы будет необходимо ввести пароль для этого раздела, иначе пользователь не сможет получить доступ в систему под своим именем.

Примечание. Если кодируемые разделы, не создавались, этот шаг пропускается автоматически.

LUKS надо устанавливать при разметке вручную, удаляя и пересоздавая каждый раздел. LUKS будет требовать пароля при загрузке для каждого раздела.

5.4.13. Завершение установки

На экране последнего этапа установки отображается информация о завершении установки ОС Альт СП (рис. 43).

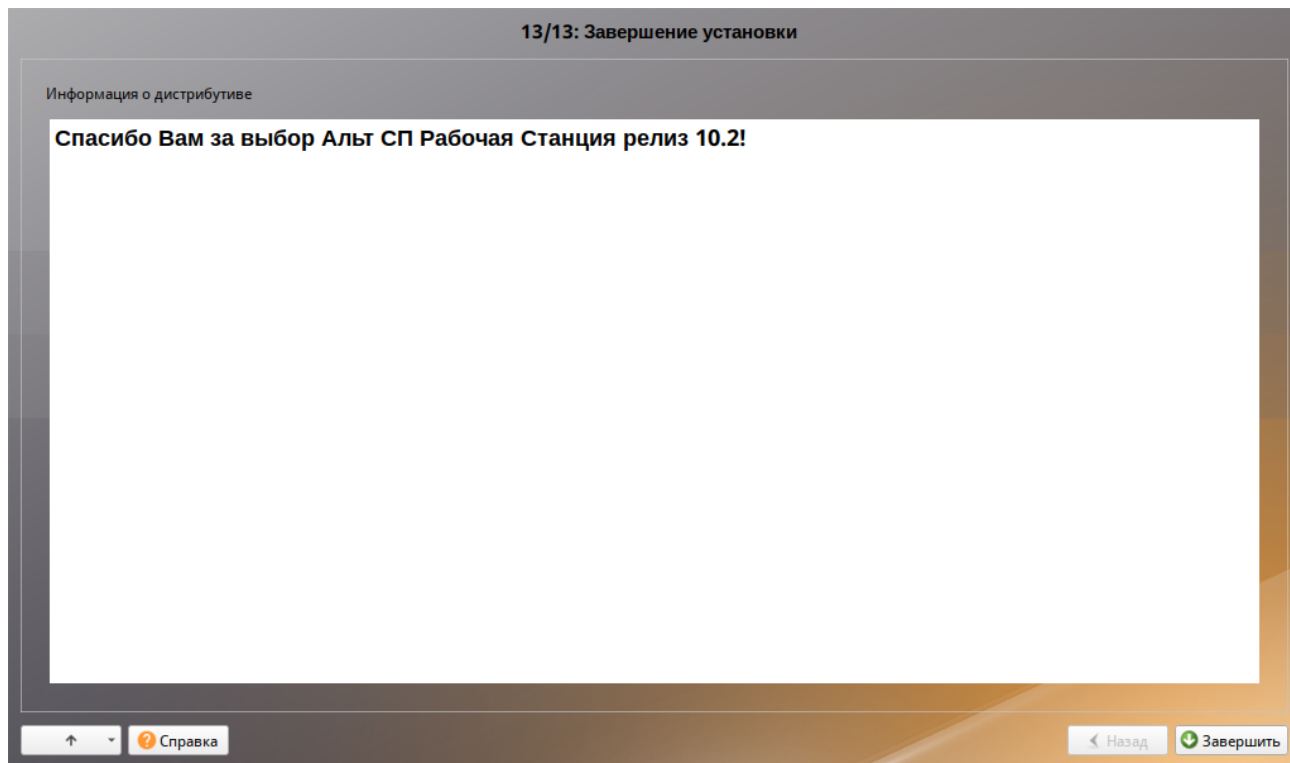


Рис. 43 – Установка. Завершение установки

После нажатия кнопки «Завершить» и перезагрузки компьютера выполняется штатная загрузка установленной ОС.

Не забудьте извлечь установочный компакт-диск (если это не происходит автоматически). Далее можно загружать установленную систему в обычном режиме.

5.5. Автоматическая установка системы (autoinstall)

Возможна установка ОС Альт СП в автоматическом режиме. Для этого нужно иметь установочный диск и доступный по сети (по протоколам HTTP или FTP) каталог с несколькими файлами. Настроить FTP-сервер можно, например, в ЦУС (подробнее см. п. 8.7.11).

5.5.1. Файлы автоустановки

Файлы автоустановки:

- `pkg-groups.tar` – архив, содержащий дополнительные к базовой системе группы пакетов;
- `vm-profile.scm` – различные варианты автоматической разбивки жесткого диска на языке Scheme;
- `autoinstall.scm` – сценарий автоматической установки на языке Scheme;
- `install-scripts.tar` – архив, содержащий дополнительные скрипты для `preinstall.d` и `postinstall.d` в одноименных каталогах. Скрипты должны быть исполняемыми. Скрипты из архива заменяют одноименные скрипты инсталлятора.

Файлы, описывающие процесс установки, нужно поместить в каталог, доступный по сети по протоколам HTTP или FTP (например, `metadata`).

5.5.2. Формат файла `vm-profile.scm`

Файл `vm-profile.scm` содержит сценарий, написанный на языке Scheme. Сценарий описывает формат автоматической разбивки жесткого диска.

Пример файла `vm-profile.scm` с одним профилем (`workstation`) разбивки жесткого диска:

```
((workstation
  (title . "Setup for workstation")
  (action . trivial)
  (actiondata ("swap" (size 2048000 . 2048000) (fsim . "SWAPFS") (methods plain))
              ("/" (size 40960000 . 40960000 ) (fsim . "Ext4") (methods plain))
              ("/home" (size 20480000 . #t ) (fsim . "Ext4") (methods plain))))
```

В примере указана разбивка:

- подкачка (`swap`) – 1024 Мбайт;
- корневой раздел (`/`) – 20 Гбайт;
- `/home` – все остальное, но не меньше 10 Гбайт.

Примечание. Все числа в файле `vm-profile.scm` указываются в виде 512-байтных блоков, поэтому чтобы получить размер в байтах, нужно умножить значения на 512.

Примечание. Добавление записи для `/boot/efi` не требуется – установщик добавит ее сам.

Пример файла `vm-profile.scm` с тремя профилями разбивки жесткого диска:

```
((workstation
  (title . "Setup for workstation")
  (action . trivial)
  (actiondata ("swap" (size 2048000 . 2048000) (fsim . "SWAPFS") (methods plain))
              ("/" (size 40960000 . 40960000 ) (fsim . "Ext4") (methods plain))
              ("/home" (size 20480000 . #t ) (fsim . "Ext4") (methods plain))))
(workstation_lvm
  (title . "Setup for workstation LVM")
  (action . trivial)
  (actiondata ("swap" (size 2048000 . 2048000) (fsim . "SWAPFS") (methods lvm))
              ("/" (size 16384000 . #t) (fsim . "Ext4") (methods lvm))))
(timeshift
  (title . "Timeshift-compatible setup")
  (action . trivial)
  (actiondata ("swap" (size 2048000 . 2048000) (fsim . "SWAPFS") (methods plain))
              ("@" (size 40632320 . #t) (fsim . "Btrfs") (methods plain) (subvols
"@home" . "/home")))))
)
```

В этом примере указаны профили:

- `workstation` – подкачка (`swar`), корневой раздел (`/`) и раздел `/home`;
- `workstation_lvm` – подкачка (`swar`) и корневой раздел в томе LVM;
- `timeshift` – подкачка (`swar`) и раздел Btrfs с разбивкой на подразделы `@` и `@home`.

Имя профиля указывается в файле `autoinstall.scm`, например:

```
("/evms/profiles/workstation_lvm" action apply commit #f clearall #t exclude ())
```

5.5.3. Формат файла `pkg-groups.tar`

Файл `pkg-groups.tar` представляет собой tar-архив с двумя подкаталогами:

- `groups` – содержит описание групп программного обеспечения в файлах `*.directory`;
- `lists` – содержит файлы со списками пакетов для каждой группы и скрытый файл `.base`, содержащий список пакетов «базовой системы» (то есть те пакеты, которые устанавливаются в любом случае).

Файл `pkg-groups.tar` проще всего взять из установочного ISO-образа из каталога `/Metadata/`. При необходимости файл можно доработать.

Для изменения списка пакетов:

- распаковать архив, например, выполнив команду:

```
$ tar xf pkg-groups.tar
```

- перейти в подкаталог `lists` и добавить файл группы. Имена пакетов указываются по одному в каждой строке, например:

```
admc
alterator-gpupdate
gpupdate
local-policy
admx-basealt
samba-dc-common
admx-firefox
admx-chromium
gpui
```

- упаковать архив, например, выполнив команду:

```
$ tar cf pkg-groups.tar lists
```

Имя файла используемой группы затем указывается через пробел в `autoinstall.scm`:

```
(("pkg-install") action "write" lists "group-1 group-2" auto #t)
```

где `group-1` и `group-2` – имена файлов со списками пакетов из подкаталога `lists`.

Примечание. В качестве источника пакетов при установке выступает сам диск, поэтому указание пакетов, которых нет на диске, приведет к сбою установки.

5.5.4. Формат файла `autoinstall.scm`

Файл `autoinstall.scm` представляет собой командный скрипт для программы установки, написанный с использованием языка программирования Scheme. Каждая строка скрипта – команда для модуля программы установки.

Пример файла `autoinstall.scm`:

```
; установка языка операционной системы (ru_RU)
("/sysconfig-base/language" action "write" lang ("ru_RU"))
; установка переключателя раскладки клавиатуры на Ctrl+Shift
("/sysconfig-base/kbd" language ("ru_RU") action "write" layout "ctrl_shift_toggle")
; установка часового пояса в Europe/Moscow, время в BIOS будет храниться в UTC
("/datetime-installer" action "write" commit #t name "RU" zone "Europe/Moscow" utc #t)
; автоматическая разбивка жесткого диска
("/evms/control" action "write" control open installer #t)
("/evms/control" action "write" control update)
("/evms/profiles/workstation" action apply commit #f clearall #t exclude ())
```

```

("/evms/control" action "write" control commit)
("/evms/control" action "write" control close)
; перемонтирование
("/remount-destination" action "write")
; установка пакетов операционной системы
("pkg-init" action "write")
; установка только базовой системы
; (дополнительные группы пакетов из pkg-groups.tar указываются по именам через пробел)
("/pkg-install" action "write" lists "" auto #t)
("/preinstall" action "write")
; установка загрузчика GRUB в efi с паролем '123'
("/grub" action "write" device "efi" passwd #t passwd_1 "123" passwd_2 "123")
; настройка сетевого интерфейса на получение адреса по DHCP
("/net-eth" action "write" reset #t)
("/net-eth" action "write" name "enp0s3" ipv "4" configuration "dhcp" default ""
search "" dns "" computer_name "newhost" ipv_enabled #t)
("/net-eth" action "write" commit #t)
; установка пароля суперпользователя root '123'
("/root/change_password" passwd_2 "123" passwd_1 "123")
; задание первого пользователя 'user' с паролем '123'
("/users/create_account" new_name "user" gecos "user" allow_su #t auto #f passwd_1
"123" passwd_2 "123" autologin #f)

```

В данном примере будет выполнена установка системы в минимальном профиле (дополнительное ПО в состав устанавливаемых пакетов включаться не будет). Если, например, нужно установить программы, указанные в файле `admc`, то нужно указать этот файл в списке устанавливаемых пакетов:

```
("/pkg-install" action "write" lists "admc" auto #t)
```

При установке системы в режиме EFI загрузчик устанавливается в специальный раздел `efi`. Если установка происходит в режиме Legacy, то загрузчик GRUB нужно установить на первый жесткий диск, например:

```
("/grub" action "write" device "/dev/sda" passwd #t passwd_1 "123"
passwd_2 "123")
```

Пример настройки сетевого интерфейса на статический IP-адрес:

```

("/net-eth" action "write" reset #t)
("/net-eth" action "write" name "enp0s3" ipv "4" configuration
"static" default "192.168.0.1" search "" dns "8.8.8.8" computer_name
"newhost" ipv_enabled #t)
("/net-eth" action "add_iface_address" name "enp0s3" addip
"192.168.0.25" addmask "24" ipv "4")
("/net-eth" action "write" commit #t)

```

где:

- 192.168.0.25 – IP-адрес;
- 192.168.0.1 – шлюз по умолчанию;
- 8.8.8.8 – DNS-сервер;
- newhost – имя хоста.

В конец файла `autoinstall.scm` можно добавить шаг `/postinstall`, который позволяет в конце установки или при первом запуске ОС выполнить команду или скрипт. Например:

```
("/postinstall/firsttime" script "ftp://192.168.0.123/metadata/update.sh")
```

У шага `/postinstall` есть два уровня запуска:

- `laststate` – скрипт запускается при завершении альтератора (перед перезагрузкой после установки);
- `firsttime` – скрипт запускается во время первого запуска ОС.

И два метода (`method`) указания скрипта запуска:

- `script` – скрипт загружается с сервера и выполняется;
- `run` – выполняется заданная команда или набор команд (возможно указание перенаправления).

Примеры:

```
("/postinstall/firsttime" script "http://server/script.sh")
("/postinstall/firsttime" run "curl --silent --insecure
http://server/finish")
```

```
("/postinstall/laststate" script "http://server/script.sh")
("/postinstall/laststate" run "curl --silent --insecure
http://server/gotoreboot") два метода (method)
```

Примечание. На уровне `laststate` для работы с установленной системой требуется указывать пути с `$destdir` или выполнять команды через `run_chroot`:

```
#!/bin/sh
```

```
a= . install2-init-functions
```

```
run_chroot sh -c "date > /root/STAMP_1"
date > $destdir/root/STAMP_2
```

5.5.5. Формат файла `install-scripts.tar`

Файл `install-scripts.tar` представляет собой `tar`-архив, содержащий дополнительные скрипты.

Скрипты `preinstall.d` выполняются сразу после установки базовой системы. Как правило, это скрипты для дополнительной настройки базовой системы (перед установкой дополнительного набора ПО) и для переноса настроек из среды

инсталлятора. Добавлять сюда свои собственные скрипты стоит только тогда, когда цели четко определены. Скрипты `postinstall.d` выполняются сразу после последнего шага инсталлятора. Как правило, это скрипты, удаляющие служебные пакеты инсталлятора из базовой системы. Если нужно сделать какие-нибудь специфические настройки системы, то это можно сделать здесь.

Скрипты `preinstall.d` нужно поместить в каталог `preinstall.d`, скрипты `postinstall.d` – в каталог `postinstall.d`. Упаковать архив можно, выполнив команду:

```
$ tar cf install-scripts.tar preinstall.d postinstall.d
```

Примечание. Данные скрипты выполняются в среде установщика, а не в среде установленной системы. Для работы с установленной системой требуется указывать пути с `$destdir` или выполнять команды через `run_chroot`:

```
#!/bin/sh
```

```
a= . install2-init-functions
```

```
run_chroot sh -c "date > /root/STAMP_1"  
date > $destdir/root/STAMP_2
```

5.5.6. Запуск автоматической установки

Для включения режима автоматической установки ядру инсталлятора ОС нужно передать параметр загрузки `ai` (без значения) и параметр `curl` с указанием каталога с установочными файлами. Формат адреса в `curl` должен быть представлен в виде URL. Пример параметров загрузки:

```
ai curl=ftp://<IP-адрес>/metadata/
```

Чтобы начать процесс автоматической установки ОС, нужно загрузиться с носителя, на котором записан дистрибутив. Затем клавишами перемещения курсора `<↑>`, `<↓>` выбрать пункт меню «Установить ALT SP Workstation 10.2» и нажать клавишу `<E>`. В открывшемся редакторе следует найти строку, начинающуюся с `linux /boot/vmlinuz`, в ее конец дописать требуемые параметры (рис. 44).

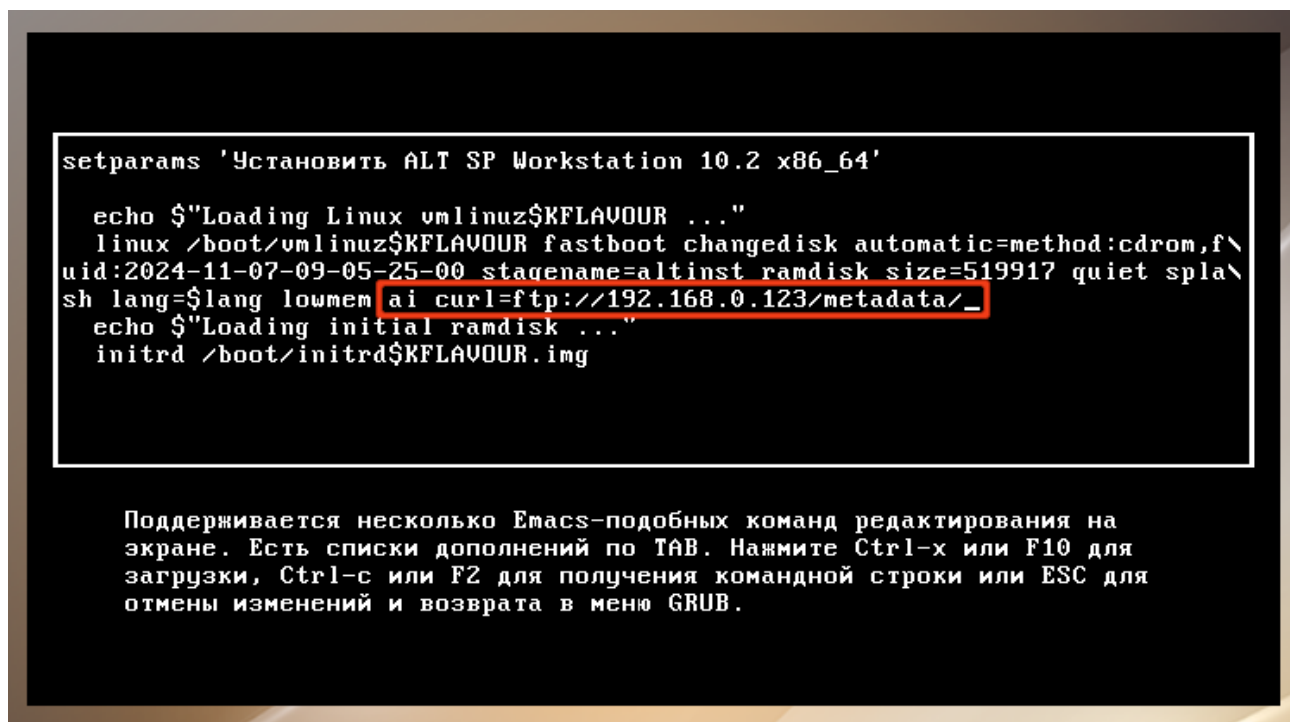


Рис. 44 – Включение режима автоматической установки

После нажатия клавиши <F10> начнется автоматическая установка системы.

При невозможности получения файлов из указанного источника по сети, программа установки будет смотреть в следующих местах:

- на диске в каталоге /Metadata/;
- в образе установщика в каталоге /usr/share/install2/metadata/.

5.6. Установка OEM-версии ОС Альт СП (рабочая станция)

Под установкой в режиме OEM понимается предварительная установка ОС Альт СП (рабочая станция) производителем или дистрибьютором на компьютеры, ноутбуки, планшеты и т. д. В этом режиме можно выполнить всю аппаратную настройку и выбрать пакеты программ, а пользователю будет предоставлена возможность сделать все персональные настройки (выбор имени пользователя, настройка языка и т. д.).

Для того чтобы выполнить OEM-установку, необходимо при установке дистрибутива передать ядру инсталлятора ОС параметр загрузки oem. Параметр oem включает стандартный режим установки OEM, при котором при установке

отсутствуют шаги: «Настройка сети», «Администратор системы», «Системный пользователь», а при первом запуске эти шаги присутствуют.

Ядру инсталлятора ОС можно также передать параметры `OEM_NET`, `OEM_ROOT`, `OEM_USER`, предназначенные для отключения/включения шагов «Настройка сети», «Администратор системы», «Системный пользователь» в инсталляторе и при первом запуске. Данные параметры могут принимать значения:

- «pre» – включить шаг только при установке;
- «post» (по умолчанию) – включить шаг только при первоначальной настройке;
- «pre-post» – включить шаг при установке и при первоначальной настройке;
- «no» – отключить шаг при установке и при первоначальной настройке.

Например, можно включить шаг «Администратор системы» при установке и при первоначальной настройке (рис. 45), чтобы иметь возможность донастроить систему после установки перед передачей компьютера конечному пользователю.

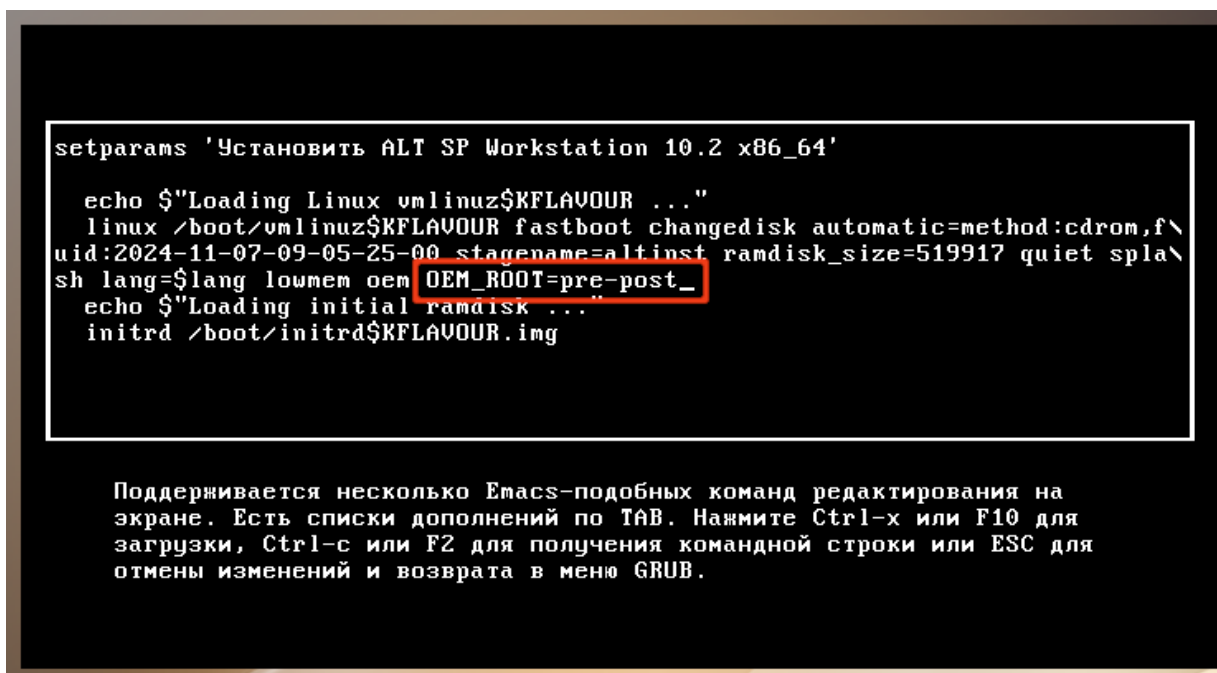


Рис. 45 – Включить шаг «Администратор системы» при установке и при первоначальной настройке

5.6.1. Установка в режиме OEM (предустановка)

Для начала процесса предустановки ОС Альт СП необходимо загрузиться с носителя, на котором записан дистрибутив. Затем клавишами перемещения курсора <↑>, <↓> выбрать пункт меню «Установить ALT SP Workstation 10.2» и нажать клавишу <E>. В открывшемся редакторе следует найти строку, начинающуюся с `linux /boot/vmlinuz`, в ее конец дописать параметр `oem` (рис. 46). После нажатия клавиши <F10> начнется установка OEM-версии системы.

ОЕМ-установка состоит из следующих шагов:

- выбор основного языка системы;
- лицензионное соглашение;
- выбор часового пояса, по которому будут установлены часы;
- подготовка диска;
- перемонтирование;
- установка системы;
- сохранение настроек;
- установка загрузчика;
- установка пароля на LUKS-разделы (если на этапе «Подготовка диска» был создан кодированный раздел);
- завершение установки.

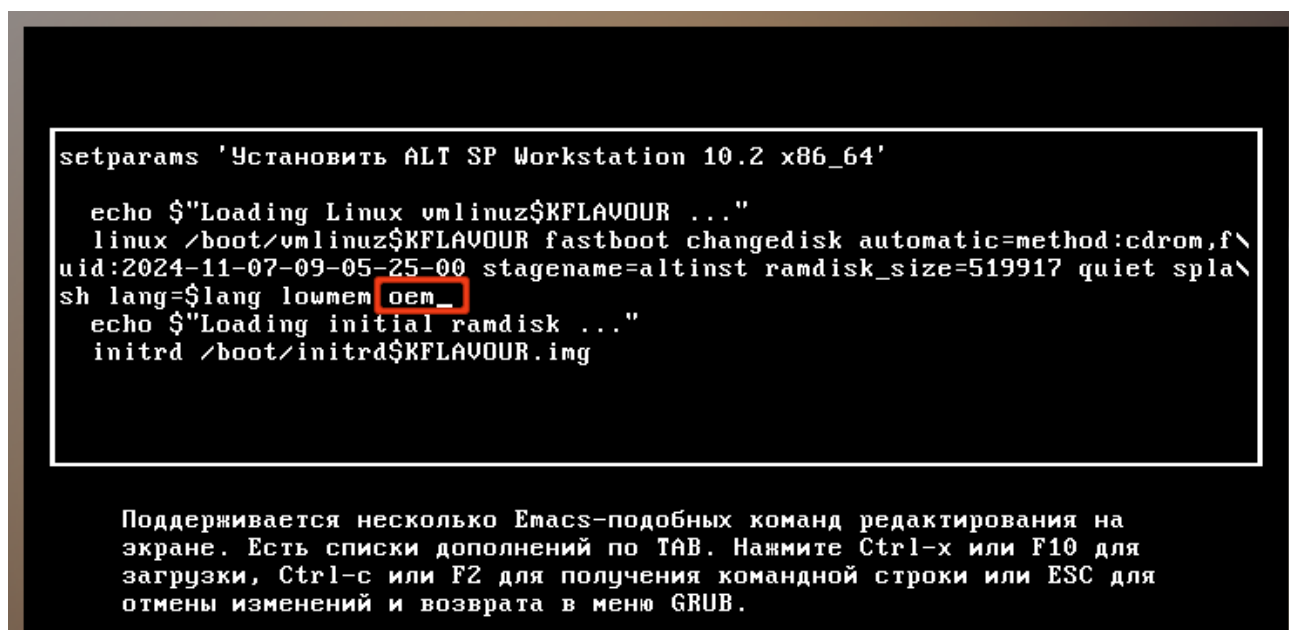


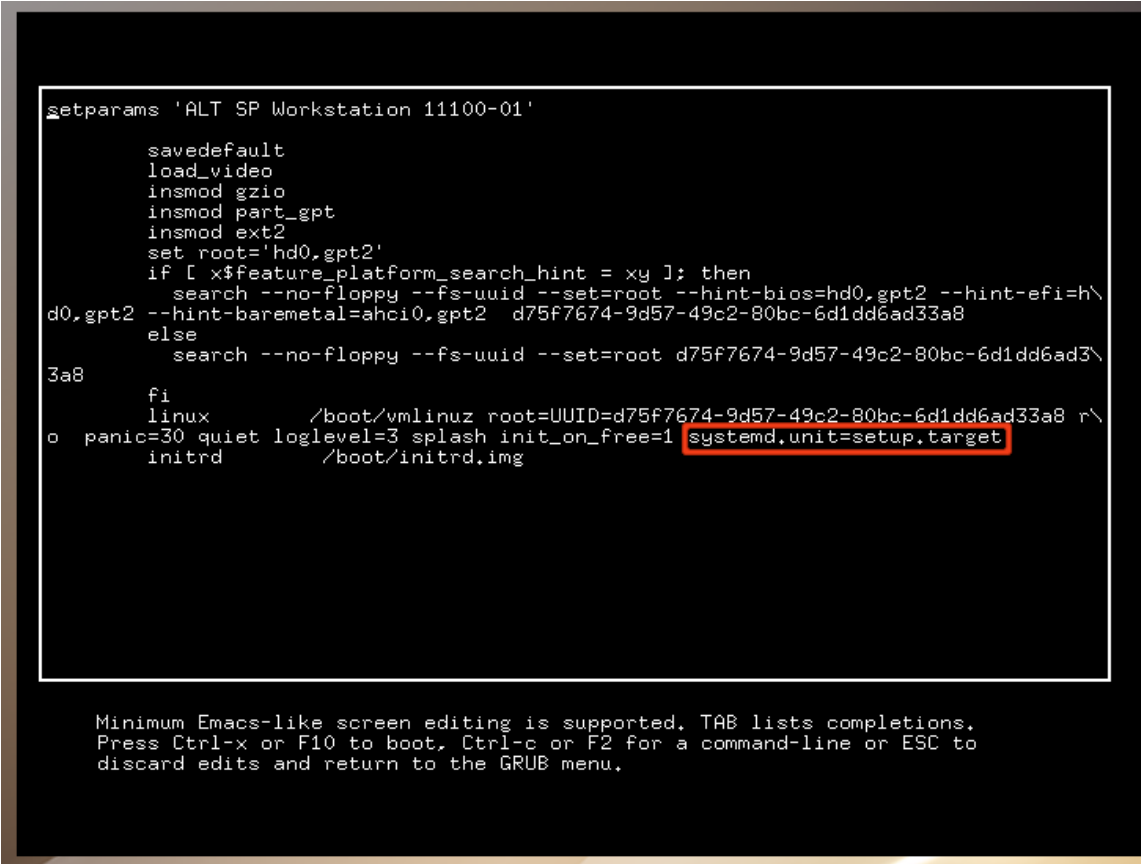
Рис. 46 – Включение режима OEM-установки

5.6.2. Режим загрузки OEM

После первой загрузки ОС пользователь попадет в мастер настройки системы, который состоит из следующих шагов:

- выбор основного языка системы;
- лицензионное соглашение;
- выбор часового пояса, по которому будут установлены часы;
- настройка параметров работы сетевой карты и настройки сети;
- установка пароля учетной записи администратора (root);
- создание учетной записи системного пользователя;
- завершение настройки.

Примечание. После установки в режиме OEM в параметрах загрузки будет прописан параметр `systemd.unit=setup.target` (рис. 47). Это специальная цель для `systemd`, которая запускает `alterator-setup`. Для того чтобы загрузиться один раз в обычном режиме, необходимо удалить этот параметр. После завершения работы `alterator-setup` пакеты, связанные с `alterator-setup`, будут удалены, а из параметров загрузки навсегда будет удален `systemd.unit=setup.target`.



```
setparams 'ALT SP Workstation 11100-01'

savedefault
load_video
insmod gzio
insmod part_gpt
insmod ext2
set root='hd0,gpt2'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-bios=hd0,gpt2 --hint-efi=h\
d0,gpt2 --hint-baremetal=ahci0,gpt2 d75f7674-9d57-49c2-80bc-6d1dd6ad33a8
else
  search --no-floppy --fs-uuid --set=root d75f7674-9d57-49c2-80bc-6d1dd6ad3\
3a8
fi
linux /boot/vmlinuz root=UUID=d75f7674-9d57-49c2-80bc-6d1dd6ad33a8 r\
o panic=30 quiet loglevel=3 splash init_on_free=1 systemd.unit=setup.target
initrd /boot/initrd.img

Minimum Emacs-like screen editing is supported. TAB lists completions.
Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a command-line or ESC to
discard edits and return to the GRUB menu.
```

Рис. 47 – Режим загрузки OEM. Параметры загрузки

5.7. Обновление системы до актуального состояния

После установки системы лучше сразу обновиться до актуального состояния. Можно не обновлять систему и сразу приступать к работе только в том случае, если не планируется подключение к сети или Интернету и нет необходимости устанавливать дополнительные программы.

Для обновления системы нужно выполнить команды (с правами администратора):

```
# apt-get update
# apt-get dist-upgrade
# update-kernel
# apt-get clean
# reboot
```

Примечание. Получить права администратора (см. также п. 21.2) можно, выполнив в терминале команду:

```
$ su -
```

или зарегистрировавшись в системе (например, на второй консоли – нажать клавиши <Ctrl>+<Alt>+<F2>) под именем root.

Подробнее про обновление пакетов можно прочитать в п. 18.8, п. 18.9 и п. 18.11 «Обновление ядра».

5.8. Установка графической оболочки на ОС Альт СП Сервер

Стандартная установка варианта исполнения ОС Альт СП Сервер включает базовую систему, работающую в консольном режиме. Для установки графической оболочки, и переключения в графический режим работы следует выполнить следующие команды:

```
# apt-get update
# apt-get install mate-default lightdm-gtk-greeter \
fonts-ttf-dejavu mate-screensaver-screenkeyboard gvfs \
theme-mate-windows icon-theme-Papirus
# sed -i 's/#keyboard=/keyboard=onboard --xid/' \
/etc/lightdm/lightdm-gtk-greeter.conf
# systemctl set-default graphical.target
# systemctl enable --now lightdm
# reboot
```

Примечание. Для установки указанных пакетов потребуется подключить репозиторий с компакт-диска дистрибутива ОС Альт СП Рабочая станция или репозиторий в интернете (<http://update.altsp.su>).

После выполнения установки будет выведено сообщение о нарушении целостности. Для восстановления целостности системы, если система контроля целостности IMA/EVM не инициализирована, выполнить команду:

```
# integalert fix
```

5.9. Проблемы при установке системы

Примечание. При возникновении проблем с UEFI или Legacy/CSM рекомендуется изменить выбор используемого вида прошивки на другой. Не следует выбирать режим смешанной загрузки Legacy/UEFI! Рекомендуется отключить всевозможные оптимизации и ускорение UEFI-загрузки, а также отключить на время установки SecureBoot.

Если в системе не произошла настройка какого-либо компонента после стадии установки пакетов, следует довести установку до конца, загрузить систему и попытаться в спокойной обстановке повторить настройку.

Нажатием клавиши <E> можно вызвать редактор параметров текущего пункта загрузки. В открывшемся редакторе (рис. 48) следует найти строку, начинающуюся с `linux /boot/vmlinuz`, в ее конец дописать требуемые параметры, отделив пробелом и нажать <F10>.

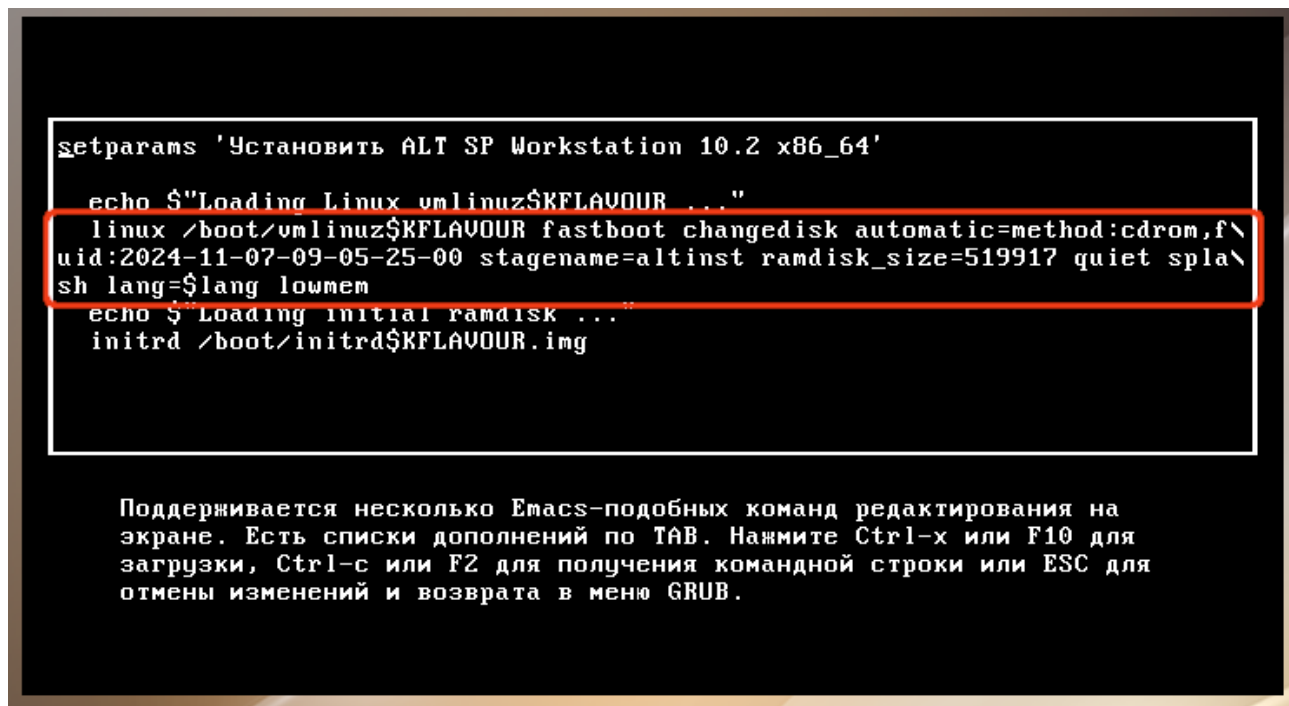


Рис. 48 – Редактор параметров пункта загрузки

В строке «Параметры загрузки», меню начального загрузчика, можно вручную задать параметры, передаваемые ядру, например:

- `nomodeset` – не использовать `modeset`-драйверы для видеокарты;
- `vga=normal` – отключить графический экран загрузки установщика;
- `xdriver=vesa` – явно использовать видеодрайвер `vesa`. Данным параметром можно явно указать нужный вариант драйвера;
- `acpi=off noapic` – отключение ACPI (управление питанием), если система не поддерживает ACPI полностью.

6. НАЧАЛО ИСПОЛЬЗОВАНИЯ ОС АЛЬТ СП

6.1. Запуск ОС

Запуск ОС Альт СП выполняется автоматически после запуска компьютера и отработки набора программ BIOS (БСВВ).

На экране появляется меню, в котором перечислены возможные варианты загрузки ОС (рис. 49, рис. 50).

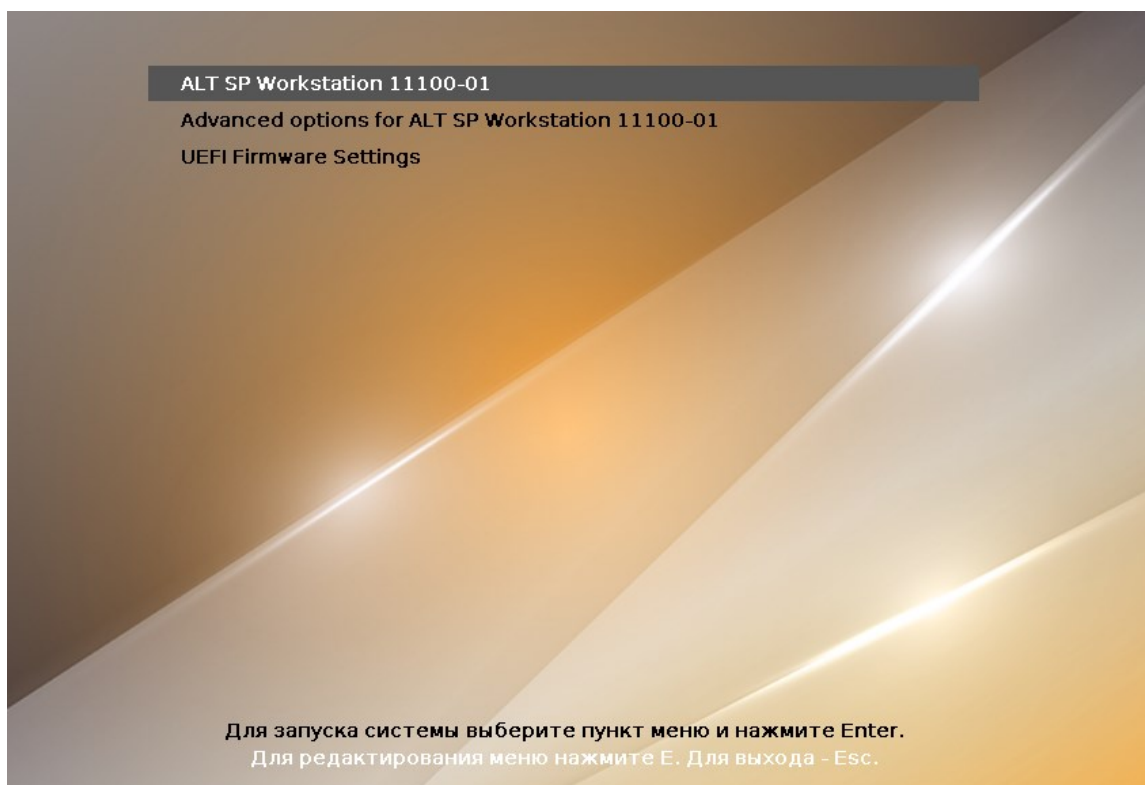


Рис. 49 – Варианты загрузки. Рабочая станция



Рис. 50 – Варианты загрузки. Сервер

По умолчанию, если не были нажаты управляющие клавиши на клавиатуре, загрузка ОС Альт СП продолжится автоматически.

Для выбора дополнительных параметров загрузки нужно выбрать пункт «Дополнительные параметры для ALT SP...» («Advanced options for ALT SP...»).

Примечание. Если при установке системы был установлен пароль на загрузчик, потребуется ввести имя пользователя «boot» и заданный на шаге «Установка загрузчика» пароль (рис. 51).

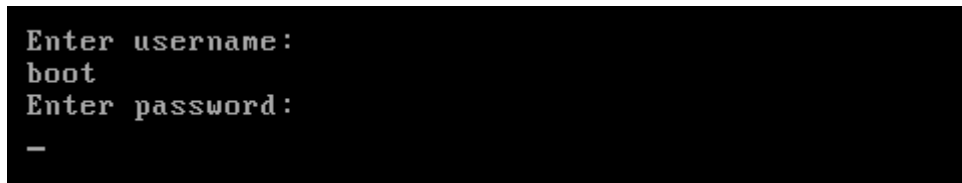


Рис. 51 – Пример части окна ввода пароля на загрузчик

Откроется окно с возможностью выбора способа дальнейшей загрузки ОС (рис. 52, рис. 53), например:

- «ALT SP Workstation 11100-01, vmlinuz»;
- «ALT SP Workstation 11100-01, vmlinuz (recovery mode)»;
- «ALT SP Workstation 11100-01, *».

* – зависит от актуального дистрибутива.

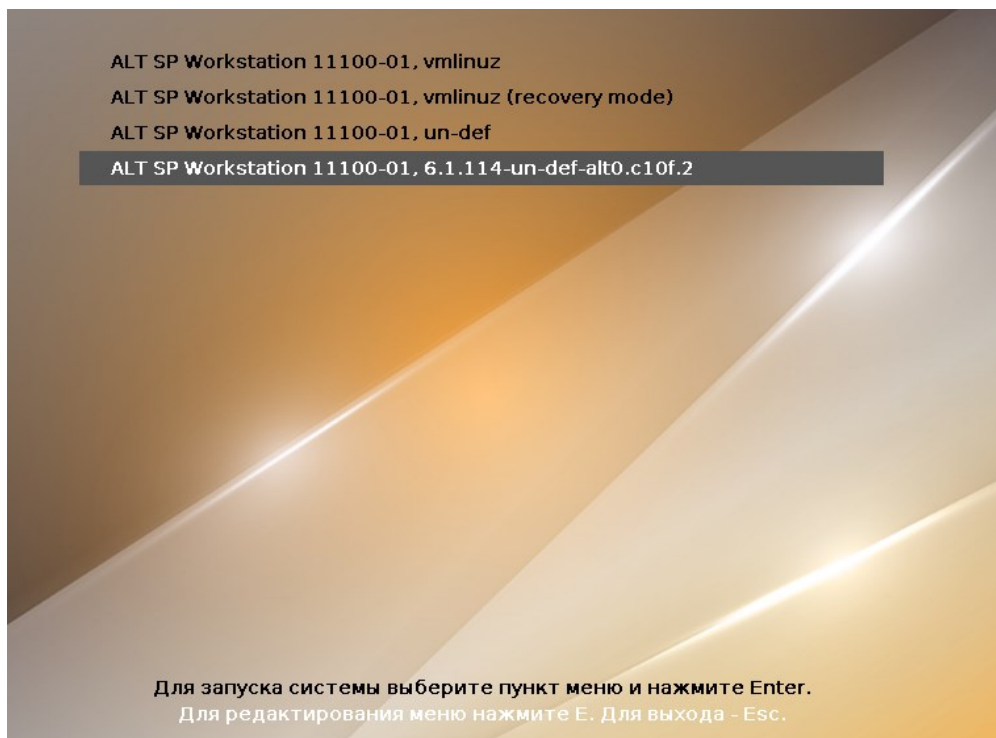


Рис. 52 – Пример окна дополнительные параметры



Рис. 53 – Пример окна дополнительные параметры. Сервер

Окно с перечнем дополнительных настроек загрузки (рис. 54) вызывается нажатием клавиши <E>.

Примечание. Если при установке системы был установлен пароль на загрузчик, то потребуется ввести имя пользователя «boot» и заданный на шаге «Установка загрузчика» пароль (см. рис. 51).

Примечание. Дополнительные опции загрузчика могут быть добавлены:
- в файле /etc/sysconfig/grub2 в строке GRUB_CMDLINE_LINUX_DEFAULT=..., после внесения изменений в файл следует обновить настройки загрузчика, выполнив команду:
update-grub
и перезагрузить ОС.

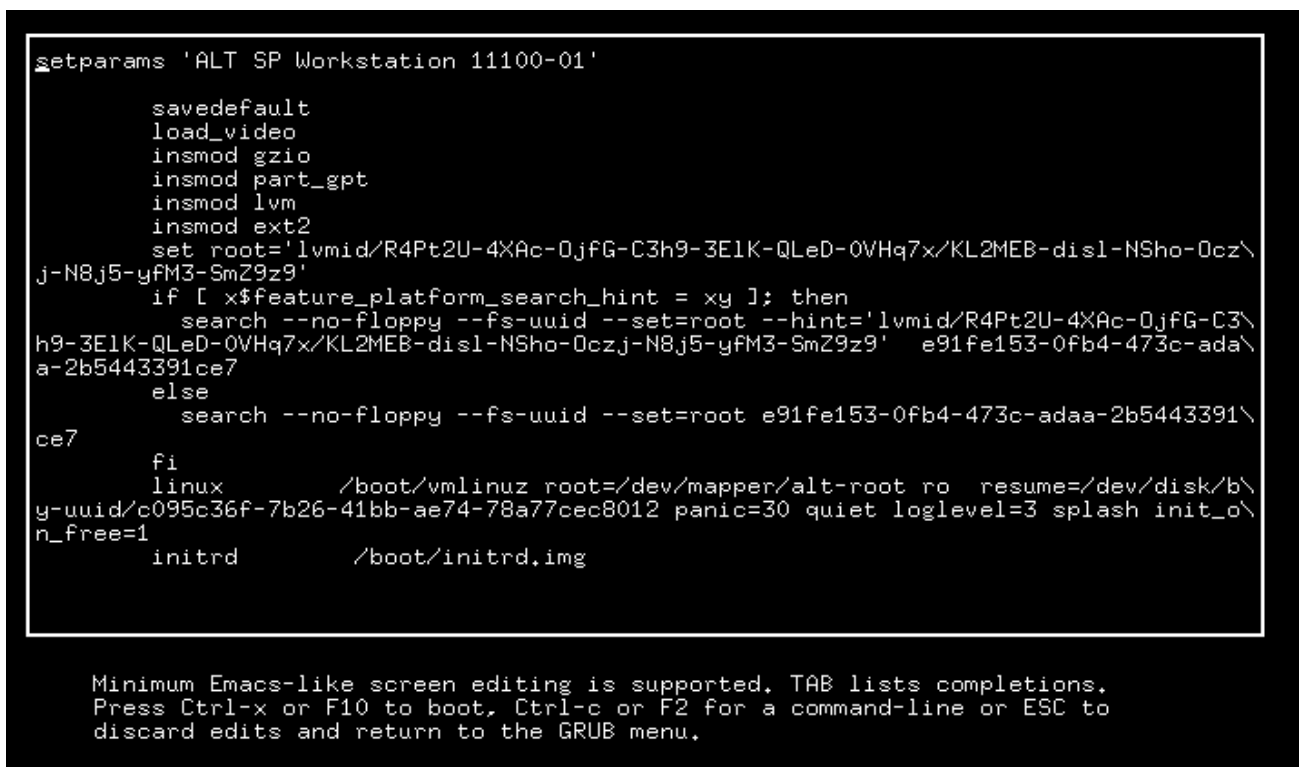


Рис. 54 – Пример окна с перечнем дополнительных настроек загрузчика GRUB

В процессе загрузки ОС Альт СП пользователь может следить за информацией процесса загрузки, которая отображает этапы запуска различных служб и программных серверов в виде отдельных строк (рис. 55) на экране монитора.

```
[ OK ] Finished Permit User Sessions.
[ OK ] Started Naming services LDAP client daemon..
[ OK ] Started OpenSSH server daemon.
[ OK ] Started Uxie Cron Daemon.
[ OK ] Started Getty on tty1.
[ OK ] Reached target Login Prompts.
       Starting Setup Virtual Console on tty1...
[ OK ] Finished Setup Virtual Console on tty1.
[ OK ] Started Corosync Cluster Engine.
[ OK ] Started Pacemaker High Availability Cluster Manager.
[ OK ] Started Postfix Mail Transport Agent.
[ OK ] Started PCS GUI and remote configuration interface (Ruby).
       Starting PCS GUI and remote configuration interface...
[ OK ] Started PCS GUI and remote configuration interface.
[ OK ] Reached target Multi-User System.
       Starting Record Runlevel Change in UTMP...
[ OK ] Finished Record Runlevel Change in UTMP.
```

Рис. 55 – Загрузка ОС

При этом каждая строка начинается словом вида [XXXXXXXX] (OK или FAILED), являющегося признаком нормального или ненормального завершения этапа загрузки. Слово XXXXXXXX=FAILED (авария) свидетельствует о неуспешном завершении этапа загрузки, что требует вмешательства и специальных действий администратора системы.

6.2. Получение доступа к шифруемым разделам

В случае если был создан шифруемый раздел (см. п. 5.4.4.4.3), потребуется вводить пароль при обращении к этому разделу (рис. 56).

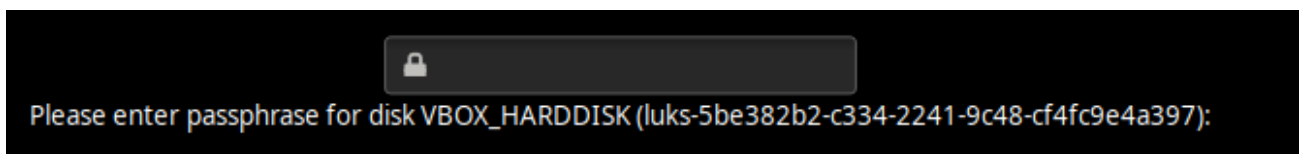


Рис. 56 – Пример запрос пароля для доступа к шифруемым разделам

Если не ввести пароль за отведенный промежуток времени, то загрузка системы завершится ошибкой. В этом случае следует перезагрузить систему, нажав для этого два раза <Enter>, а затем клавиши <Ctrl>+<Alt>+<Delete>.

6.3. Вход в систему

6.3.1. Идентификация и аутентификация в графической оболочке МАТЕ

В состав ОС может входить графическая оболочка МАТЕ. Оболочка состоит из набора различных программ и технологий, используемых для управления ОС и предоставляющих пользователю графический интерфейс для работы в виде оконных менеджеров.

При загрузке в графическом режиме работа загрузчика ОС заканчивается переходом к окну входа в систему (рис. 57).

Для продолжения работы и входа в ОС Альт СП в графическом режиме нужно выбрать одну из учетных записей, предлагаемых в окне аутентификации. Далее ввести пароль текущей учетной записи и нажать на кнопку «Войти».

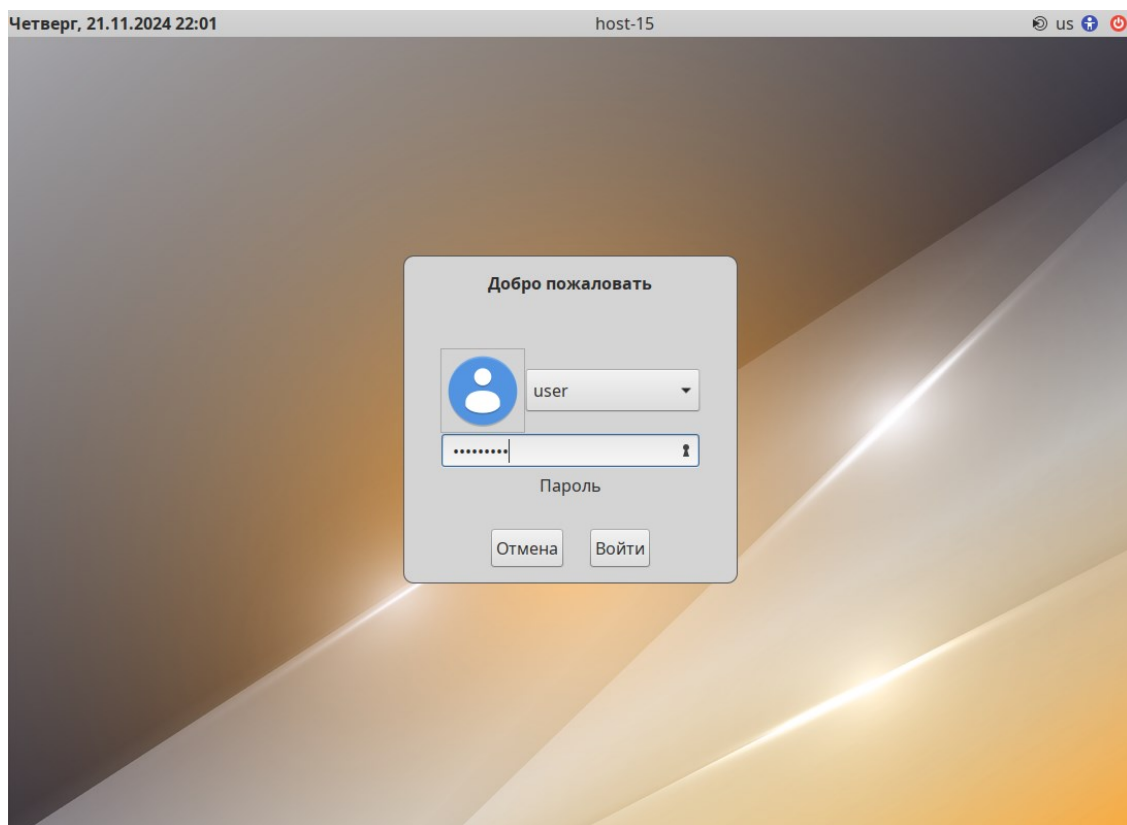


Рис. 57 – Окно входа в систему

Для выбора учетной записи, не показанной в списке выбора, нужно раскрыть выпадающий список со значением логина текущей учетной записи и выбрать пункт «Другие...» (рис. 58).

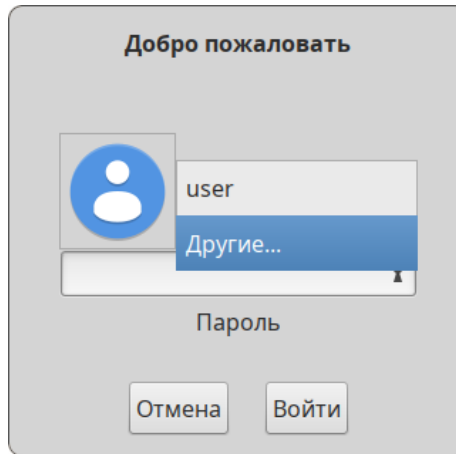


Рис. 58 – Выбор пользователя

После этого откроется окно ввода логина учетной записи (рис. 59), в котором нужно ввести логин учетной записи, и нажать кнопку «Войти». В следующем окне нужно ввести пароль учетной записи, и нажать кнопку «Войти».

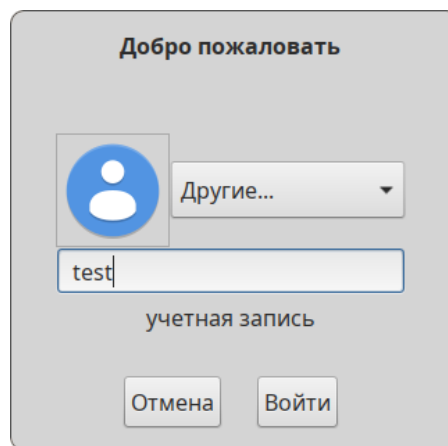



Рис. 59 – Ввод имени учетной записи

Чтобы запустить виртуальную клавиатуру на странице входа, следует нажать клавишу <F3> или щелкнуть на значок  на верхней панели, а затем отметить пункт «Экранная клавиатура» (рис. 60).

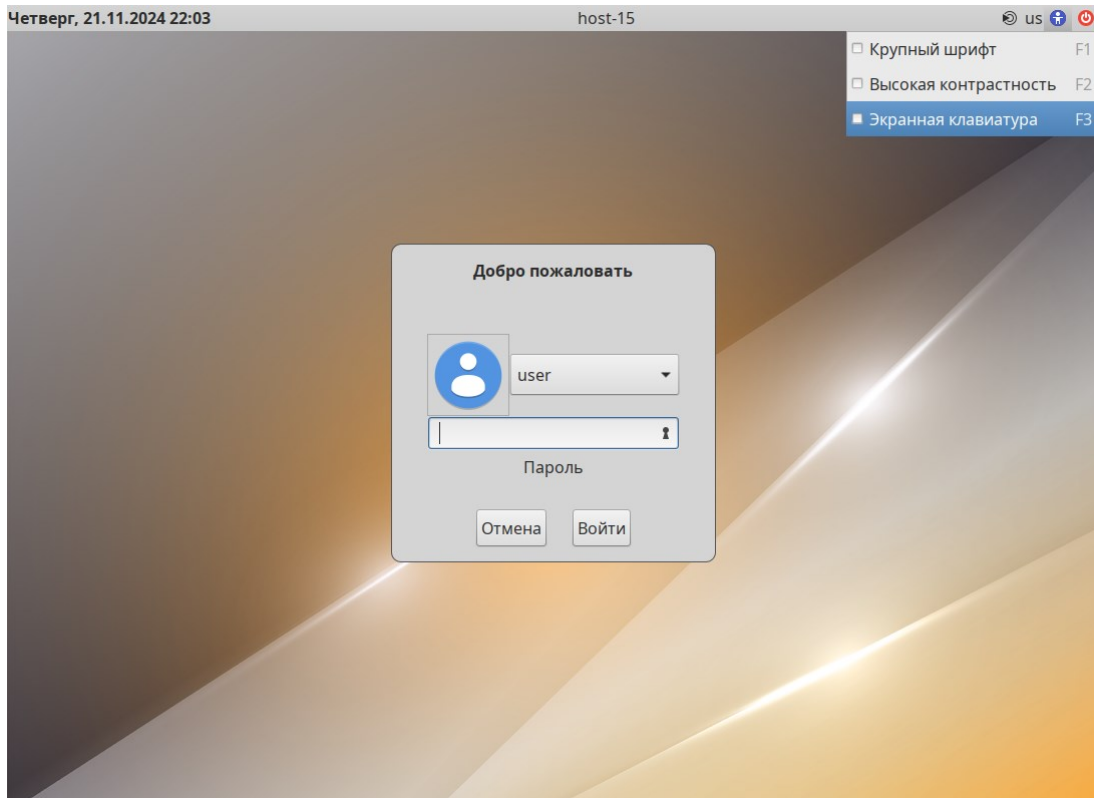


Рис. 60 – Страница входа в систему

На экране появится виртуальная клавиатура, ее можно использовать для ввода имени пользователя и пароля (рис. 61).

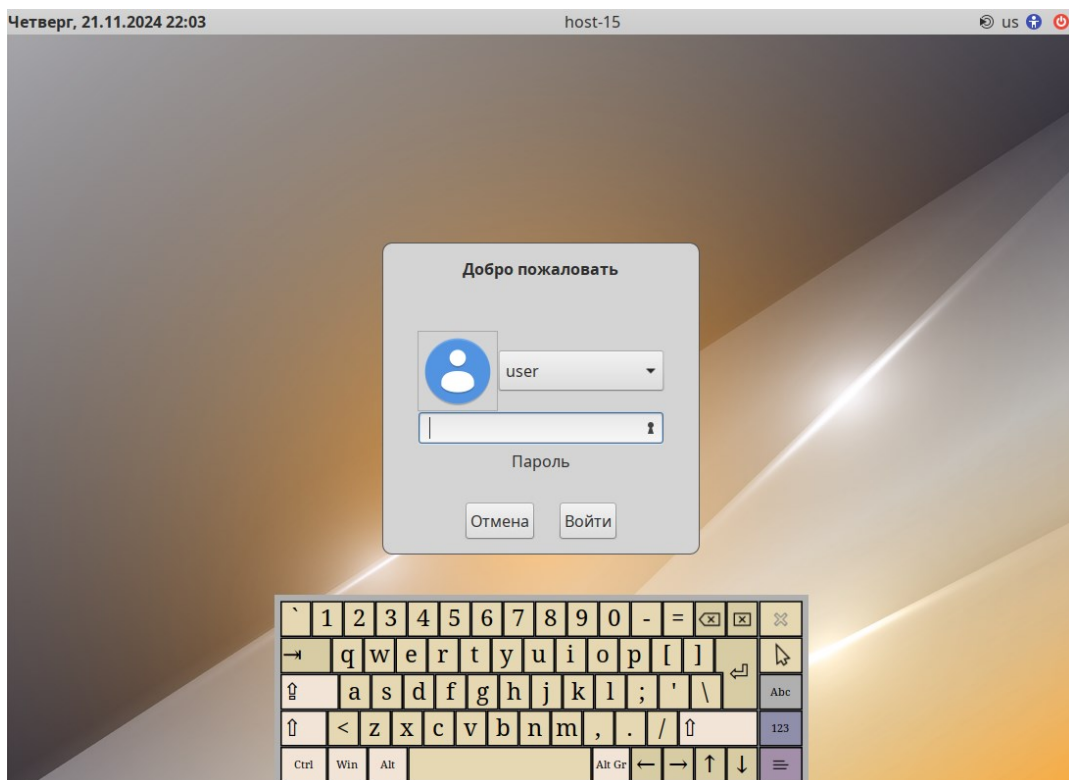


Рис. 61 – Виртуальная клавиатура при входе в систему

В результате успешного прохождения процедуры аутентификации и входа в систему запустится графическая оболочка ОС Альт СП (рис. 62).

Примечание. Работа в системе с использованием учетной записи администратора небезопасна, вследствие этого вход в систему в графическом режиме для администратора (root) запрещен. Попытка зарегистрироваться в системе будет прервана сообщением об ошибке.

В случае если графическая оболочка MATE была включена в состав ОС при установке, однако не стартовала автоматически, ее допускается вызвать вручную из консоли с помощью следующих команд:

```
~/ .xinitrc  
exec mate-session
```

Далее нужно использовать команду `startx` для запуска MATE.

Подробнее о приложениях для ОС Альт СП Рабочая станция и рабочем столе MATE приведено в документе «Руководство пользователя. ЛКНВ.11100-01 91 03».

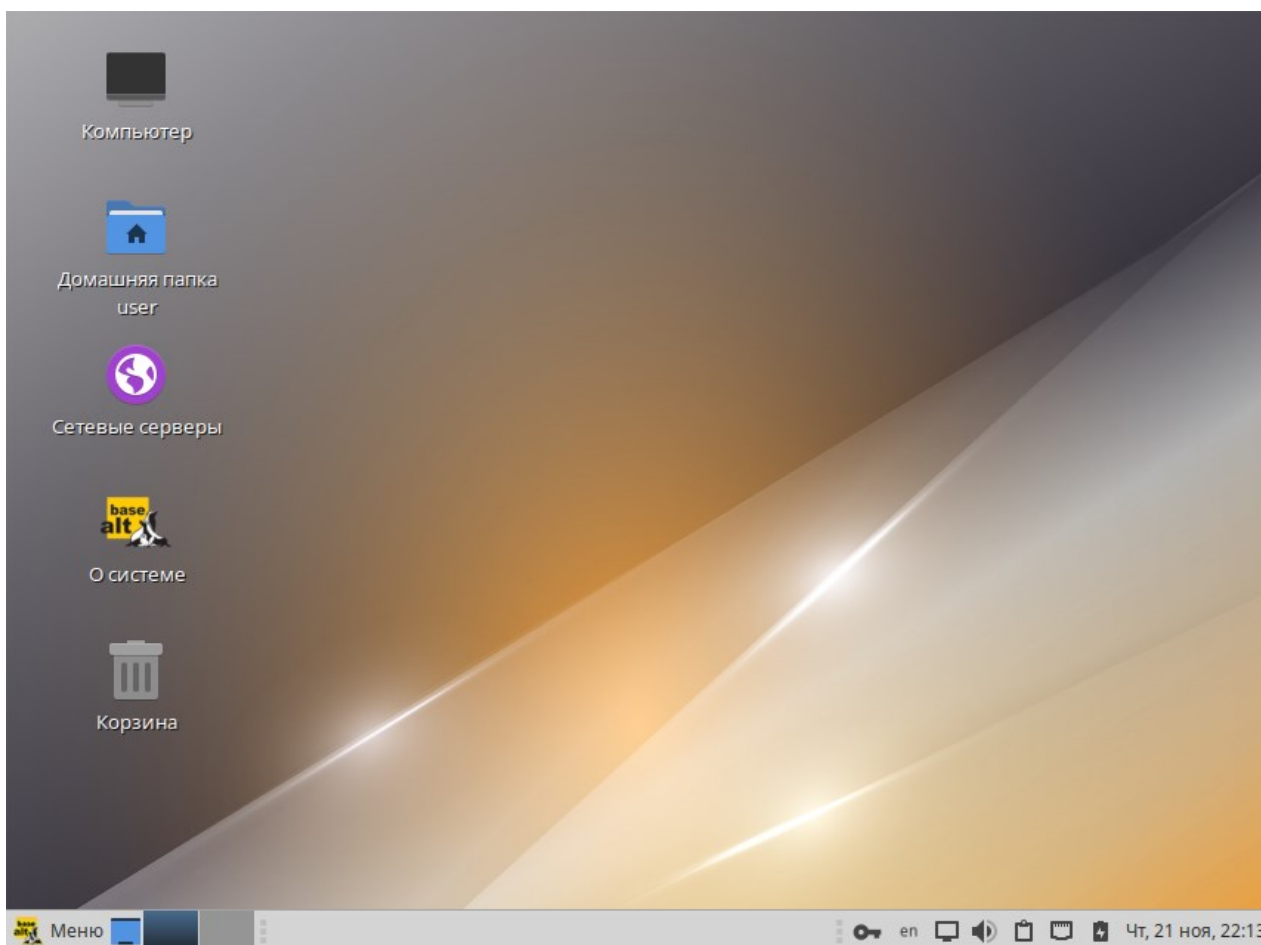


Рис. 62 – Рабочий стол MATE

6.3.2. Идентификация и аутентификация в консольном режиме

При загрузке в консольном режиме работа загрузчика завершается запросом на ввод логина и пароля учетной записи. В случае необходимости перехода на другую консоль нажмите клавиши <Ctrl>+<Alt>+<F2>.

Для продолжения работы в консольном режиме нужно ввести логин учетной записи пользователя и подтвердить его нажатием клавиши <Enter>. Затем ввести пароль и подтвердить его аналогичным образом.

В случае успешного прохождения процедуры аутентификации и входа в систему ОС перейдет к штатному режиму работы и предоставит дальнейший доступ к консоли (рис. 63).



```
host-15 login: user
Password:
Last login: Tue Nov 19 15:52:00 MSK 2024 from 192.168.0.177 on pts/4
[user@host-15 ~]$
```

Рис. 63 – Приглашение для ввода команд

6.3.3. Виртуальная консоль

В процессе работы ОС Альт СП активно несколько виртуальных консолей. Каждая виртуальная консоль доступна по одновременному нажатию клавиш <Ctrl>, <Alt> и функциональной клавиши с номером этой консоли от <F1> до <F6>.

На первых шести виртуальных консолях (от <Ctrl>+<Alt>+<F1> до <Ctrl>+<Alt>+<F6>) пользователь может зарегистрироваться и работать в текстовом режиме. Если была установлена графическая оболочка МАТЕ, она будет загружаться в первой виртуальной консоли. Двенадцатая виртуальная консоль (<Ctrl>+<Alt>+<F12>) выполняет функцию системной консоли – на нее выводятся сообщения о происходящих в системе событиях.

6.4. Блокирование сеанса доступа

6.4.1. Блокирование сеанса доступа после установленного времени бездействия (неактивности) пользователя или по его запросу

После авторизации и загрузки графической рабочей среды МАТЕ, пользователю предоставляется рабочий стол для работы с графическими приложениями.

Для безопасности данных компьютера и, чтобы другие пользователи не могли получить доступ к работающим приложениям, блокируйте свой экран, даже если оставляете компьютер на короткое время.

Заблокировать сеанс доступа можно по запросу пользователя: панель инструментов МАТЕ «Меню» → «Система» → «Заблокировать экран», или вызвать клавишами <Ctrl>+<Alt>+<L>.

При работе в графическом режиме блокирование сеанса доступа также происходит после установленного времени бездействия (по умолчанию 5 минут) посредством срабатывания программы – хранителя экрана (screensaver).

Время бездействия системы устанавливается: панель инструментов МАТЕ «Меню» → «Приложения» → «Параметры» → «Хранитель экрана».

При разблокировке экрана появляется виртуальная клавиатура (рис. 64), ее можно использовать для ввода пароля.



Рис. 64 – Разблокирование сеанса доступа

Для разблокировки требуется ввести пароль пользователя и нажать на кнопку «Разблокировать».

Примечание. Если виртуальная клавиатура при разблокировке экрана не нужна, можно удалить пакет `mate-screensaver-screenkeyboard`

При заблокированном экране другие пользователи могут входить в систему под своими учетными записями, нажав на экране ввода пароля кнопку «Переключить пользователя».

6.4.2. Блокировка виртуальных текстовых консолей

Программа `vlock` позволяет заблокировать сеанс при работе в консоли.

Выполнение команды `vlock` без дополнительных параметров заблокирует текущий сеанс виртуальной консоли, без прерывания доступа других пользователей:

```
$ vlock
Блокировка tty2 установлена user.
Используйте Alt-функциональные клавиши для перехода в другие
виртуальные консоли.
Пароль:
```

Чтобы предотвратить доступ ко всем виртуальным консолям машины, следует выполнить команду:

```
$ vlock -a
Теперь вывод на консоль полностью заблокирован user.
Пароль:
```

В этом случае `vlock` блокирует текущую активную консоль, а параметр `-a` предотвращает переключение в другие виртуальные консоли.

Примечание. Для разблокировки консоли необходимо ввести пароль пользователя.

6.4.3. Настройка блокировки возможности пользователя изменять настройки блокировки системы

Для блокировки возможности пользователя изменять настройки блокировки системы нужно выполнить следующие действия:

- 1) должен быть создан файл `/etc/dconf/profile/user` со следующим содержимым:

```
user-db:user
system-db:local
```

2) создать каталоги /etc/dconf/db/local.d/ и

/etc/dconf/db/local.d/locks (если их еще не существует):

```
# mkdir /etc/dconf/db/local.d/
# mkdir /etc/dconf/db/local.d/locks
```

3) создать файл /etc/dconf/db/local.d/screensaver, в который поместить текст:

```
[org/mate/screensaver]
idle-activation-enabled=true
lock-enabled=true
```

4) в файле /etc/dconf/db/local.d/session установить время бездействия в минутах:

```
[org/mate/session]
idle-delay=2
```

5) запретить пользователям изменять время бездействия, режим для этого создать файл /etc/dconf/db/local.d/locks/00-screensaver со следующим содержимым:

```
#prevent users from changing screensaver
/org/mate/screensaver/mode
/org/mate/desktop/session/idle-delay
```

б) выполнить обновление:

```
# dconf update
```

Примечание. Если машины находятся в «Альт Домен», эти настройки можно распространить на машины, используя групповые политики (см. п. 10.4.1).

6.5. Завершение сеанса пользователя

6.5.1. Графический режим

Для завершения сеанса пользователя в графическом режиме следует выбрать на панели инструментов МАТЕ «Меню» → «Система» → «Завершить сеанс».

Далее откроется окно (рис. 65), в котором предоставляется выбор дальнейших действий:

- переключить пользователя – сеанс пользователя в графическом режиме блокируется, другой пользователь может войти в систему под своим именем;
- завершить сеанс – выполняется завершение сеанса пользователя в графическом режиме.

Если не производить никаких действий, то сеанс пользователя будет автоматически завершён через 1 минуту.

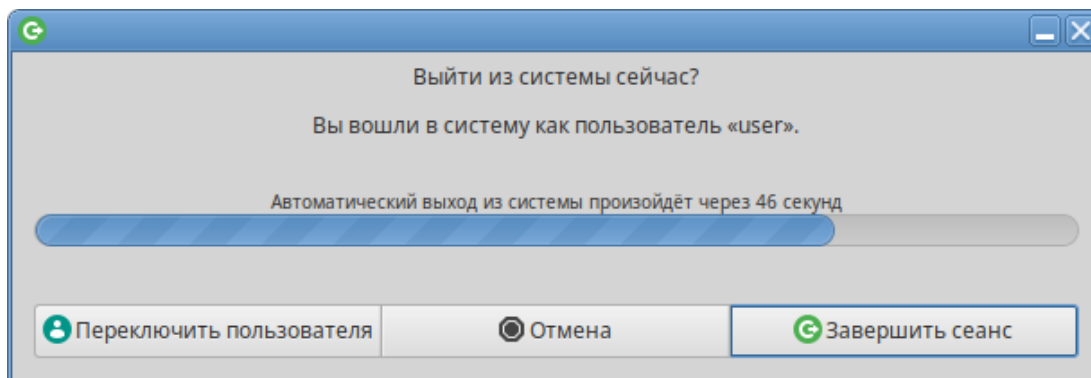


Рис. 65 – Окно выхода из системы

Примечание. Завершение сеанса произойдет до блокировки экрана, если установить время до завершения сеанса меньше, чем время, указанное для блокировки экрана (см. п. 6.4.3).

6.5.2. Консольный режим

Завершить сеанс пользователя в консольном режиме можно, выполнив команду `exit`.

6.5.3. Настройки завершения сеанса пользователя

Для каждого пользователя можно настроить автоматическое завершение сеанса после установленного времени бездействия (неактивности) пользователя.

Действия выполняются от администратора (`root`).

Для графического сеанса пользователя нужно создать файл `/etc/logout`, в который поместить допустимое время простоя (в секундах) для каждого пользователя, например:

```
user1 300
user2 200
```

Формат файла `/etc/logout`:

<user> <время в секундах от момента последнего действия>

Для консольного режима добавить в конце файла `/home/пользователь/.bash_profile` строку с указанием допустимого времени простоя (в секундах): `TMOUT=300`

Примечание. Для применения настроек необходимо перезагрузить ОС.

6.6. Выключение/перезагрузка компьютера

Для корректного завершения работы ОС (перезагрузки) во время ее работы запрещается выключать питание компьютера или перезагружать компьютер нажатием на кнопку «Reset», так как для корректного завершения работы требуется размонтирование файловой системы.

Перед окончанием работы с ОС нужно завершить все работающие программы.

6.6.1. Графический режим

Для выключения/перезагрузки компьютера следует выбрать на панели инструментов МАТЕ «Меню» → «Система» → «Выйти».

Далее откроется окно (рис. 66), в котором предоставляется выбор дальнейших действий:

- ждущий режим – компьютер переводится в режим экономии энергии;
- спящий режим – компьютер переводится в режим энергосбережения, позволяющий отключить питание компьютера, сохранив при этом текущее состояние ОС;
- перезагрузить – выполняется перезапуск ОС;
- выключить – выполняется выключение компьютера.

Если не производить никаких действий, то компьютер будет автоматически выключен через 1 минуту.

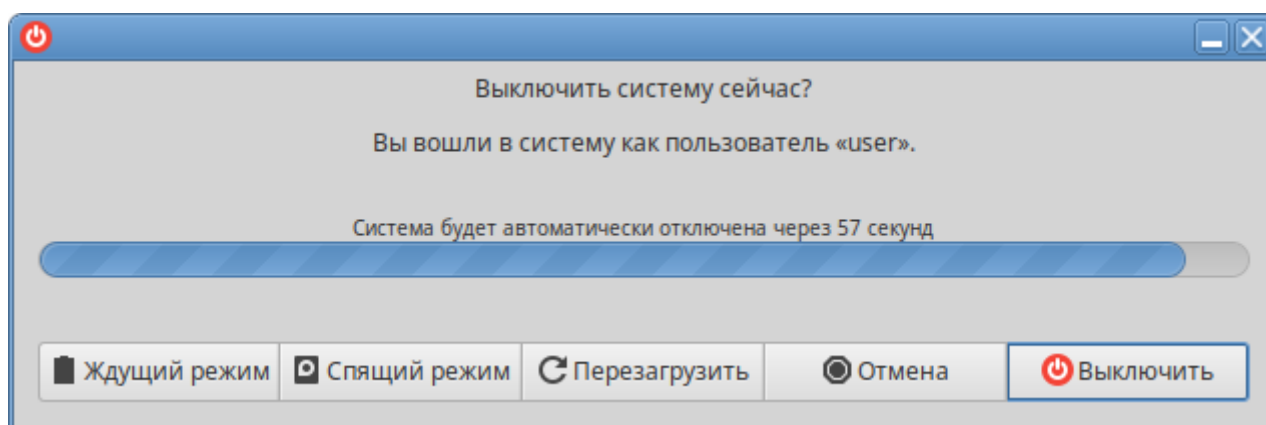


Рис. 66 – Окно выключения компьютера

6.6.2. Консольный режим

Перезагрузить систему в консольном режиме можно, выполнив команду:

```
$ systemctl reboot
```

Завершить работу и выключить компьютер (с отключением питания):

```
$ systemctl poweroff
```

Перевести систему в ждущий режим:

```
$ systemctl suspend
```

7. НАСТРОЙКИ СИСТЕМЫ

7.1. Центр управления системой

Для управления настройками установленной системы можно использовать ЦУС (также см. применение ЦУС в документе «Руководство по комплексу средств защиты. ЛКНВ.11100-01 99 03»).

ЦУС состоит из нескольких независимых диалогов-модулей. Каждый модуль отвечает за настройку определенной функции или свойства системы. Модули настройки сгруппированы по задачам.

Список установленных модулей можно просмотреть, выполнив команду от администратора:

```
# alterator-standalone
```

ЦУС можно использовать для разных целей, например (в скобках указаны имена соответствующих модулей):

- просмотра системных журналов (logs) (п. 8.7.1);
- управления системными службами (services) (п. 8.7.2);
- конфигурирования сетевых интерфейсов (net-eth) (рис. 145);
- настройки межсетевого экрана (net-iptables) (п. 8.5.1);
- настройки ограничений на использование внешних носителей (usbguard) (см. Руководство по КСЗ);
- настройки ограничения доступа к файловой системе USB-устройства (usbmount) (см. Руководство по КСЗ);
- создания, удаления и редактирования учетных записей пользователей (users);
- изменения пароля администратора системы (root) (п. 8.7.6);
- настройки даты и времени (datetime) (п. 8.7.7);
- настройки ограничений выделяемых ресурсов памяти пользователям (квоты) (quota п. 8.7.9);
- конфигурирования групповых политик (grpupdate);
- управления выключением удаленного компьютера (ahttpd-power, доступно только в веб-интерфейсе).

Примечание. Соответствующие наименования пакетов ЦУС alterator-*<имя_модуля>*, например, alterator-net-eth.

Чтобы исключить возможность несанкционированного доступа к ЦУС, по окончании работы нужно завершить сеанс, нажав на кнопку «Выход».

7.1.1. Графический интерфейс

Графический интерфейс ЦУС можно запустить следующими способами:

- комбинацией клавиш `<ALT>+<F2>` открыть окно быстрого запуска приложений и ввести в поле название программы – асс;
- выбрать на панели инструментов МАТЕ «Меню» → «Приложения» → «Администрирование» → «Центр управления системой»;
- при помощи консоли (приложение «Терминал»), в которой нужно ввести команду асс;
- зная имя модуля, запустить графический интерфейс для него, можно также выполнив команду:

```
$ alterator-standalone <имя-модуля>
```

Запуск ЦУС требует прав администратора – введите пароль root (рис. 67).

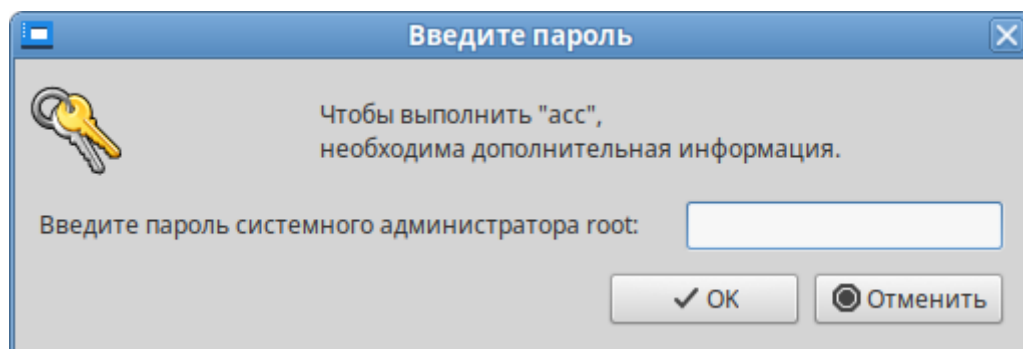


Рис. 67 – Запрос пароля для запуска «Центра управления системой»

После успешного входа откроется окно ЦУС (рис. 68).

Кнопка «Режим эксперта» (рис. 68) позволяет выбрать один из режимов:

- основной режим (кнопка отжата);
- режим эксперта (кнопка нажата).

Выбор режима влияет на количество отображаемых модулей. В режиме эксперта отображаются все модули, а в основном режиме только наиболее используемые.

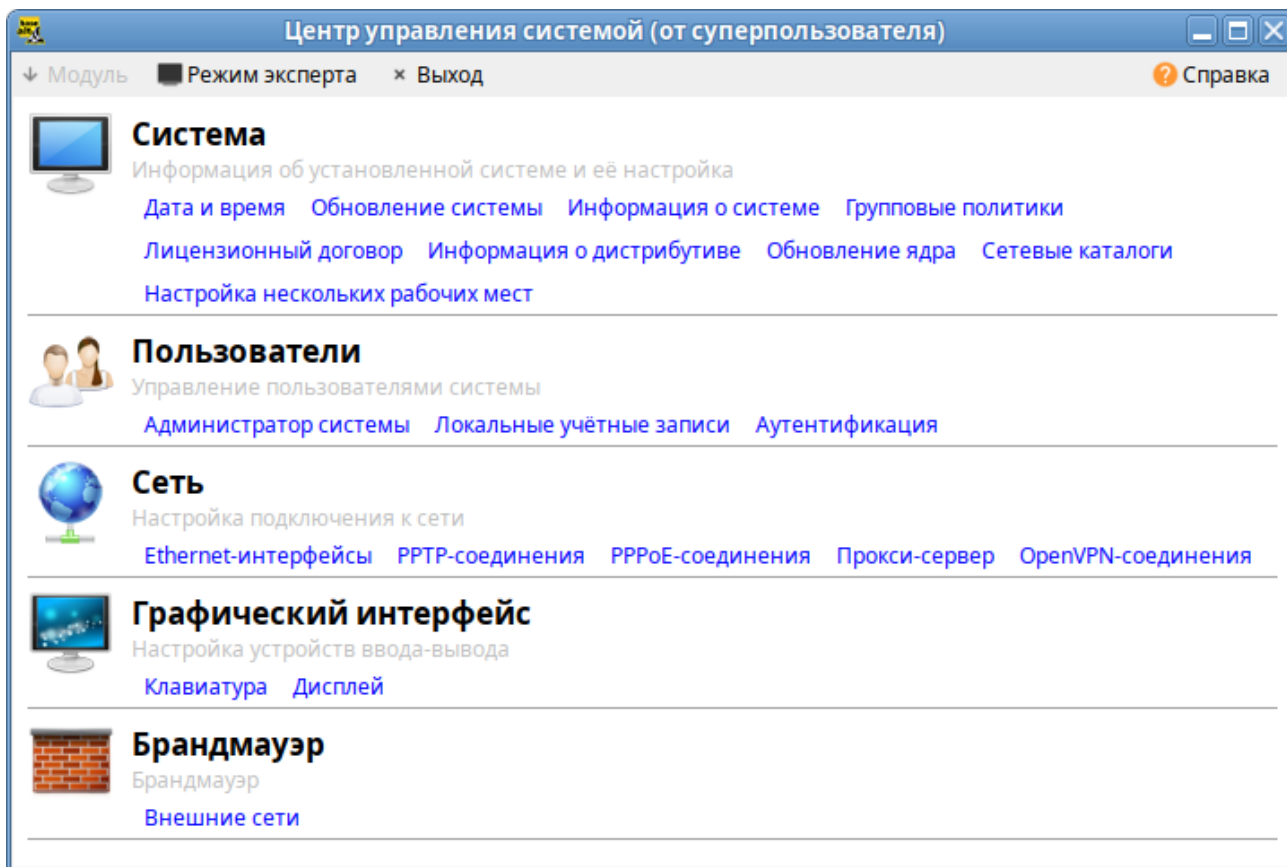


Рис. 68 – Окно «Центр управления системой»

7.1.2. Веб-интерфейс ЦУС

ЦУС имеет веб-ориентированный интерфейс, позволяющий управлять системой с любого компьютера сети.

Для запуска веб-ориентированного интерфейса, должен быть установлен пакет alterator-fbi:

```
# apt-get install alterator-fbi
```

Должны быть запущены сервисы ahttpd и alteratord:

```
# systemctl enable --now ahttpd
```

```
# systemctl enable --now alteratord
```


Работа с ЦУС может происходить из любого веб-браузера. Для начала работы нужно перейти по адресу `https://localhost:8080/` или `https://IP-адрес:8080/`.

IP-адрес можно узнать, выполнив команду:

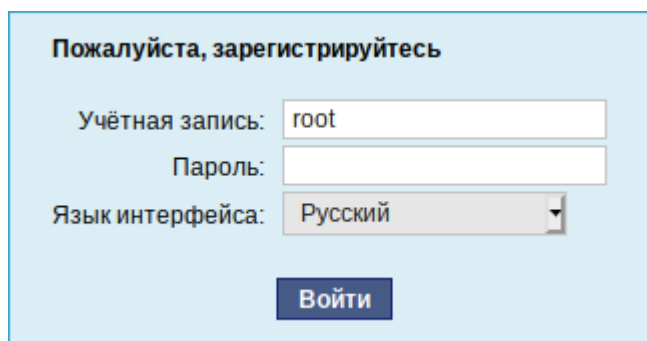
```
$ ip addr
```

Примечание. IP-адрес будет указан после слова `inet`:

```
inet 192.168.0.147/24 brd 192.168.0.255 scope global eth0
```

Где `192.168.0.147` – IP-адрес.

Для начала работы с ЦУС нужно зарегистрироваться. Запуск ЦУС требует прав администратора (ввести пароль `root`) (рис. 69). Дополнительно на этапе регистрации можно выбрать язык интерфейса. По умолчанию предлагается язык, определенный настройками веб-браузера.



Пожалуйста, зарегистрируйтесь

Учётная запись:

Пароль:

Язык интерфейса:

Рис. 69 – Запрос пароля администратора для запуска веб-интерфейса ЦУС

После успешного входа будут доступны все возможности ЦУС (рис. 70) на той машине, к которой было произведено подключение через веб-интерфейс.

Веб-интерфейс ЦУС можно настроить (кнопка «Настройка»), выбрав один из режимов:

- основной режим;
- режим эксперта.

Выбор режима влияет на количество отображаемых модулей. В режиме эксперта отображаются все модули, а в основном режиме только наиболее используемые.

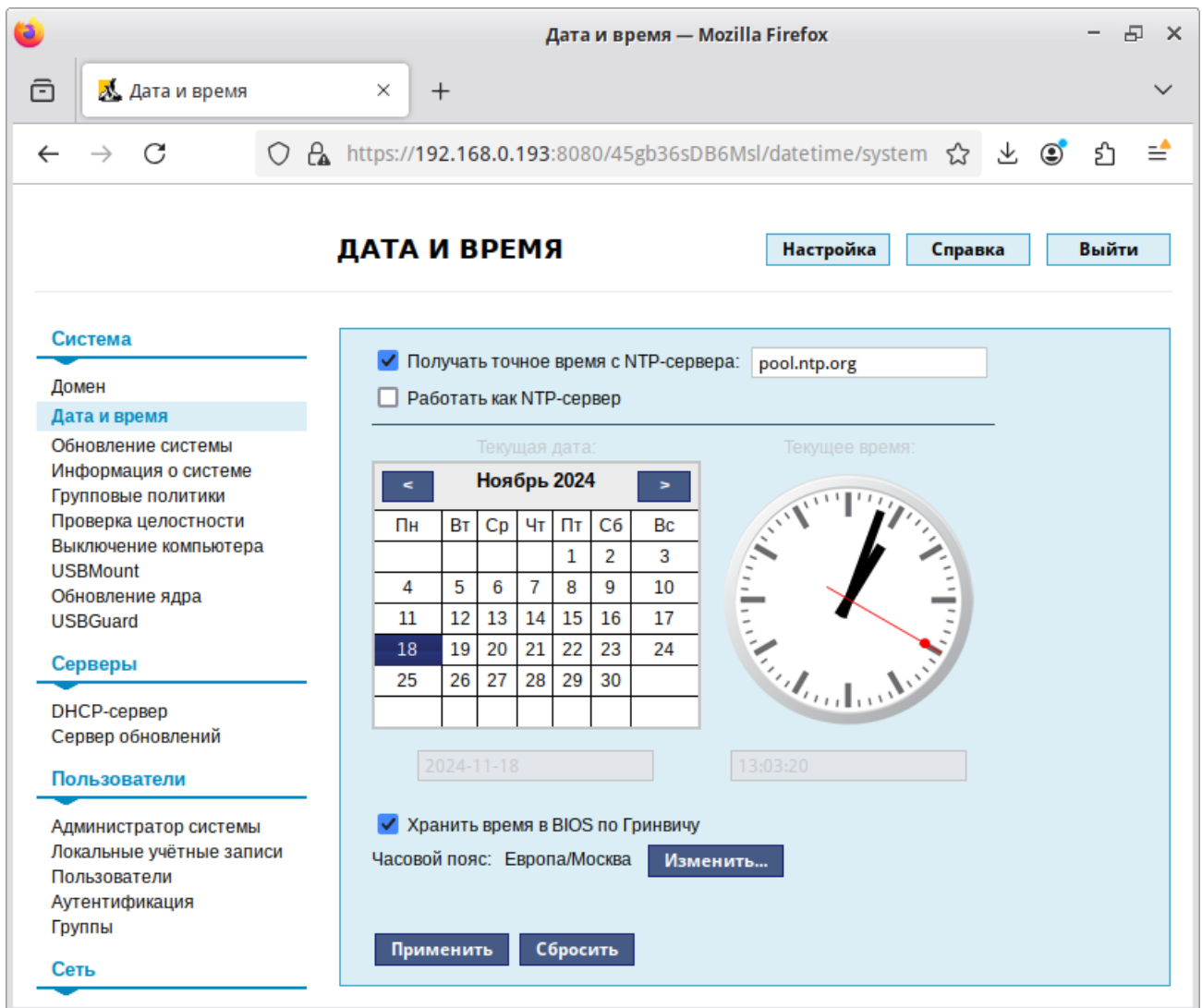


Рис. 70 – Окно веб-интерфейса «Центр управления системой»

ЦУС содержит справочную информацию по модулю, которую можно прочитать, нажав на кнопку «Справка» (см. п. 7.1.5).

⚠ После работы с ЦУС, в целях безопасности, не следует оставлять открытым веб-браузер. Необходимо обязательно выйти из сеанса работы с ЦУС, нажав на кнопку «Выйти».

7.1.3. Установка и удаление модулей ЦУС

Состав модулей, предоставляющих различные возможности для настройки системы в веб-интерфейсе, можно изменять.

Установленные пакеты, которые относятся к ЦУС, можно просмотреть, выполнив команду:

```
# rpm -qa | grep alterator
```

Для поиска прочих пакетов ЦУС выполните команду:

```
# apt-cache search alterator*
```

Модули можно дополнительно загружать и удалять как обычные программы:

```
# apt-get install alterator-net-openvpn
```

```
# apt-get remove alterator-net-openvpn
```

Примечание. После установки модуля, у которого есть веб-интерфейс, для того чтобы он отобразился в веб-интерфейсе, необходимо перезапустить службу ahttpd:

```
# systemctl restart ahttpd
```

7.1.4. Права доступа к модулям ЦУС

Администратор имеет доступ ко всем модулям, установленным в системе, и может назначать права доступа для пользователей к определенным модулям.

Для разрешения доступа пользователю к конкретному модулю, администратору в веб-интерфейсе ЦУС нужно выбрать нужный модуль и нажать ссылку «Параметры доступа к модулю», расположенную в нижней части окна модуля (рис. 71).

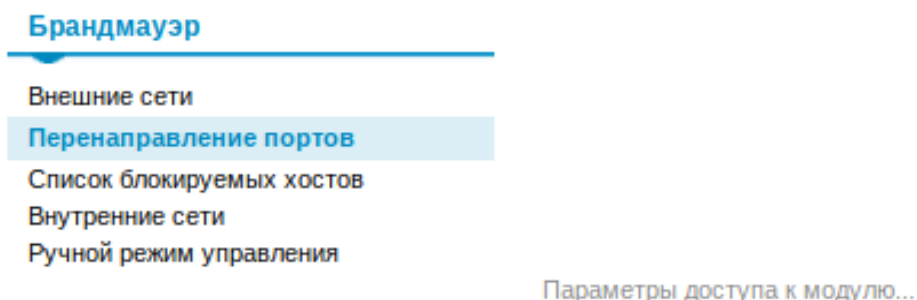


Рис. 71 – Ссылка «Параметры доступа к модулю»

В открывшемся окне, в списке «Новый пользователь», нужно выбрать пользователя, который получит доступ к данному модулю, и нажать на кнопку «Добавить». Для сохранения настроек нужно перезапустить НТТР-сервер, для этого достаточно нажать на кнопку «Перезапустить НТТР-сервер» (рис. 72).

Для удаления доступа пользователя к определенному модулю, администратору, в окне этого модуля нужно нажать ссылку «Параметры доступа к модулю», в открывшемся окне в списке пользователей, которым разрешен доступ, выбрать пользователя, нажать на кнопку «Удалить» (рис. 72) и нажать на кнопку «Перезапустить HTTP-сервер».

Параметры доступа к модулю

Следующие пользователи имеют доступ:

newuser	Удалить
---------	---------

Новый пользователь:

user	Добавить
------	----------

Замечание: Все ваши изменения вступят в силу после перезапуска HTTP сервера.

Перезапустить HTTP-сервер

Рис. 72 – Параметры доступа к модулю

Системный пользователь, пройдя процедуру аутентификации (рис. 73), может просматривать и вызывать модули, к которым он имеет доступ (рис. 74).

Пожалуйста, зарегистрируйтесь

Учётная запись: newuser

Пароль: ●●●

Язык интерфейса: Русский

Войти

Рис. 73 – Запрос пароля учетной записи пользователя для запуска веб-интерфейса ЦУС

Настройка Справка Выйти

DHCP-СЕРВЕР

Система

Дата и время

Серверы

DHCP-сервер

Сеть

Ethernet-интерфейсы

Общие настройки

Версия IP: IPv4

Включить службу DHCP

Интерфейс: enp0s3 (192.168.0.1 - 192.168.0.254)

(максимально допустимый диапазон адресов)

Начальный IP адрес:

Конечный IP адрес:

Срок действия адреса: 1 час

Информация, предоставляемая клиентам

DNS-сервер:

Домен поиска:

Шлюз по умолчанию:

Применить Сбросить

Рис. 74 – Веб-интерфейс ЦУС, запущенный от системного пользователя

7.1.5. Получение справочной информации

Модули ЦУС содержат встроенную справку (рис. 75), поясняющую назначение конкретного модуля. Справка вызывается кнопкой «Справка».

Настройка Справка Выйти

ETHERNET-ИНТЕРФЕЙСЫ

Ethernet-интерфейсы

IP (Internet Protocol) — основа стека протоколов TCP/IP. **IP-адрес** и **Маска сети** — обязательные параметры каждого узла IP-сети. Первый параметр — уникальный идентификатор машины, от второго напрямую зависит, к каким машинам локальной сети данная машина будет иметь доступ. Если требуется выход во внешнюю сеть, то не забудьте про параметр **Шлюз по умолчанию**.

В случае наличия *DHCP-сервера* можно все вышеперечисленные параметры получить автоматически — просто включите **Использовать DHCP**.

Если в компьютере имеется несколько сетевых карт, то возможна ситуация, когда при очередной загрузке ядро присвоит имена интерфейсов (eth0, eth1) в другом порядке. В результате интерфейсы получат не свои настройки. Чтобы этого не происходило, вы можете привязать интерфейс к имени по его аппаратному адресу (MAC) или по местоположению на системной шине.

Общие сетевые настройки

Существует ряд общих сетевых параметров, не привязанных к какому либо конкретному интерфейсу.

Имя компьютера — имя машины в локальной сети. Имя компьютера, в отличие от традиционного имени хоста в Unix (hostname), не содержит названия сетевого домена.

Рис. 75 – Получение справочной информации о модуле ЦУС

7.2. Выбор программ, запускаемых автоматически при входе в систему

Для более удобной работы с системой можно выбрать определенные программы, которые будут запущены автоматически при входе пользователя в систему. Автозапускаемые программы автоматически сохраняют свое состояние и безопасно завершаются сеансовым менеджером при выходе из системы и перезапускаются при входе.

Инструмент настройки сессии позволяет настроить, какие программы будут автоматически запущены при входе в систему. Для запуска инструмента настройки сессии, выбрать на панели инструментов МАТЕ «Меню» → «Приложения» → «Параметры» → «Запускаемые приложения».

7.2.1. Вкладка автоматического запуска программ

Список автоматически запускаемых программ представлен на вкладке «Автоматически запускаемые программы» (рис. 76). Этот список содержит краткое описание каждой программы и отметку, указывающую запускать программу или нет.

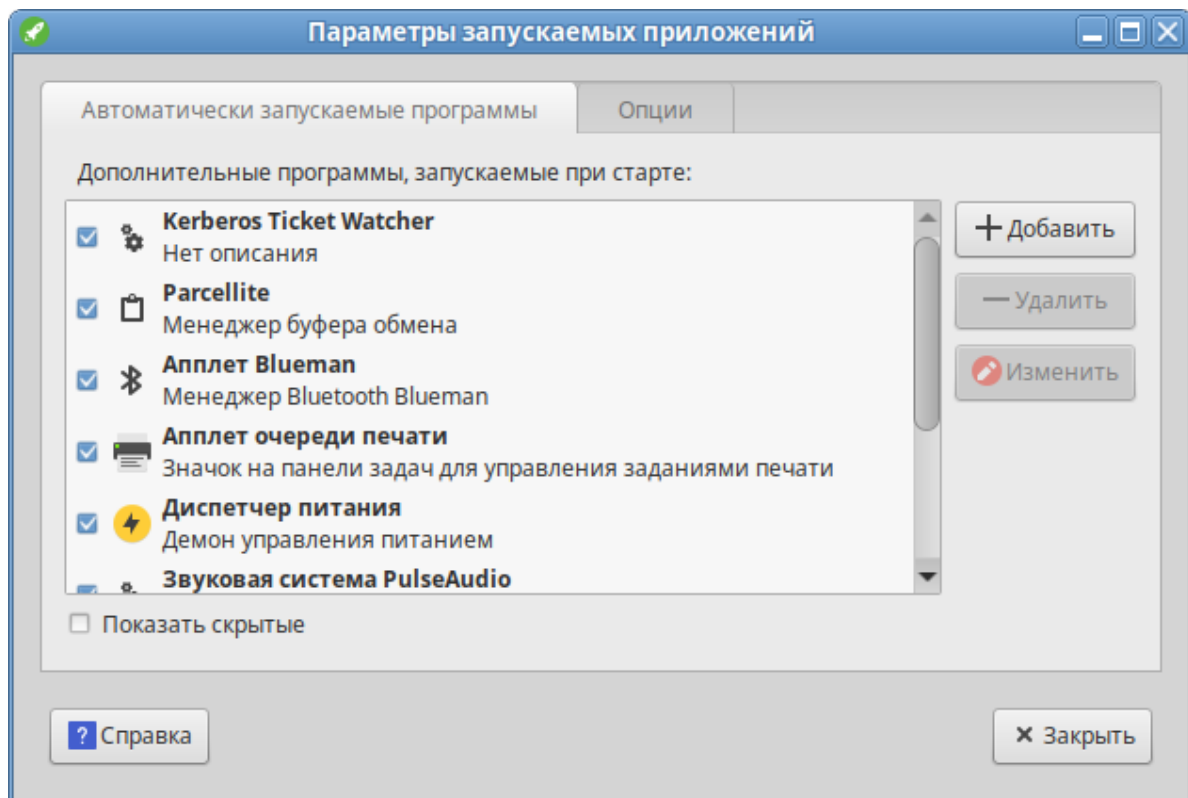


Рис. 76 – Автоматически запускаемые программы

На этой вкладке можно добавлять, удалять и изменять автозапускаемые приложения.

Для добавления новой автоматически запускаемой программы, следует выполнить следующие шаги:

- нажать на кнопку «Добавить». Откроется окно «Новая автоматически запускаемая программа»;
- указать имя программы и команду, которая запустит приложение (рис. 77);
- нажать на кнопку «Добавить».

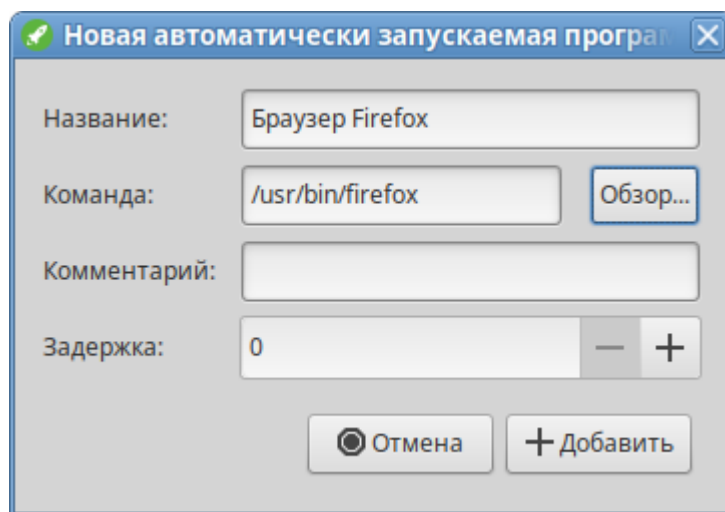


Рис. 77 – Добавление автоматически запускаемой программы

7.2.2. Вкладка настроек сессии

Менеджер сеанса может запомнить, какие приложения были запущены при выходе из системы, и автоматически запустить их при входе в систему. Для того чтобы это происходило каждый раз при выходе из системы, следует на вкладке «Опции» отметить пункт «Автоматически запоминать запущенные приложения при выходе из сеанса» (рис. 78).

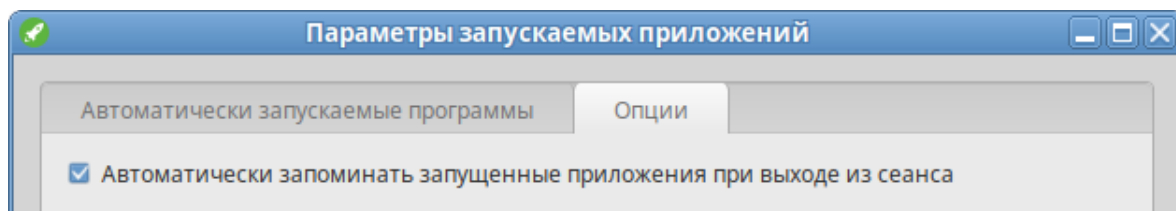


Рис. 78 – Запоминать запущенные приложения при выходе из сеанса

7.3. Режим киоск по ограничению запуска программ

В режиме киоск пользователь имеет право запускать программы только явно разрешенные администратором.

7.3.1. Настройка ограничения в ЦУС

Примечание. Для работы киоска должны быть установлены пакеты alterator-kiosk и kiosk-mate-profiles:

```
# apt-get install alterator-kiosk kiosk-mate-profiles
```

Для включения режима киоск необходимо в ЦУС перейти в раздел «Система» → «Настройка kiosk».

Для разрешения запуска определенных приложений, необходимо выбрать соответствующий профиль из списка «Профили», установить отметку в поле «Включен» (рис. 79).

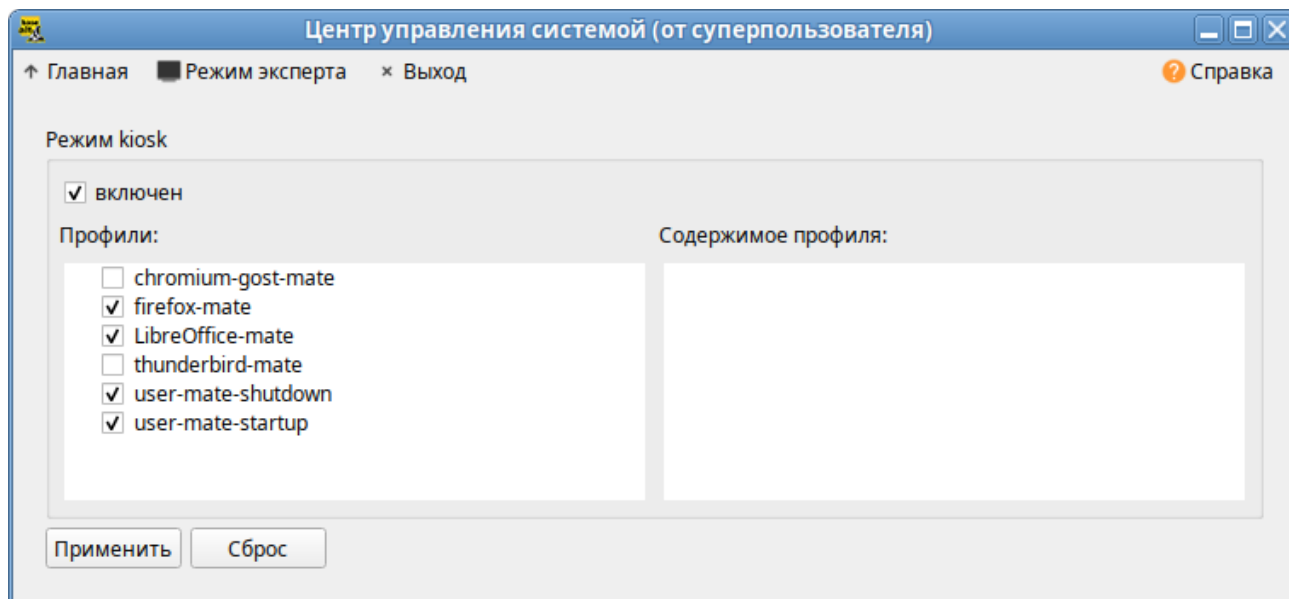


Рис. 79 – Настройка kiosk

Режим киоск будет применен после нажатия кнопки «Применить».

Список приложений, из которых состоит профиль, можно увидеть в окне «Содержимое профиля» (профиль выделяется щелчком любой кнопки мыши):

Примечание. Для создания нового профиля необходимо создать новый файл в каталоге `/etc/alterator/kiosk/profiles/` и вписать в него разрешенные к запуску программы. Например, для создания профиля atril, достаточно в файл `/etc/alterator/kiosk/profiles/` добавить строку:

```
U /usr/bin/atril
```


Для выключения режима киоск необходимо зарегистрироваться в системе под пользователем root (например, на второй консоли <Ctrl>+<Alt>+<F2>), выполнить команду:

```
# echo "0" > /etc/alterator/kiosk/mode
```

и перезагрузить систему.

7.3.2. Управление режимом киоск в консоли

Для управления режимом киоск, можно воспользоваться командой `kiosk`. Все команды выполняются с правами администратора.

Примечание. Утилита `kiosk` используется для временного включения/отключения режима киоск. После перезагрузки компьютера будет включен тот режим, который был установлен в модуле ЦУС «Настройка `kiosk`».

Примеры использования команды `kiosk`:

- просмотреть пути в белом списке:

```
# kiosk --user-list
/bin/basename
/bin/dbus-daemon
/bin/dbus-update-activation-environment
/bin/false
```

...

- добавить указанный путь в белый список:

```
# kiosk --user-list-append /путь
```

- удалить указанный путь из белого списка:

```
# kiosk --user-list-remove /путь
```

- активировать режим киоск:

```
# kiosk --set-mode 1
```

- деактивировать режим киоск:

```
# kiosk --set-mode 0
```

- просмотреть состояние режима:

```
# kiosk --get-mode
```

7.4. Задание хешей паролей

В ОС Альт СП реализована возможность хранения аутентификационной информации пользователей, полученной с использованием хеш-функций по ГОСТ Р 34.11–2012.

Примечание. Смена алгоритма хеширования происходит при изменении пароля пользователя, например, если истекает срок его действия, или пользователь сменил его. До этого момента алгоритм хеширования остается тем, с которым пароль был задан изначально. Поэтому, перед проверкой изменения алгоритма хэширования, измените пароль пользователя.

7.4.1. Смена алгоритма в консоли

Установить пакет `tcb-hash-prefix-control`:

```
# apt-get install tcb-hash-prefix-control
```

Список возможных хеш-функций можно вывести, выполнив команду:

```
# control tcb-hash-prefix help
bcrypt_2b: prefix=$2b$ count=8 (4 - 31 limit)
bcrypt_2y: prefix=$2y$ count=8 (4 - 31 limit)
bcrypt_2a: prefix=$2a$ count=8 (4 - 31 limit)
yescrypt: prefix=$y$ count=8 (0 - 11 limit)
scrypt: prefix=$7$ count=8 (0 - 11 limit)
gost_yescrypt: prefix=$gy$ count=8 (0 - 11 limit)
sha256: prefix=$5$ count=10000 (1000 - 100000 limit)
sha512: prefix=$6$ count=10000 (1000 - 100000 limit)
default: hash prefix managed by libcrypt
```

Просмотреть текущее значение хеш-функции:

```
# control tcb-hash-prefix
default
```

Изменить тип хеша по умолчанию на `gost-yescrypt`:

```
# control tcb-hash-prefix gost_yescrypt
```

Установить пароль пользователю:

```
# passwd user
```

Проверка:

```
# passwd -S user
Password set, gost-yescrypt encryption.
```

7.4.2. Смена алгоритма в ЦУС

Установить пакет `alterator-secsetup`:

```
# apt-get install alterator-secsetup
```

Для изменения типа хеша по умолчанию на ГОСТ Р 34.11–2012 необходимо в ЦУС перейти в раздел «Система» → «Настройки безопасности».

В открывшемся окне следует отметить пункт «Включить хеширование паролей пользователей по алгоритму ГОСТ Р 34.11-2012» и нажать кнопку «Применить» (рис. 80).

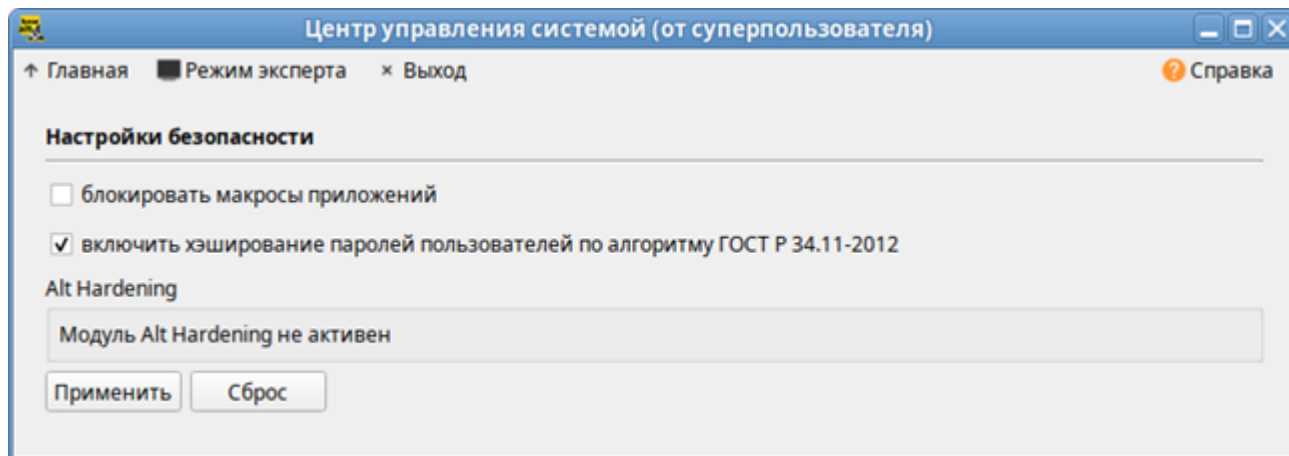


Рис. 80 – Задание хешей паролей в соответствии с ГОСТ Р 34.11–2012

Проверить настройку можно, установить пароль пользователю и выполнив команду:

```
# passwd user
# passwd -S user
Password set, gost-yescrypt encryption.
```

7.5. Настройка фильтрации пакетов с помощью утилиты iptables

Утилита iptables – стандартный интерфейс командной строки для управления фильтрацией сетевых пакетов и сбора статистики сетевого взаимодействия.

Утилита iptables позволяет фильтровать сетевые пакеты по следующим параметрам:

- на основе сетевых адресов отправителя и получателя (IP-адреса, MAC-адреса);
- по протоколам tcp, udp, icmp;
- с учетом входного и выходного сетевого интерфейса;
- на основе используемого порта;
- с учетом даты и времени.

Фильтры состоят из правил. Каждое правило – это строка, содержащая в себе критерии, определяющие, подпадает ли пакет под заданное правило, и действие, которое нужно выполнить в случае удовлетворения критерия.

7.5.1. Устройство фильтра iptables

Для iptables в общем виде правила выглядят так:

```
iptables [-t table] command [match] [target/jump]
```

Если в правило не включается спецификатор `[-t table]`, то по умолчанию предполагается использование таблицы `filter`, если же предполагается использование другой таблицы, то это требуется указать явно. Спецификатор таблицы так же можно указывать в любом месте строки правила, однако для удобства чтения лучше указывать таблицу в начале правила.

Непосредственно за именем таблицы должна стоять команда управления фильтром. Если спецификатора таблицы нет, то команда всегда должна стоять первой. Команда определяет действие iptables (вставить правило, добавить правило в конец цепочки, или удалить правило). Тело команды в общем виде выглядит так:

```
[команда] [цепочка]
```

Ключ команда указывает на то, что нужно сделать с правилом, например, команда `-A` указывает на то, что правило нужно добавить в конец указанной цепочки.

Цепочка указывает, в какую цепочку нужно добавить правило. Стандартные цепочки – `INPUT`, `OUTPUT`, `FORWARD`, `PREROUTING` и `POSTROUTING`. Они находятся в таблицах фильтра. Не все таблицы содержат все стандартные цепочки. Подробнее таблицы и цепочки описаны ниже.

Раздел `[match]` задает критерии проверки, по которым определяется, подпадает ли пакет под действие этого правила или нет. Здесь можно указать самые разные критерии – IP-адрес источника пакета или сети, сетевой интерфейс.

Раздел `[target]` указывает, какое действие должно быть выполнено при условии выполнения критериев в правиле. Здесь можно передать пакет в другую цепочку правил, «сбросить» пакет и забыть про него, выдать на источник сообщение об ошибке и т. д.

Когда пакет приходит на сетевое устройство, он обрабатывается соответствующим драйвером и далее передается в фильтр в ядре ОС. Далее пакет проходит ряд таблиц и затем передается либо локальному приложению, либо переправляется на другую машину (рис. 81).

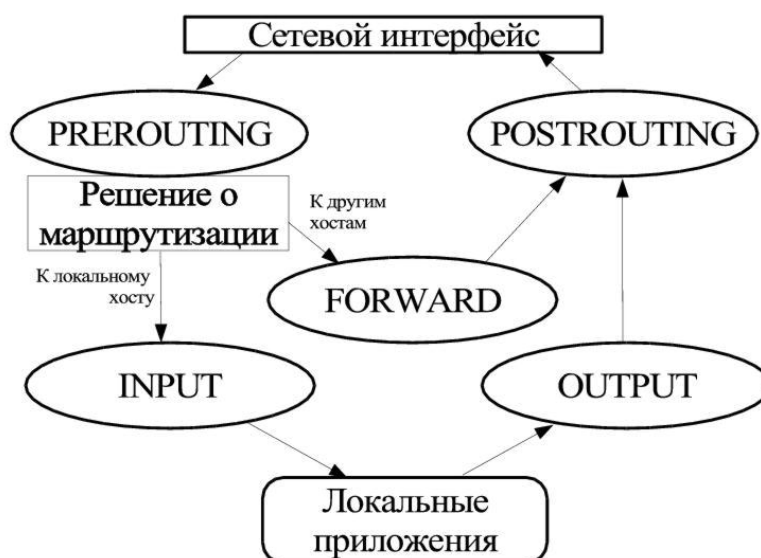


Рис. 81 – Схема движения пакетов в iptables

7.5.2. Встроенные таблицы фильтра iptables

По умолчанию используется таблица filter. Опция `-t` в правиле указывает на используемую таблицу. С ключом `-t` можно указывать следующие таблицы: `nat`, `mangle`, `filter`.

7.5.2.1. Таблица nat

Таблица `nat` используется главным образом для преобразования сетевых адресов Network Address Translation. Через эту таблицу проходит только первый пакет из потока. Преобразование адресов автоматически применяется ко всем последующим пакетам.

Таблица имеет три цепочки PREROUTING, OUTPUT и POSTROUTING:

- цепочка PREROUTING используется для внесения изменений в пакеты на входе в фильтр;
- цепочка OUTPUT используется для преобразования пакетов, созданных приложениями внутри компьютера, на котором установлен фильтр, перед принятием решения о маршрутизации;

- цепочка POSTROUTING используется для преобразования пакетов перед выдачей их в сеть.

7.5.2.2. Таблица mangle

Таблица mangle используется для внесения изменений в заголовки пакетов. Примером может служить изменение поля TTL, TOS или MARK. Таблица имеет две цепочки PREROUTING и OUTPUT:

- цепочка PREROUTING используется для внесения изменений на входе в фильтр перед принятием решения о маршрутизации;
- цепочка OUTPUT – для внесения изменений в пакеты, поступающие от внутренних приложений. Таблица mangle не должна использоваться для преобразования сетевых адресов (Network Address Translation) или маскардинга (masquerading), для этих целей используется таблица nat.

7.5.2.3. Таблица filter

Таблица filter используется, главным образом, для фильтрации пакетов.

Таблица имеет три цепочки – FORWARD, INPUT, OUTPUT:

- цепочка FORWARD используется для фильтрации пакетов, идущих транзитом через данный компьютер;
- цепочка INPUT предназначена для обработки входящих пакетов, направляемых локальным приложениям данного компьютера;
- цепочка OUTPUT используется для фильтрации исходящих пакетов, сгенерированных локальными приложениями данного компьютера.

7.5.3. Команды утилиты iptables

В таблице 1 приведены команды, которые используются в iptables.

Т а б л и ц а 1 – Команды утилиты iptables

Команда	Пример	Пояснения
-A, --append	iptables -A INPUT	Добавляет новое правило в конец заданной цепочки
-D, --delete	iptables -D INPUT --dport 80 -j DROP iptables -D INPUT 1	Удаление правила из цепочки. Команда имеет два формата записи, первый – когда задается критерий сравнения с опцией -D (см. первый пример), второй – порядковый номер правила. Если задается критерий сравнения, то удаляется правило, которое имеет в себе этот критерий, если задается номер правила, то будет удалено правило с заданным номером. Счет правил в цепочках начинается с 1
-R, --replace	iptables -R INPUT 1 -s 192.168.0.1 -j DROP	Данная команда заменяет одно правило другим. Используется в основном во время отладки новых правил
-I, --insert	iptables -I INPUT 1 --dport 80 -j ACCEPT	Вставляет новое правило в цепочку. Число, следующее за именем цепочки, указывает номер правила, перед которым нужно вставить новое правило, другими словами число задает номер для вставляемого правила. В примере, указывается, что данное правило должно быть 1-м в цепочке INPUT
-L, --list	iptables -L INPUT	Вывод списка правил в заданной цепочке, в данном примере предполагается вывод правил из цепочки INPUT. Если имя цепочки не указывается, то выводится список правил для всех цепочек. Формат вывода зависит от наличия дополнительных ключей в команде, например, -n, -v, и пр.
-F, --flush	iptables -F INPUT	Удаление всех правил из заданной цепочки (таблицы). Если имя цепочки и таблицы не указывается, то удаляются все правила, во всех цепочках
-Z, --zero	iptables -Z INPUT	Обнуление всех счетчиков в заданной цепочке. Если имя цепочки не указывается, то подразумеваются все цепочки. При использовании ключа -v совместно с командой -L, на вывод будут поданы и состояния счетчиков пакетов, попавших под действие каждого правила. Допускается совместное использование команд -L и -Z. В этом случае будет выдан сначала список правил со счетчиками, а затем произойдет обнуление счетчиков
-N, --new-chain	iptables -N allowed	Создается новая цепочка с заданным именем в заданной таблице. В приведенном выше примере создается новая цепочка с именем allowed.

Окончание таблицы 1

Команда	Пример	Пояснения
		Имя цепочки должно быть уникальным и не должно совпадать с зарезервированными именами цепочек и действий (DROP, REJECT и т. п.)
-X, --delete-chain	iptables -X allowed	Удаление заданной цепочки из заданной таблицы. Удаляемая цепочка не должна иметь правил и не должно быть ссылок из других цепочек на удаляемую цепочку. Если имя цепочки не указано, то будут удалены все цепочки, определенные командой -N в заданной таблице
-P, --policy	iptables -P INPUT DROP	Определяет политику по умолчанию для заданной цепочки. Политика по умолчанию определяет действие, применяемое к пакетам, не попавшим под действие ни одного из правил в цепочке. В качестве политики по умолчанию допускается использовать DROP, ACCEPT и REJECT
-E, --rename-chain	iptables -E allowed disallowed	Команда -E выполняет переименование пользовательской цепочки. В примере цепочка allowed будет переименована в цепочку disallowed. Эти переименования не изменяют порядок работы, а носят только косметический характер

Команда должна быть указана всегда. Список доступных команд можно просмотреть с помощью команды `iptables -h` или, что то же самое, `iptables --help`. Некоторые команды могут использоваться совместно с дополнительными ключами.

7.5.4. Ключи утилиты iptables

В таблице 2 приводится список дополнительных ключей и описывается результат их действия.

Т а б л и ц а 2 – Ключи утилиты iptables

Ключ	Пример	Пояснения
-v, --verbose	--list, --append, --insert, --delete, --replace	Используется для повышения информативности вывода и, как правило, используется совместно с командой --list. В случае использования с командой --list, в вывод этой команды включаются: имя интерфейса, счетчики пакетов и байт для каждого правила. Формат вывода счетчиков предполагает вывод кроме цифр числа еще и символьные множители К (x1000), М (x1,000,000) и G (x1,000,000,000). Для того чтобы заставить команду --list выводить полное число (без употребления множителей) требуется применять ключ -x. Если ключ -v, --verbose используется с командами --append, --insert, --delete или --replace, то на вывод будет выдан подробный отчет о произведенной операции
-x, --exact	--list	Для всех чисел в выходных данных выводятся их точные значения без округления и без применения множителей К, М, G
-n, --numeric	--list	Iptables выводит IP-адреса и номера портов в числовом виде, предотвращая попытки преобразовать их в символические имена
--line-numbers	--list	Включает режим вывода номеров строк при отображении списка правил
-c, --set-counters	--insert, --append, --replace	Используется при создании нового правила для установки счетчиков пакетов и байт в заданное значение. Например, ключ --set-counters 20 4000 установит счетчик пакетов = 20, а счетчик байт = 4000
--modprobe	Любая команда	Определяет команду загрузки модуля ядра

7.5.5. Основные действия над пакетами в фильтре iptables

В таблице 3 приведены доступные над пакетами действия.

Т а б л и ц а 3 – Действия над пакетами iptables

Действие	Пояснения
ACCEPT	Пакет прекращает движение по цепочке (и всем вызвавшим цепочкам, если текущая цепочка была вложенной) и считается принятым, тем не менее, пакет продолжит движение по цепочкам в других таблицах и может быть отвергнут там
DROP	Отбрасывает пакет и iptables «забывает» о его существовании. Отброшенные пакеты прекращают свое движение полностью
RETURN	Прекращает движение пакета по текущей цепочке правил и производит возврат в вызывающую цепочку, если текущая цепочка была вложенной, или, если текущая цепочка лежит на самом верхнем уровне (например, INPUT), то к пакету будет применена политика по умолчанию

Окончание таблицы 3

Действие	Пояснения
LOG	Служит для журналирования отдельных пакетов и событий. В системный журнал могут заноситься заголовки IP-пакетов и другая интересующая информация
REJECT	Используется, как правило, в тех же самых ситуациях, что и DROP, но в отличие от DROP, команда REJECT выдает сообщение об ошибке на хост, передавший пакет
SNAT	Используется для преобразования сетевых адресов (Source Network Address Translation), т. е. изменение исходящего IP-адреса в IP-заголовке пакета
DNAT	Destination Network Address Translation используется для преобразования адреса места назначения в IP-заголовке пакета
MASQUERADE	В основе своей представляет то же самое, что и SNAT только не имеет ключа <code>--to-source</code> . Причиной тому то, что маскардинг может работать, например, с dialup подключением или DHCP, т. е. в тех случаях, когда IP-адрес присваивается устройству динамически. Если используется динамическое подключение, то нужно использовать маскардинг, если же используется статическое IP-подключение, то лучшим выходом будет использование действия SNAT
REDIRECT	Выполняет перенаправление пакетов и потоков на другой порт той же самой машины. К примеру, можно пакеты, поступающие на HTTP порт перенаправить на порт HTTP проху. Действие REDIRECT очень удобно для выполнения «прозрачного» проксирования (transparent проху), когда компьютеры в локальной сети даже не подозревают о существовании прокси
TTL	Используется для изменения содержимого поля «время жизни» (Time To Live) в IP-заголовке. Один из вариантов применения этого действия – это устанавливать значение поля «Time To Live» во всех исходящих пакетах в одно и то же значение. Если установить на все пакеты одно и то же значение TTL, то тем самым можно лишить провайдера одного из критериев определения того, что подключение к Интернету разделяется между несколькими компьютерами. Для примера можно привести число «TTL = 64», которое является стандартным для ядра Linux

7.5.6. Основные критерии пакетов в фильтре iptables

В таблице 4 приведены возможные критерии для фильтрации пакетов в фильтре iptables.

Т а б л и ц а 4 – Критерии пакетов в фильтре iptables

Критерий	Пояснения
-p, --protocol	Используется для указания типа протокола. Примерами протоколов могут быть TCP, UDP и ICMP. Список протоколов можно посмотреть в файле <code>/etc/protocols</code> . Прежде всего, в качестве имени протокола в данный критерий можно передавать три вышеупомянутых протокола, а также ключевое слово ALL. В качестве протокола допускается передавать число – номер протокола

Продолжение таблицы 4

Критерий	Пояснения
-s, --src, --source	IP-адрес(а) источника пакета. Адрес источника может указываться без маски или префикса (например, 192.168.1.1), тогда подразумевается единственный IP-адрес. Можно указать адрес в виде address/mask, например, как 192.168.0.0/255.255.255.0, или более современным способом 192.168.0.0/24, т. е. фактически определяя диапазон адресов. Символ «!», установленный перед адресом, означает логическое отрицание, т. е. --source ! 192.168.0.0/24 означает любой адрес кроме адресов 192.168.0.x
-d, --dst, --destination	IP-адрес(а) получателя. Имеет синтаксис схожий с критерием --source, за исключением того, что подразумевает адрес места назначения. Точно так же может определять, как единственный IP-адрес, так и диапазон адресов. Символ «!» используется для логической инверсии критерия
-i, --in-interface	Интерфейс, с которого был получен пакет. Использование этого критерия допускается только в цепочках INPUT, FORWARD и PREROUTING, в любых других случаях будет вызывать сообщение об ошибке
-o, --out-interface	Задаёт имя выходного интерфейса. Этот критерий допускается использовать только в цепочках OUTPUT, FORWARD и POSTROUTING, в противном случае будет генерироваться сообщение об ошибке
-f, --fragment	Правило распространяется на все фрагменты фрагментированного пакета, кроме первого, сделано это потому, что нет возможности определить исходящий/входящий порт для фрагмента пакета, а для ICMP-пакетов определить их тип. С помощью фрагментированных пакетов могут производиться атаки на межсетевой экран, так как фрагменты пакетов могут не отлавливаться другими правилами
-sport, --source-port	Исходный порт, с которого был отправлен пакет. В качестве параметра может указываться номер порта или название сетевой службы. Соответствие имен сервисов и номеров портов можно найти в файле /etc/services. При указании номеров портов правила обрабатываются несколько быстрее
--dport, --destination-port	Порт, на который адресован пакет. Аргументы задаются в том же формате, что и для --source-port
--tcp-flags	SYN, ACK, FIN SYN определяет маску и флаги tcp-пакета. Пакет считается удовлетворяющим критерию, если из перечисленных флагов в первом списке в единичное состояние установлены флаги из второго списка. В качестве аргументов критерия могут выступать флаги SYN, ACK, FIN, RST, URG, PSH, а также зарезервированные идентификаторы ALL и NONE. ALL означает ВСЕ флаги, а NONE – НИ ОДИН флаг. Так, критерий --tcp-flags ALL NONE означает, что все флаги в пакете должны быть сброшены. Символ «!» означает инверсию критерия. Имена флагов в каждом списке должны разделяться запятыми, пробелы служат для разделения списков
--icmp-type	Тип сообщения ICMP определяется номером или именем. Числовые значения определяются в RFC 792. Чтобы получить список имен ICMP значений выполните команду iptables --protocol icmp --help. Символ «!» инвертирует критерий, например, --icmp-type ! 8

Окончание таблицы 4

Критерий	Пояснения
--state	Для использования данного критерия в правиле перед --state нужно явно указать -m state. Проверяется признак состояния соединения. Можно указывать 4 состояния: INVALID, ESTABLISHED, NEW и RELATED. INVALID подразумевает, что пакет связан с неизвестным потоком или соединением и возможно содержит ошибку в данных или в заголовке. ESTABLISHED указывает на то, что пакет принадлежит уже установленному соединению, через которое пакеты идут в обоих направлениях. NEW подразумевает, что пакет открывает новое соединение или пакет принадлежит однонаправленному потоку. RELATED указывает на то, что пакет принадлежит уже существующему соединению, но при этом он открывает новое соединение. Примером может служить передача данных по FTP, или выдача сообщения ICMP об ошибке, которое связано с существующим TCP или UDP соединением. Признак NEW – это не то же самое, что установленный бит SYN в пакетах TCP, посредством которых открывается новое соединение, и подобного рода пакеты могут быть потенциально опасны в случае, когда для защиты сети используется один сетевой экран

7.5.7. Модули iptables

Возможности фильтрации пакетов расширяются через модули. Модули подключаются автоматически при выборе протокола (-p/--protocol) или вручную опцией -m/--match, после которой следует имя подключаемого модуля и его опции.

Справку по опциям модуля можно получить с помощью ключа -h/--help. Допустимо указание нескольких модулей. Результаты фильтрации, выдаваемые модулем, можно инвертировать указав ! перед его именем.

В таблице 5 приведены возможные критерии для фильтрации пакетов в фильтре iptables.

Т а б л и ц а 5 – Модули iptables

Модуль	Опции	Пояснение
connlimit	[!] --connlimit-above n – пакет подойдет под описание, если количество одновременных подключений на данный момент больше (меньше), чем n; --connlimit-mask bits – позволяет задать маску блока адресов	Позволяет задавать возможное количество одновременных подключений к машине от заданного IP или блока адресов. Пример. Допускать не больше 20 соединений на порт 80 с одного хоста iptables -A INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above 20 -j REJECT --reject-with tcp-reset

Продолжение таблицы 5

Модуль	Опции	Пояснение
icmp	--icmp-type [!] тип – тип ICMP в виде числа или имени в соответствии с iptables -p icmp -h	Расширение загружается при указании -protocol icmp.
iprange	[!]--src-range ip-ip – диапазон IP-адресов отправителя; [!]--dst-range ip-ip – диапазон IP-адресов получателя	Выделяет не один адрес, как --src, а все адреса от ip1 до ip2
ipv4options (не подключен по умолчанию)	--flags [!]параметр[,...] – сопоставляет наличие/отсутствие(!) параметров (по имени или номеру); --any – хотя бы один --flags ipv4 или их комбинация. Примеры параметров: - ssrr – strict source routing – маршрутизация указывается источником; - lsrr – loose source routing – свободная маршрутизация; - rr – record-route – запись маршрута; - ra – оповещения маршрутизатора; - srr – source-routing – режим маршрутизации; - ts – timestamp	Результат теста зависит от параметров заголовка IPv4, таких как параметры маршрутизации, запись маршрута, запрос времени, оповещение маршрутизатора. Примеры. Отбрасывать пакеты с флагом ssrr: iptables -A INPUT -m ipv4options --flags ssrr -j DROP Отбрасывать пакеты любые пакеты ipv4: iptables -A INPUT -m ipv4options --any -j DROP
length	--length [!] размер[:размер]	Позволяет проверять размеры пакетов (точно или по диапазону)
limit	--limit частота – максимальная средняя частота положительных результатов. После числа можно указывать единицы: `/second', `/minute', `/hour', `/day'; значение по умолчанию – 3/hour. --limit-burst number – ограничение на исходное число пропускаемых пакетов (по умолчанию – 5)	Выдает положительный результат с фиксированной частотой. Правило использующее этот модуль будет выполняться до момента достижения лимита (и наоборот, если указан «!»). Может использоваться вместе с целью LOG для получения ограниченного протоколирования
limit	--limit частота – максимальная средняя частота положительных результатов. После числа можно указывать единицы: `/second', `/minute', `/hour', `/day'; значение по умолчанию – 3/hour. --limit-burst number – ограничение на исходное число пропускаемых пакетов (по умолчанию – 5)	Выдает положительный результат с фиксированной частотой. Правило использующее этот модуль будет выполняться до момента достижения лимита (и наоборот, если указан «!»). Может использоваться вместе с целью LOG для получения ограниченного протоколирования

Окончание таблицы 5

Модуль	Опции	Пояснение
multiport	<pre>[!]<code>--source-ports</code> port1,port2,port3:port4 - исходный порт равен одному из указанных; [!]<code>--destination-ports</code> port1,port2,port3:port4 - порт назначения равен одному из указанных; [!]<code>--ports</code> port1,port2,port3:port4 - исходный и порт назначения и равны одному из указанных</pre>	Позволяет указывать в тексте правила несколько (до 15) портов и диапазонов портов (порт:порт). Используется только вместе с <code>-p tcp</code> или <code>-p udp</code>
state	<code>--state</code> состояния – список фильтруемых состояний через запятую (см. таблицу 4)	Проверяется признак состояния соединения (state)
string	<pre><code>--algo</code> bm kmp – стратегия сравнения/поиска (bm = Boyer- Moore, kmp = Knuth-Pratt-Morris); <code>--from</code> позиция – позиция в данных, с которой следует начинать поиск. Значение по умолчанию – 0. <code>--to</code> позиция – позиция в данных, при достижении которой следует прекращать поиск. Значение по умолчанию – размер пакета; <code>--string</code> последовательность – последовательность символов, которую следует искать в пакете; <code>--hex-string</code> pattern – последовательность символов, которую следует искать в пакете (в шестнадцатеричном представлении)</pre>	Позволяет выполнять фильтрацию пакетов, основываясь на анализе содержимого области данных пакета
tcp	см. таблицу 4	Это расширение загружается при указании <code>--protocol tcp</code>
u32	<code>--u32 "Start&Mask=Range"</code>	Позволяет извлекать из пакета данные размером до 4 байт, применять к ним операции логического И, сдвига, и проверять принадлежность получающихся данных определенным диапазонам. В простейшей форме, u32 вырезает блок из 4 байт начиная со Start, применяет к ним маску Mask и сравнивает результат с Range-m u32
udp	см. таблицу 4	Это расширение загружается при указании <code>--protocol udp</code>

Список доступных модулей можно просмотреть, выполнив команду:

```
# ls /lib/modules/$(uname -r)/kernel/net/netfilter/
```

Загруженные модули iptables можно найти в записи файловой системы proc

```
/proc/net/ip_tables_matches:
```

```
# cat /proc/net/ip_tables_matches
```

Загрузка модуля:

```
# modprobe <модуль>
```

Например:

```
# modprobe xt_limit
```

```
# modprobe xt_length
```

```
# modprobe xt_u32
```

7.5.8. Использование фильтра iptables

ОС Альт СП уже включает в себя предустановленный iptables. Для его настройки рекомендуется использовать возможности системы настройки сети /etc/net (см. п. 8.2.1).

7.5.9. Примеры команд iptables

Список текущих правил:

```
iptables -nvL --line-numbers
```

Очистка всех правил:

```
iptables -F
```

Очистка правил в цепочке:

```
iptables -F INPUT
```

Удаления пятого правила в цепочке INPUT:

```
iptables -D INPUT 5
```

7.5.9.1. Фильтрация по источнику пакета

Для фильтрации по источнику используется опция `-s`.

Например, запретить все входящие пакеты с узла 192.168.1.95:

```
iptables -A INPUT -s 192.168.1.95 -j DROP
```

Можно использовать доменное имя для указания адреса хоста:

```
iptables -A INPUT -s test.host.net -j DROP
```

Также можно указать целую подсеть:

```
iptables -A INPUT -s 192.168.1.0/24 -j DROP
```

Можно использовать отрицание (знак «!»). Например, все пакеты с хостов отличных от 192.168.1.96 будут уничтожаться:

```
iptables -A INPUT ! -s 192.168.1.96 -j DROP
```

Разрешить трафик по localhost:

```
iptables -A INPUT -i lo -j ACCEPT
```

Записывать в журнал попытки спуфинга с префиксом "IP_SPOOF A: " и запретить соединение:

```
iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j LOG --log-prefix "IP_SPOOF A: "
```

```
iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
```

7.5.9.2. Фильтрация по адресу назначения

Для фильтрации по адресу назначения используется опция `-d`.

Например, запретить все исходящие пакеты на хост 192.168.1.95:

```
iptables -A OUTPUT -d 192.168.156.156 -j DROP
```

Запретить доступ к ресурсу `vk.com`:

```
iptables -A OUTPUT -d vk.com -j REJECT
```

Как и в случае с источником пакета, можно использовать адреса подсети и доменные имена. Отрицание также работает.

7.5.9.3. Фильтрация по протоколу

Опция `-p` указывает на протокол. Можно использовать `all`, `icmp`, `tcp`, `udp` или номер протокола (из `/etc/protocols`).

Разрешить входящие эхо-запросы:

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

7.5.9.4. Фильтрация по порту источника

Разрешить все исходящие пакеты с порта 80:

```
iptables -A INPUT -p tcp --sport 80 -j ACCEPT
```

Заблокировать все входящие запросы порта 80:

```
iptables -A INPUT -p tcp --dport 80 -j DROP
```

Для указания порта нужно указать протокол (`tcp` или `udp`). Можно использовать отрицание.

Открыть диапазон портов:

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport
7000:7010 -j ACCEPT
```

7.5.9.5. Фильтрация по порту назначения

Разрешить подключения по HTTP:

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Разрешить подключения по SSH:

```
iptables -A INPUT -p tcp -i eth0 --dport 22 -j ACCEPT
```

Разрешить получать данные от DHCP-сервера:

```
iptables -A INPUT -p UDP --dport 68 --sport 67 -j ACCEPT
```

Разрешить rsync с определенной сети:

```
iptables -A INPUT -i eth0 -p tcp -s 192.168.1.0/24 --dport 873 -m
state --state NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp --sport 873 -m state --state
ESTABLISHED -j ACCEPT
```

Разрешить IMAP/IMAP2 трафик:

```
iptables -A INPUT -i eth0 -p tcp --dport 143 -m state --state
NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp --sport 143 -m state --state
ESTABLISHED -j ACCEPT
```

Разрешить исходящие HTTP, FTP, DNS, SSH, SMTP:

```
iptables -A OUTPUT -p TCP -o eth0 --dport 443 -j ACCEPT
```

```
iptables -A OUTPUT -p TCP -o eth0 --dport 80 -j ACCEPT
```

```
iptables -A OUTPUT -p TCP -o eth0 --dport 53 -j ACCEPT
```

```
iptables -A OUTPUT -p UDP -o eth0 --dport 53 -j ACCEPT
```

```
iptables -A OUTPUT -p TCP -o eth0 --dport 25 -j ACCEPT
```

```
iptables -A OUTPUT -p TCP -o eth0 --dport 22 -j ACCEPT
```

```
iptables -A OUTPUT -p TCP -o eth0 --dport 21 -j ACCEPT
```

Разрешить mysql для локальных пользователей:

```
iptables -I INPUT -p tcp --dport 3306 -j ACCEPT
```

Разрешить CUPS (сервер печати, порт 631) для пользователей внутри локальной сети:

```
iptables -A INPUT -s 192.168.1.0/24 -p udp -m udp --dport 631 -j ACCEPT
```

```
iptables -A INPUT -s 192.168.1.0/24 -p tcp -m tcp --dport 631 -j ACCEPT
```

Разрешить синхронизацию времени NTP для пользователей внутри локальной сети:

```
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p \
udp --dport 123 -j ACCEPT
```

7.5.9.6. Перенаправление портов

Направим трафик с порта 442 на 22, это значит, что входящие ssh-соединения могут быть принятыми с порта 422 и 22:

```
iptables -t nat -A PREROUTING -p tcp -d 192.168.1.15 --dport 422\
-j DNAT --to 192.168.1.15:22
```

Также надо разрешить входящие соединения с порта 422:

```
iptables -A INPUT -i eth0 -p tcp --dport 422 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 422 -m state --state
ESTABLISHED -j ACCEPT
```

Как и в случае с портом источника, нужно указать протокол. Можно использовать отрицание.

7.5.9.7. Ограничение по локальным пользователям

Ограничение по локальным пользователям нельзя поручить внешнему межсетевому экрану, так как он не имеет этой информации.

Отбросить все пакеты, исходящие от процессов пользователя с UID=500:

```
# iptables -A OUTPUT -m owner --uid-owner 500 -j DROP
```

Попытка соединения с удаленным узлом, пользователя с UID=500:

```
# su - test
$ wget ya.ru
--2017-03-07 13:53:14-- http://ya.ru/
Распознается ya.ru (ya.ru)... ошибка: Имя или служба не известны.
wget: не удастся разрешить адрес «ya.ru»
```

Попытка соединения с локальным узлом, пользователя с UID=500:

```
# su - test
$ wget localhost
--2017-03-07 13:55:20-- http://localhost/
Распознается localhost (localhost)... 127.0.0.1
Подключение к localhost (localhost)|127.0.0.1|:80... ^C
```

7.5.9.8. Фильтрация по содержимому пакета

Отбросить все пакеты, данные в которых содержат подстроку virus:

```
# iptables -I INPUT -j DROP -p tcp -s 0.0.0.0/0 -m string --algo
kmp --string "virus "
```

Записывать в журнал пакеты со строкой secret внутри:

```
# iptables -A INPUT -m string --algo kmp --string "secret" \
-j LOG --log-level info --log-prefix "SECRET "
```

Просмотр журнала:

```
# journalctl |grep SECRET
апр 03 16:47:18 host-15.localdomain kernel: SECRET IN=eth0 OUT=
MAC=08:00:27:d5:f3:78:74:e5:0b:3e:2c:88:08:00 SRC=192.168.3.101 DST=192.168.3.104
LEN=47 TOS=0x00 PREC=0x00 TTL=64 ID=30811 DF PROTO=TCP SPT=53878 DPT=8080 WINDOW=229
RES=0x00 ACK PSH URGP=0
апр 03 16:58:47 host-15.localdomain kernel: SECRET IN=eth0 OUT=
MAC=08:00:27:d5:f3:78:74:e5:0b:3e:2c:88:08:00 SRC=192.168.3.101 DST=192.168.3.104
LEN=47 TOS=0x00 PREC=0x00 TTL=64 ID=38640 DF PROTO=TCP SPT=54510 DPT=8080 WINDOW=229
RES=0x00 ACK PSH URGP=0
```

Статистика правил iptables и счетчики обработанных пакетов в цепочке

INPUT:

```
# iptables -nvL INPUT --line-numbers
Chain INPUT (policy ACCEPT 1711 packets, 1400K bytes)
num pkts bytes target prot opt in out source destination
1 47 49550 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0
STRING match "virus" ALGO name kmp TO 65535
2 0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0
STRING match "virus " ALGO name kmp TO 65535
3 17 66141 LOG tcp -- * * 0.0.0.0/0 0.0.0.0/0
STRING match "secret" ALGO name kmp TO 65535 LOG flags 0 level 6 prefix "SECRET "
```

7.6. Настройка экспорта аудита на удаленный узел

Для настройки экспорта аудита на удаленный узел нужно настроить OpenVPN-соединение (см. подробнее п. 8.4) между принимающей и передающей стороной, настроить межсетевой экран и внести изменения в конфигурационные файлы аудита.

На принимающей стороне – сервер:

- 1) скопировать файл /usr/share/doc/openvpn-*/server.conf (* – версия openvpn) в директорию /etc/openvpn/ для его редактирования и последующего запуска сервера VPN;
- 2) в скопированном на предыдущем этапе файле server.conf, проверьте имена и пути файлов сертификата сервера (.crt), его ключа (.key), а также

сертификата CA (.crt) и DH (dh*.pem), а также закомментировать параметр `proto udp` и раскомментировать `proto tcp`;

3) установить утилиту `easy-rsa`:

```
# apt-get install easy-rsa
```

4) сгенерировать все ключи и сертификаты. Ввести для них пароли:

```
# easyrsa init-pki
# easyrsa build-ca
# easyrsa build-server-full server
# easyrsa build-client-full client1
# easyrsa gen-dh
# easyrsa sign-req client client1
# easyrsa sign-req server server
```

5) перенести полученные ключи и сертификаты в каталог `/etc/openvpn/keys/`.

Настройка OpenVPN-клиента на передающей стороне:

1) скопировать из `/usr/share/doc/openvpn-*/client.conf` (* – версия `openvpn`) в директорию `/etc/openvpn/` для его редактирования и последующего запуска клиента VPN;

2) скопировать ранее сгенерированные ключи и сертификаты в директорию `/etc/openvpn/keys/` и указать их в `client.conf`;

3) открыть `client.conf` найти строку `remote` и изменить ее на:

```
remote 10.10.3.87 1194
```

где `10.10.3.87` – это IP-адрес сервера на внешнем интерфейсе принимающей стороны.

Также, закомментировать параметр `proto udp` и раскомментировать `proto tcp`.

Отредактировать конфигурационные файлы аудита:

- на принимающей стороне в файле `/etc/audit/auditd.conf` исправить параметр `tcp_listen_port=1060`;

- на передающей стороне в файле `/etc/audit/audisp-remote.conf` исправить параметры:

```
remote_server = 10.8.0.1
port = 1060
#queue_error_action
```

где `10.8.0.1` – IP-адрес сервера `vpn` на созданном интерфейсе-туннеле принимающей стороны;

- на передающей стороне изменить параметр: `active = yes` в файле `/etc/audit/plugins.d/au-remote.conf`;

- перезапустить систему на принимающей и передающей сторонах.

Запустить сервер на принимающей стороне:

```
# openvpn /etc/openvpn/server.conf
```

Запустить OpenVPN-клиент на передающей стороне:

```
# openvpn /etc/openvpn/client.conf
```

Команды установки правила пропуска tcp пакетов с портом назначения 1060 только через устройство vpn (например, tun0) на принимающей стороне:

```
# iptables -A INPUT -p tcp --dport 1060 -i tun0 -j ACCEPT
```

```
# iptables -A INPUT -p tcp --dport 1060 -j DROP
```

Для проверки аудита передающей стороны на принимающей стороне выполнить команду:

```
# ausearch -hn имя_передающей_стороны
```

Если ничего не отображается, то, возможно, было указано неверное имя передающей стороны. Для проверки, что лог приходит, можно, например, авторизоваться на передающей стороне, а затем проверить лог на принимающей стороне командой:

```
# ausearch -m USER_AUTH
```

Имя передающей стороны будет указано в параметре `hostname` лога.

7.7. Настройка системы сигнализации на основе icinga

Icinga2 – система мониторинга с открытым исходным кодом. Изначально была создана как ответвление от системы мониторинга Nagios.

С точки зрения клиент-серверной архитектуры в Icinga2 различается три роли (рис. 82):

- мастер (Master) – серверный экземпляр Icinga2 на верхнем уровне иерархии. Мастер-узел в простых развертываниях один, в высоко-доступных развертываниях Мастер-узлов может быть несколько (кластер);

- спутник (Satellite) – вспомогательный узел, который способен выступать в качестве распространителя конфигурации Icinga для агентов и позволяет агентам не замечать недоступности основного Мастер-узла. Спутники могут

быть полезны в больших развертываниях, где требуется децентрализация основной конфигурации, например, когда требования к мониторингу одних и тех же служб различаются на разных площадках;

- агент (Agent) – клиентский узел, который получает конфигурацию мониторинга с родительского узла (Мастер или Спутник).

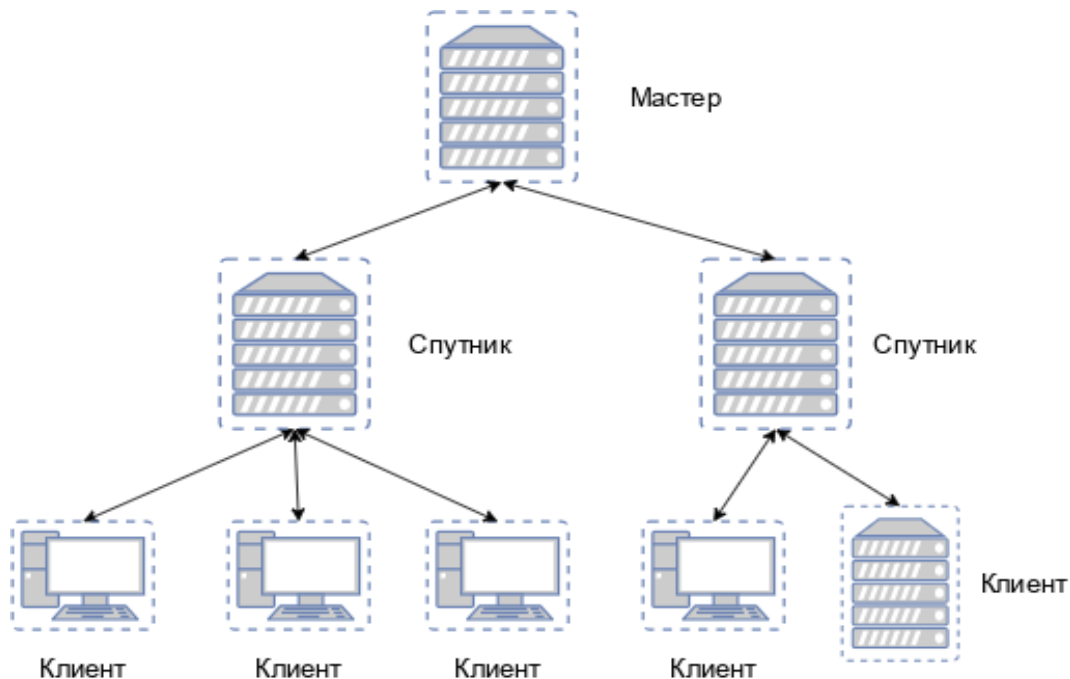


Рис. 82 – Роли Icinga2

В данном руководстве рассмотрена простая конфигурация с единственным мастер-узлом и некоторым количеством узлов агентов без участия узлов спутников.

Иерархия Icinga2 состоит из так называемых зон. Существуют определенные ограничения для дочерних зон, например, их участникам не разрешено отправлять команды конфигурации членам родительской зоны. И, наоборот, иерархия доверия позволяет главной зоне отправлять файлы конфигурации в вспомогательную зону.

Узлы агентов также имеют свою собственную уникальную зону. В качестве имени зоны необходимо использовать полное доменное имя. Узлы, являющиеся членами зоны, являются так называемыми объектами Endpoint (конечными точками).

Сервер Icinga2 – это главный сервер, который собирает все данные мониторинга и отображает их. Главный сервер состоит из процесса-демона

(Icinga2), который работает в фоновом режиме, и веб-приложения (Icingaweb2), которое используется для отображения результатов из браузера.

Примечание. Необходимо обеспечить взаимно однозначное прямое и обратное преобразование имен для всех узлов. Можно использовать DNS или обойтись соответствующими записями в локальных файлах `/etc/hosts`, например:

```
# echo "192.168.0.170 master1.test.alt" >> /etc/hosts
# echo "192.168.0.151 agent1.test.alt" >> /etc/hosts
# echo "192.168.0.152 agent2.test.alt" >> /etc/hosts
```

7.7.1. Настройка сервера мониторинга

7.7.1.1. Установка Icinga2

Установить пакеты:

```
# apt-get install icinga2 icingaweb2 icingaweb2-nginx icingaweb2-
cli icinga2-doc icingaweb2-php-fpm icingaweb2-style-altsp nagwad-
icinga-master
```

Примечание. Шаг установки пакетов `icinga2` можно пропустить, если при установке ОС на этапе «Установка системы» был выбран блок «Рабочее место контролера событий безопасности» (рис. 83).

Примечание. Все указанные пакеты доступны на ОС Альт СП Рабочая станция.

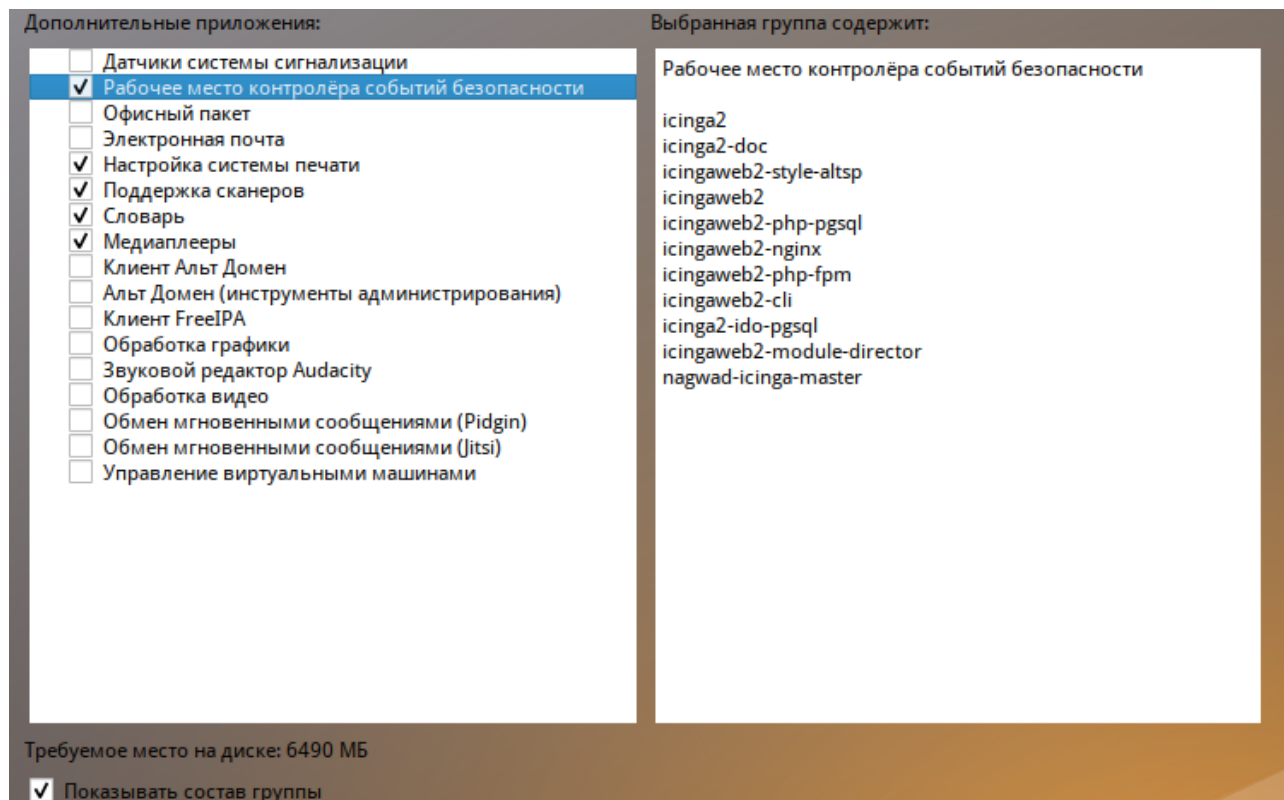


Рис. 83 – Блок «Рабочее место контролера событий безопасности»

Примечание. Начиная с версии `php 8.0`, пакеты модулей именуются

следующим образом:

```
php<мажорная>.<минорная версии>-<имя модуля>.
```

В данной инструкции используется версия php 8.3.

7.7.1.2. Установка и конфигурация БД

В процессе установки должна быть создана база данных для вывода данных icinga2 и для веб-интерфейса icinga2. Можно использовать базу данных MySQL или PostgreSQL.

7.7.1.2.1. PostgreSQL

Установить PostgreSQL и IDO-модули для PostgreSQL:

```
# apt-get install postgresql16-server icinga2-ido-pgsql
icingaweb2-php-pgsql
```

Примечание. В командах руководства используется версия postgresql 16.

Подготовить к запуску и настроить службы PostgreSQL:

- создать системные базы данных (пароль пользователя PostgreSQL необходимо запомнить):

```
# /etc/init.d/postgresql initdb
```

Введите новый пароль суперпользователя:

Повторите его:

- включить по умолчанию и запустить службу:

```
# systemctl enable --now postgresql
```

Создать базы данных для icinga2:

- создать пользователя icinga (пароль необходимо запомнить) и базы данных icinga и icingaweb (при запросе «Пароль» следует ввести пароль пользователя postgresql, созданный при создании системных баз данных):

```
# su - postgres -s /bin/sh -c 'createuser --no-superuser --no-createdb --no-createrole --encrypted --pwprompt icinga'
```

Введите пароль для новой роли:

Повторите его:

Пароль:

```
# su - postgres -s /bin/sh -c 'createdb -O icinga icinga'
```

Пароль:

```
# su - postgres -s /bin/sh -c 'createdb -O icinga icingaweb'
```

Пароль:

- импортировать в базу icinga схему Icinga2 из IDO модуля:

```
# su - postgres -s /bin/sh -c 'psql -U icinga -f
/usr/share/icinga2-ido-pgsql/schema/pgsql.sql icinga'
```

Пароль пользователя icinga:

Внести информацию о пользователе базы данных icinga в файл /etc/icinga2/features-enabled/ido-pgsql.conf, например:

```
object IdoPgsqlConnection "ido-pgsql" {
    user = "icinga"
    password = "new_icinga"
    host = "localhost"
    database = "icinga"
}
```

7.7.1.2.2. MySQL/MariaDB

Установить сервер MariaDB и IDO-модули для MySQL:

```
# apt-get install mariadb-server icingaweb2-php-mysql icinga2-ido-mysql
```

Примечание. Пакет mariadb-server доступен в репозитории или на компакт-диске дистрибутива ОС Альт СП Сервер.

Включить по умолчанию и запустить службу mysqld:

```
# systemctl enable --now mysqld
```

Создать базы данных icinga и icingaweb и пользователя icinga (пароль пользователя необходимо запомнить):

```
$ mysql -uroot -p
Enter password:
MariaDB [(none)]> create database icinga CHARACTER SET utf8
COLLATE utf8_general_ci;
MariaDB [(none)]> create database icingaweb CHARACTER SET utf8
COLLATE utf8_general_ci;
MariaDB [(none)]> grant all privileges on icinga.* to
icinga@localhost identified by '<пароль>';
MariaDB [(none)]> grant all privileges on icingaweb.* to
icinga@localhost identified by '<пароль>';
MariaDB [(none)]> quit;
```

Импортировать в базу icinga схему Icinga2 из IDO модуля (по запросу ввести пароль пользователя icinga):

```
$ mysql -uicinga -p icinga < /usr/share/icinga2-ido-
mysql/schema/mysql.sql
Enter password:
```

Внести информацию о пользователе базы данных icinga в файл /etc/icinga2/features-enabled/ido-mysql.conf, например:

```
object IdoMysqlConnection "ido-mysql" {
```

```

user = "icinga"
password = "new_icinga"
host = "localhost"
database = "icinga"
}

```

7.7.1.3. Запуск служб

Запустить и включить по умолчанию службы:

```

# systemctl enable --now php8.3-fpm.service
# systemctl enable --now nginx
# systemctl enable --now icinga2

```

7.7.1.4. Веб-интерфейс IcingaWeb2

Icinga Web 2 – веб-интерфейс панели наблюдения Icinga2.

Настроить Icinga Web 2 можно с помощью мастера настройки Icinga Web 2, который доступен при первом посещении Icinga Web 2 в веб-браузере.

7.7.1.4.1. Предварительная настройка

Создать каталог конфигурации:

```

# icingacli setup config directory --group icingaweb2
Successfully created configuration directory /etc/icingaweb2

```

При использовании веб-настройки потребуется пройти аутентификацию с использованием токена. Для генерации токена выполнить команду:

```

# icingacli setup token create
The newly generated setup token is: 5b24be3ace879072

```

Далее необходимо настроить REST API для связи Icinga и Icinga Web 2:

```

# icinga2 api setup
information/cli: Generating new CA.
information/base:      Writing      private      key      to
'/var/lib/icinga2/ca//ca.key'.
information/base:      Writing      X509      certificate  to
'/var/lib/icinga2/ca//ca.crt'.
information/cli:      Generating      new      CSR      in
'/var/lib/icinga2/certs//master1.test.alt.csr'.
information/base:      Writing      private      key      to
'/var/lib/icinga2/certs//master1.test.alt.key'.
information/base:      Writing      certificate  signing  request  to
'/var/lib/icinga2/certs//master1.test.alt.csr'.
information/cli: Signing CSR with CA and writing certificate to
'/var/lib/icinga2/certs//master1.test.alt.crt'.
information/pki:      Writing      certificate  to      file
'/var/lib/icinga2/certs//master1.test.alt.crt'.
information/cli:      Copying      CA      certificate  to
'/var/lib/icinga2/certs//ca.crt'.

```

```

information/cli: Adding new ApiUser 'root' in
'/etc/icinga2/conf.d/api-users.conf'.
information/cli: Reading '/etc/icinga2/icinga2.conf'.
information/cli: Enabling the 'api' feature.
Enabling feature api. Make sure to restart Icinga2 for these
changes to take effect.
information/cli: Updating 'NodeName' constant in
'/etc/icinga2/constants.conf'.
information/cli: Created backup file
'/etc/icinga2/constants.conf.orig'.
information/cli: Updating 'ZoneName' constant in
'/etc/icinga2/constants.conf'.
information/cli: Backup file '/etc/icinga2/constants.conf.orig'
already exists. Skipping backup.
Done.

```

Now restart your Icinga2 daemon to finish the installation!

Эта команда сгенерирует сертификаты, API-пользователя root с автогенерированным паролем (см. /etc/icinga2/conf.d/api-users.conf).

Для применения изменений перезагрузить icinga2:

```
# systemctl restart icinga2.service
```

7.7.1.4.2. Настройка Nginx

По умолчанию веб-интерфейс icinga2 доступен только с localhost. Для изменения этого поведения следует внести изменения в файл /etc/nginx/sites-available.d/icingaweb2.conf. Например, для возможности доступа к веб-интерфейсу по адресу http://192.168.0.170:81/icingaweb2 необходимо в раздел server добавить строку:

```
listen 192.168.0.170:81;
```

и перезагрузить Nginx:

```
# systemctl restart nginx
```

Примечание. Если обращение к веб-интерфейсу IcingaWeb2 происходит по IP-адресу, а не по имени, то для того чтобы Nginx при старте (например, после перезагрузки системы) не ругался на несуществующий IP, нужно разрешить поддержку нелокальных адресов. Для этого в файл /etc/sysctl.conf следует дописать строку:

```
net.ipv4.ip_nonlocal_bind = 1
```

и перезагрузить конфигурацию sysctl:

```
# sysctl -p /etc/sysctl.conf
```

Для настройки https можно создать файл `icingaweb2-ssl.conf` и дописать в него ранее сгенерированные сертификаты. Например:

1) создать новый файл конфигурации:

```
# cp /etc/nginx/sites-available.d/icingaweb2.conf
/etc/nginx/sites-available.d/icingaweb2-ssl.conf
```

2) внести изменения в файл:

```
server {
    listen 81;
    server_name master1.test.alt localhost localhost.localdomain;
    rewrite ^ https://$host$request_uri? permanent;
}
server {
    listen 443 ssl;
    server_name master1.test.alt localhost localhost.localdomain;
    ssl_certificate
/var/lib/icinga2/certs/master1.test.alt.crt;
    ssl_certificate_key
/var/lib/icinga2/certs/master1.test.alt.key;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
    ssl_ciphers HIGH:!aNULL:!MD5;
    location ~ ^/icingaweb2/index\.php(.*)$ {
        fastcgi_pass unix:/var/run/php8.3-fpm/icingaweb2.socket;
        fastcgi_index index.php;
        include fastcgi_params;
        fastcgi_param SCRIPT_FILENAME
/usr/share/icingaweb2/public/index.php;
        fastcgi_param ICINGAWEB_CONFIGDIR /etc/icingaweb2;
        fastcgi_param REMOTE_USER $remote_user;
    }
    location ~ ^/icingaweb2(.+)? {
        alias /usr/share/icingaweb2/public;
        index index.php;
        try_files $1 $uri $uri/ /icingaweb2/index.php$is_args$args;
    }
}
```

3) отключить старую конфигурацию и включить новую:

```
# rm -rf /etc/nginx/sites-enabled.d/icingaweb2.conf
# ln -s /etc/nginx/sites-available.d/icingaweb2-ssl.conf
/etc/nginx/sites-enabled.d/icingaweb2-ssl.conf
```

4) перезагрузить Nginx:

```
# systemctl restart nginx
```

В данном примере веб-интерфейс будет доступен по
<https://master1.test.alt>.

7.7.1.4.3. Настройка рабочего места администратора безопасности

Под рабочим местом администратора безопасности подразумевается веб-интерфейс Icinga Web 2. Мастер первоначальной настройки будет предложен после перехода по адресу `http://localhost:81/icingaweb2/` (URL может быть иным в зависимости от изменений, сделанных при настройке Nginx).

На первом шаге настройки Icinga Web 2 необходимо ввести ранее полученный токен (рис. 84) и нажать кнопку «Далее».

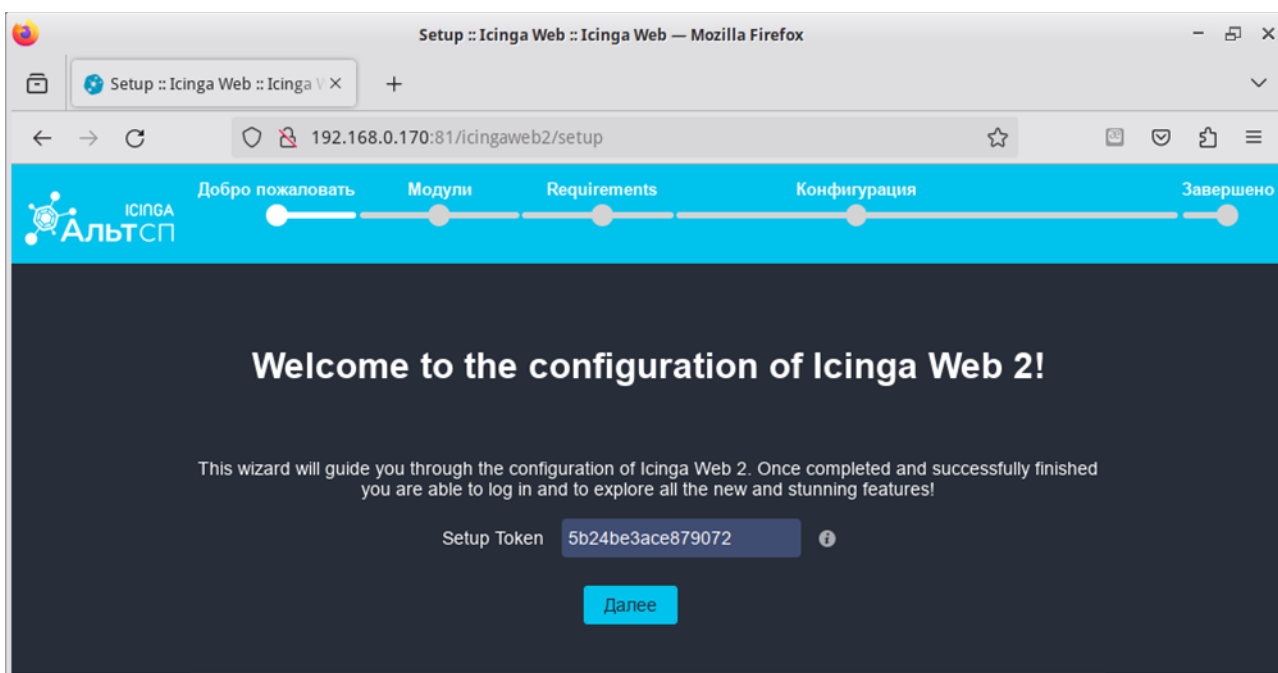


Рис. 84 – Конфигурирование Icinga Web 2

Примечание. Посмотреть текущий токен можно, выполнив команду:
`# icingacli setup token show`
5b24be3ace879072

На следующем шаге представлен набор модулей, которые обнаружила Icinga Web 2. Можно оставить значение по умолчанию (отмечен только модуль Monitoring) и нажать кнопку «Далее» (рис. 85).

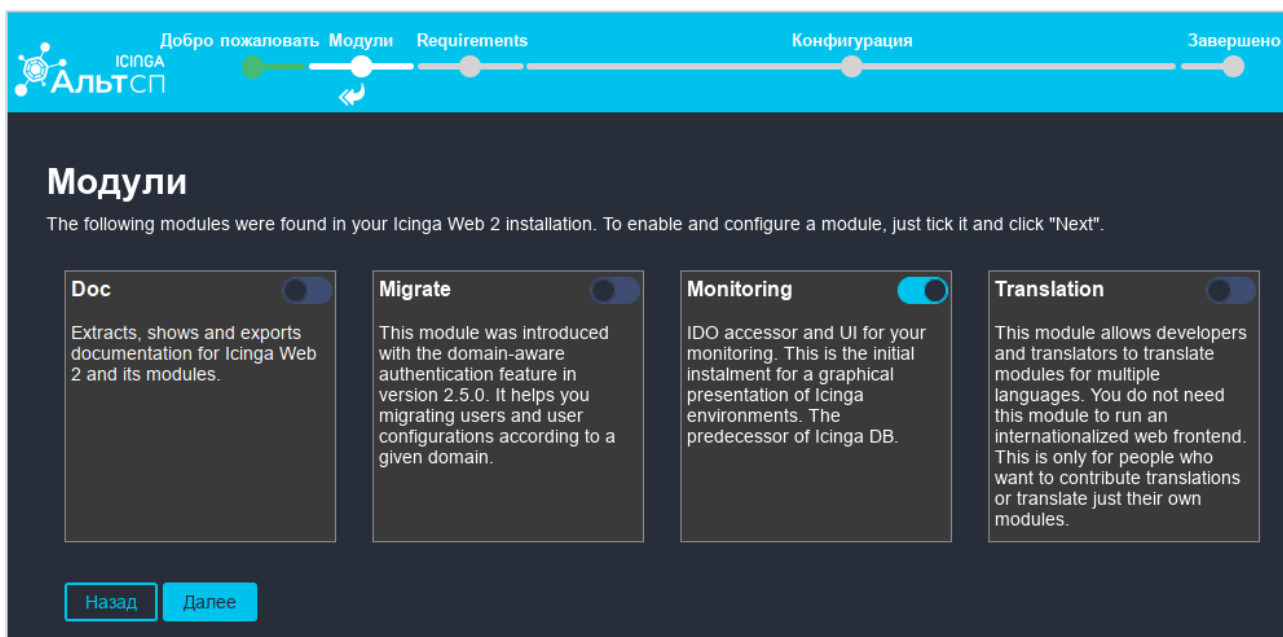


Рис. 85 – Icinga Web 2. Набор модулей

На следующей странице (рис. 86) показан набор предварительных требований. Если не все из них отмечены зеленым цветом, необходимо вернуться в консоль и обновить/установить соответствующий пакет.



Рис. 86 – Icinga Web 2. Набор предварительных требований

На следующем шаге необходимо выбрать тип аутентификации. Следует оставить, предложенную по умолчанию, аутентификацию с хранением учетных данных в БД – «База данных» (рис. 87).

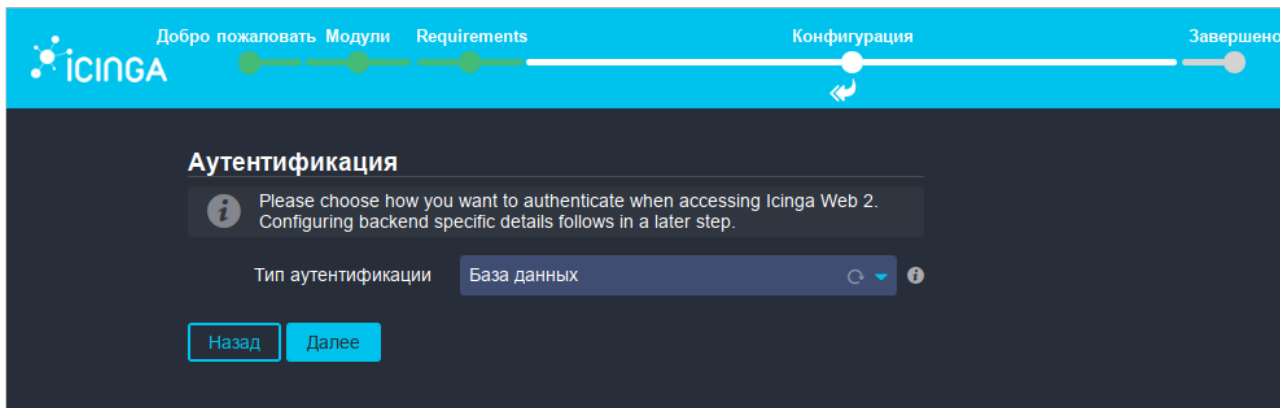


Рис. 87 – Icinga Web 2. Выбор типа аутентификации

Следующий шаг – настройка параметров подключения к базе данных для хранения учетных данных Icinga Web 2 (рис. 88, рис. 89):

- «Название ресурса» – имя ресурса данных;
- «Тип базы данных» – MySQL или PostgreSQL;
- «Узел» – узел, на котором расположена база данных. Так как база данных расположена на том же сервере, что и система мониторинга, поэтому подключаемся по localhost;
- «Порт» – порт для подключения к базе данных (при подключении к MySQL можно не указывать);
- «Название базы данных» – имя базы данных (icingaweb);
- «Имя пользователя» – имя пользователя для доступа к базе данных (icinga);
- «Пароль» – пароль пользователя.

Для проверки конфигурации следует нажать кнопку «Проверить конфигурацию». Если проверка прошла успешно, можно переходить к следующему шагу, нажав кнопку «Далее».

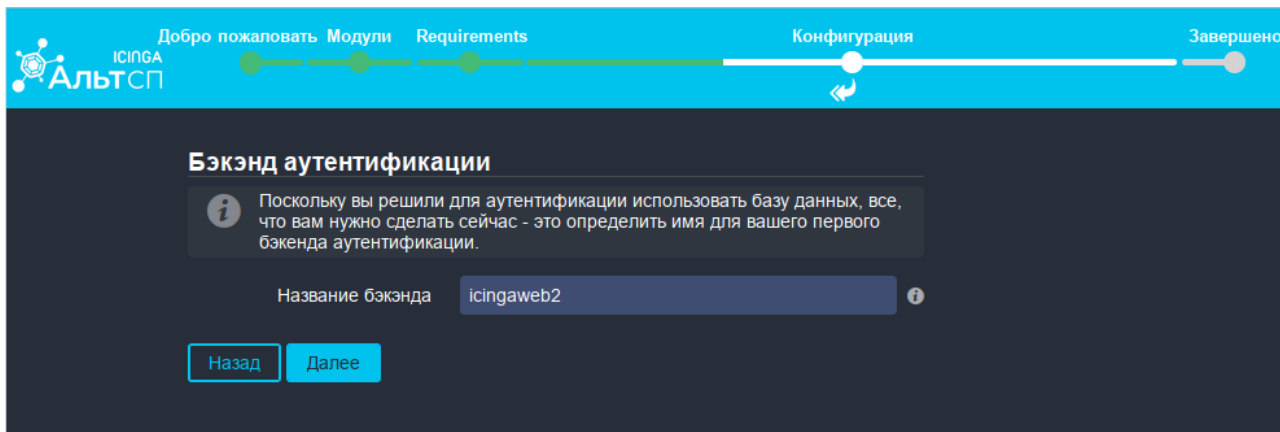
The screenshot shows the 'Источник базы данных' (Database Source) configuration step in the Icinga Web 2 wizard. The progress bar at the top indicates the current step is 'Конфигурация'. The main content area contains a message box with an information icon and text: 'Now please configure the database resource where to store users and user groups. Note that the database itself does not need to exist at this time as it is going to be created once the wizard is about to be finished.' Below this is a green success message: 'Конфигурация была успешно проверена.' The configuration fields are: 'Название ресурса *' (Resource name) set to 'icingaweb_db'; 'Тип базы данных *' (Database type) set to 'MySQL'; 'Узел *' (Host) set to 'localhost'; 'Порт' (Port) is empty; 'Название базы данных *' (Database name) set to 'icingaweb'; 'Имя пользователя *' (Username) set to 'icinga'; 'Пароль *' (Password) is masked with dots; 'Набор символов' (Character set) is empty; and 'Использовать SSL' (Use SSL) is a disabled toggle switch. At the bottom, there are three buttons: 'Назад', 'Далее', and 'Проверить конфигурацию'. A small note at the bottom left says 'Обязательное поле *'.

Рис. 88 – Icinga Web 2. Параметры подключения к базе данных MySQL

The screenshot shows the 'Источник базы данных' (Database Source) configuration step in the Icinga Web 2 wizard, similar to the previous one but for PostgreSQL. The progress bar at the top indicates the current step is 'Конфигурация'. The main content area contains the same information message and success message. The configuration fields are: 'Название ресурса *' (Resource name) set to 'icingaweb_db'; 'Тип базы данных *' (Database type) set to 'PostgreSQL'; 'Узел *' (Host) set to 'localhost'; 'Порт *' (Port) set to '5432'; 'Название базы данных *' (Database name) set to 'icingaweb'; 'Имя пользователя *' (Username) set to 'icinga'; 'Пароль *' (Password) is masked with dots; 'Набор символов' (Character set) is empty; and 'Использовать SSL' (Use SSL) is a disabled toggle switch. At the bottom, there are three buttons: 'Назад', 'Далее', and 'Проверить конфигурацию'. A small note at the bottom left says 'Обязательное поле *'.

Рис. 89 – Icinga Web 2. Параметры подключения к базе данных PostgreSQL

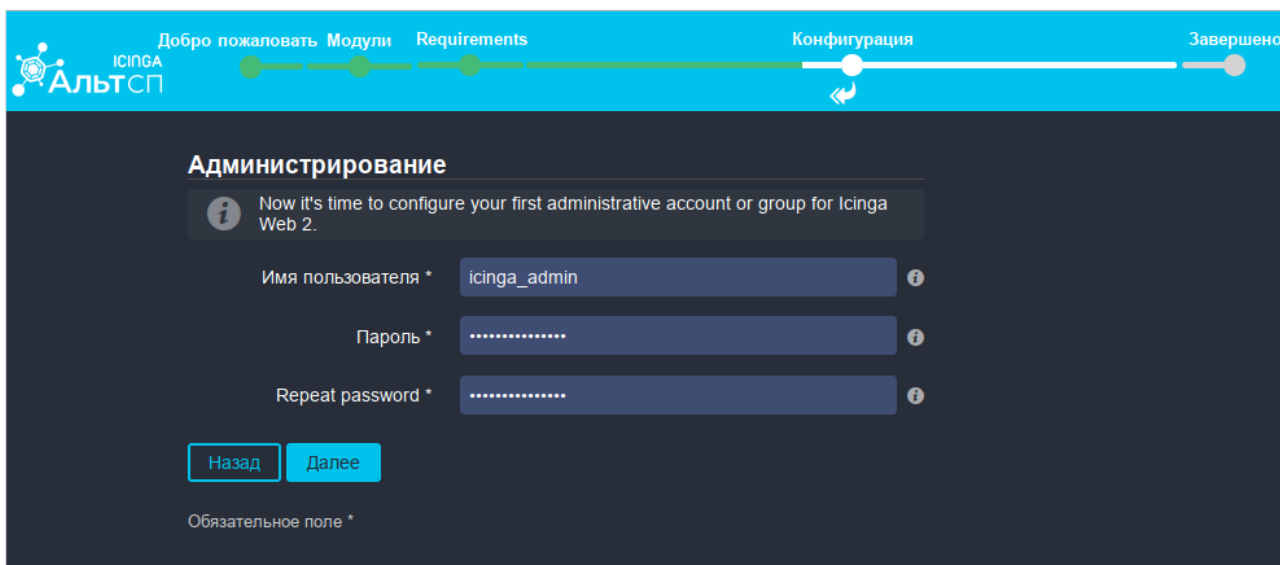
Далее нужно задать имя для бэкэнда (провайдера) аутентификации. Можно принять значение по умолчанию (рис. 90) и нажать кнопку «Далее».



The screenshot shows the Icinga Web 2 configuration wizard. At the top, there is a progress bar with five steps: 'Добро пожаловать' (Welcome), 'Модули' (Modules), 'Requirements', 'Конфигурация' (Configuration), and 'Завершено' (Completed). The 'Конфигурация' step is currently active. Below the progress bar, the title is 'Бэкэнд аутентификации' (Backend authentication). An information icon (i) is followed by the text: 'Поскольку вы решили для аутентификации использовать базу данных, все, что вам нужно сделать сейчас - это определить имя для вашего первого бэкэнда аутентификации.' (Since you decided to use a database for authentication, all you need to do now is determine the name for your first authentication backend). Below this, there is a text input field labeled 'Название бэкэнда' (Backend name) with the value 'icingaweb2'. At the bottom, there are two buttons: 'Назад' (Back) and 'Далее' (Next).

Рис. 90 – Icinga Web 2. Имя провайдера аутентификации

На следующем шаге (рис. 91) необходимо задать имя и пароль для учетной записи администратора для входа в веб-интерфейс Icinga Web 2.



The screenshot shows the Icinga Web 2 configuration wizard. At the top, there is a progress bar with five steps: 'Добро пожаловать' (Welcome), 'Модули' (Modules), 'Requirements', 'Конфигурация' (Configuration), and 'Завершено' (Completed). The 'Конфигурация' step is currently active. Below the progress bar, the title is 'Администрирование' (Administration). An information icon (i) is followed by the text: 'Now it's time to configure your first administrative account or group for Icinga Web 2.' Below this, there are three text input fields: 'Имя пользователя *' (Username) with the value 'icinga_admin', 'Пароль *' (Password) with masked characters, and 'Repeat password *' (Repeat password) with masked characters. At the bottom, there are two buttons: 'Назад' (Back) and 'Далее' (Next). Below the buttons, there is a note: 'Обязательное поле *' (Required field).

Рис. 91 – Icinga Web 2. Учетная запись администратора веб-интерфейса

Параметры конфигурации веб-приложения Icinga Web 2, предложенные на следующем шаге (рис. 92), можно оставить по умолчанию.

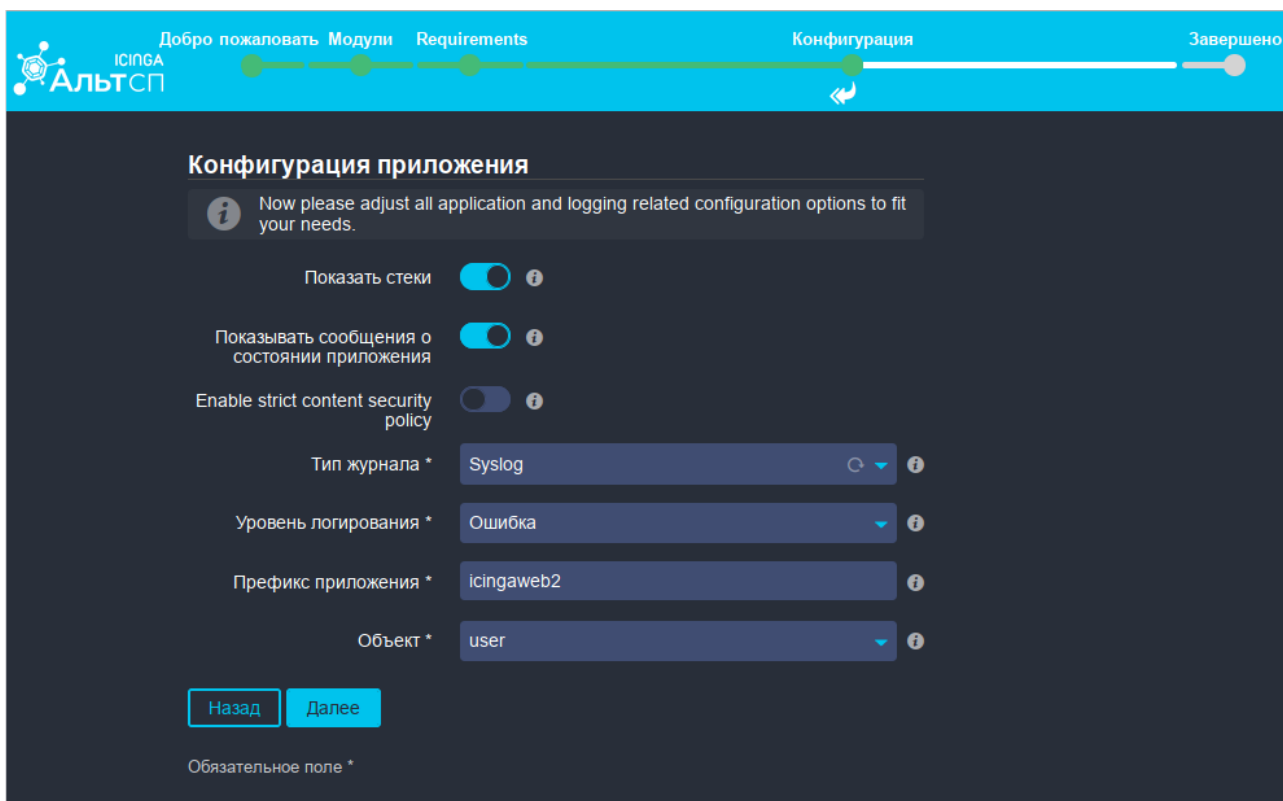


Рис. 92 – Icinga Web 2. Конфигурация приложения

На следующем шаге будет выведено сообщение об успешной конфигурации Icinga Web 2 со сводной информацией по определенным ранее параметрам (рис. 93).

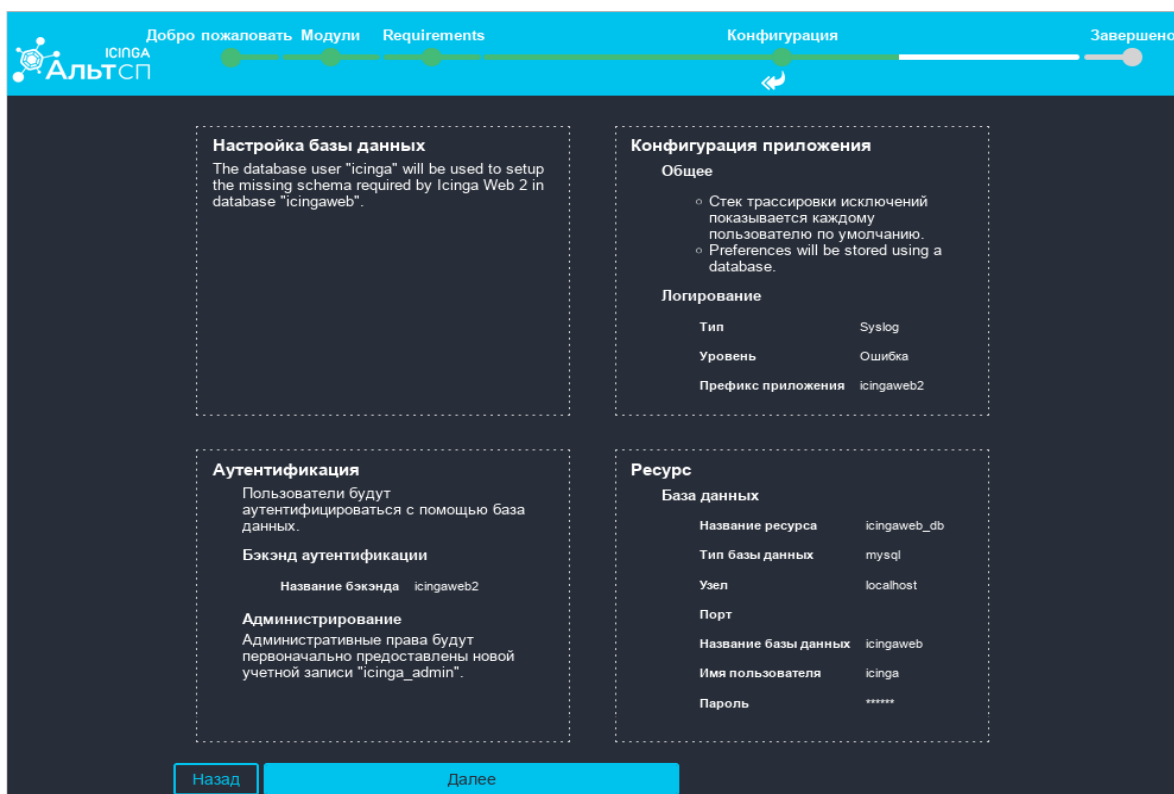


Рис. 93 – Icinga Web 2. Сообщение об успешной конфигурации сервера

Следующие шаги – настройка модуля monitoring. Сначала настраиваются параметры подключения к базе данных мониторинга (рис. 94, рис. 95):

- «Название ресурса» – имя ресурса данных;
- «Тип базы данных» – MySQL или PostgreSQL;
- «Узел» – узел, на котором расположена база данных. Так как база данных расположена на том же сервере, что и система мониторинга, поэтому подключаемся по localhost;
- «Порт» – порт для подключения к базе данных (при подключении к MySQL можно не указывать);
- «Название базы данных» – имя базы данных (icinga);
- «Имя пользователя» – имя пользователя для доступа к базе данных (icinga);
- «Пароль» – пароль пользователя.

Добро пожаловать Модули Requirements Конфигурация Завершено

Monitoring IDO Resource

Please fill out the connection details below to access the IDO database of your monitoring environment.

Конфигурация была успешно проверена.

Журнал проверки

```
Connection to icinga as icinga on localhost: successful
have_ssl: DISABLED
protocol_version: 10
version: 10.6.16-MariaDB-alt1
version_compile_os: Linux
```

Название ресурса * icinga_ido

Тип базы данных * MySQL

Узел * localhost

Порт

Название базы данных * icinga

Имя пользователя * icinga

Пароль *

Набор символов

Использовать SSL

Назад Далее Проверить конфигурацию

Обязательное поле *

Рис. 94 – Icinga Web 2. Настройка модуля monitoring (MySQL)

Добро пожаловать Модули Requirements Конфигурация Завершено

Monitoring IDO Resource

Please fill out the connection details below to access the IDO database of your monitoring environment.

Конфигурация была успешно проверена.

Журнал проверки

```
Connection to icinga as icinga on localhost:5432 successful
PostgreSQL 16.4 on x86_64-alt-linux-gnu, compiled by x86_64-alt-linux-gcc (GCC) 10.3.1 20210703 (ALT c10f2 10.3.1-alt2), 64-bit
```

Название ресурса *

Тип базы данных *

Узел *

Порт *

Название базы данных *

Имя пользователя *

Пароль *

Набор символов

Использовать SSL

Обязательное поле *

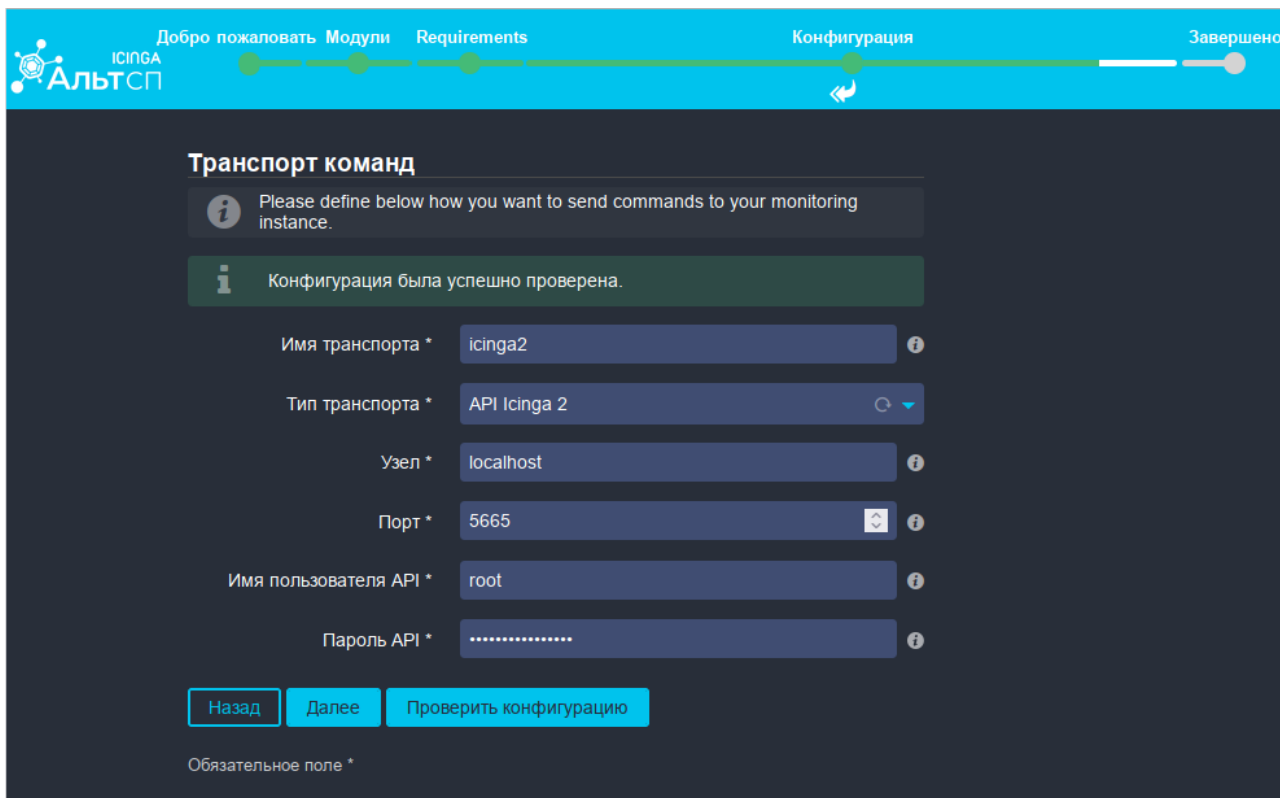
Рис. 95 – Icinga Web 2. Настройка модуля monitoring (PostgreSQL)

Для проверки конфигурации следует нажать кнопку «Проверить конфигурацию». Если проверка прошла успешно, можно переходить к следующему шагу.

Далее настраивается способ управления Icinga через Icinga Web 2 (рис. 96). Необходимо указать следующие данные:

- «Имя транспорта» – имя транспорта;
- «Тип транспорта» – в данном руководстве используется API (Icinga2 API);
- «Узел» – узел Icinga (так как Icinga и Icinga Web 2 находятся на одном сервере, поэтому можно указать localhost);
- «Порт» – порт Icinga API по умолчанию (5665);
- «Имя пользователя API» – имя пользователя для подключения к API (root);
- «Пароль API» – пароль для подключения к API.

Примечание. Имя и пароль для подключения к API указаны в файле /etc/icinga2/conf.d/api-users.conf.

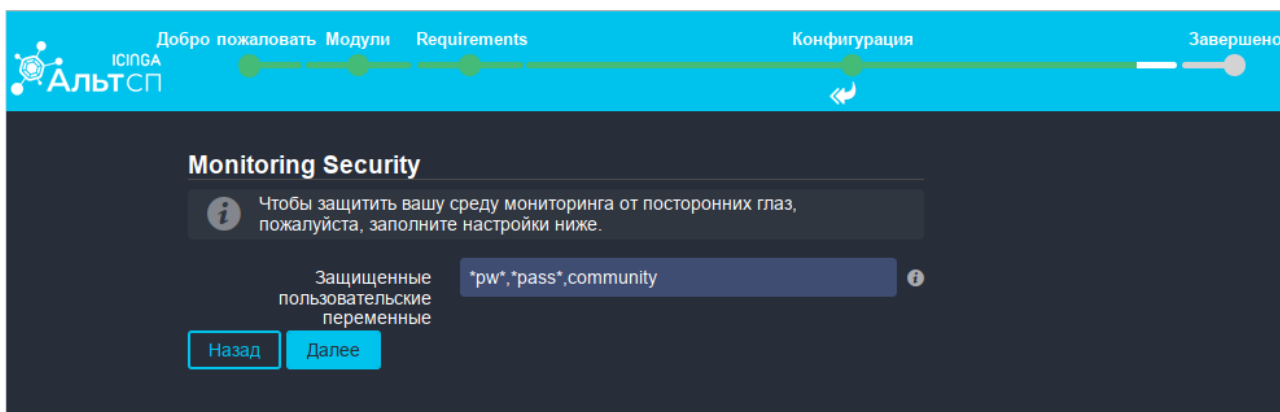


The screenshot shows the 'Transport Commands' configuration page in Icinga Web 2. At the top, a progress bar indicates the current step is 'Конфигурация' (Configuration), with previous steps 'Добро пожаловать' (Welcome), 'Модули' (Modules), and 'Requirements', and a final step 'Завершено' (Completed). The page title is 'Транспорт команд' (Transport Commands). An information icon and text state: 'Please define below how you want to send commands to your monitoring instance.' Below this, a green message box says 'Конфигурация была успешно проверена.' (Configuration was successfully checked). The form contains several fields: 'Имя транспорта *' (Transport name) with value 'icinga2'; 'Тип транспорта *' (Transport type) with a dropdown menu showing 'API Icinga 2'; 'Узел *' (Node) with value 'localhost'; 'Порт *' (Port) with value '5665'; 'Имя пользователя API *' (API user name) with value 'root'; and 'Пароль API *' (API password) with masked characters. At the bottom, there are three buttons: 'Назад' (Back), 'Далее' (Next), and 'Проверить конфигурацию' (Check configuration). A note at the bottom left says 'Обязательное поле *' (Required field *).

Рис. 96 – Icinga Web 2. Настройка способа управления Icinga через Icinga Web 2

Проверить возможность подключения можно, нажав на кнопку «Проверить конфигурацию».

На следующем шаге (рис. 97) можно задать список названий переменных для полей в разных веб-формах, в которых может отображаться парольная информация. Значения в таких полях будут отображаться в виде «звездочек».



The screenshot shows the 'Monitoring Security' configuration page in Icinga Web 2. The progress bar at the top is the same as in the previous screenshot, with 'Конфигурация' (Configuration) as the current step. The page title is 'Monitoring Security'. An information icon and text state: 'Чтобы защитить вашу среду мониторинга от посторонних глаз, пожалуйста, заполните настройки ниже.' (To protect your monitoring environment from prying eyes, please fill in the settings below). Below this, there is a text input field for 'Защищенные пользовательские переменные' (Protected user variables) with the value '*pw*,*pass*,community'. At the bottom, there are two buttons: 'Назад' (Back) and 'Далее' (Next).

Рис. 97 – Icinga Web 2. Защищенные пользовательские переменные

На последнем шаге конфигурации (рис. 98) отображается суммарная информация о конфигурации модуля мониторинга.

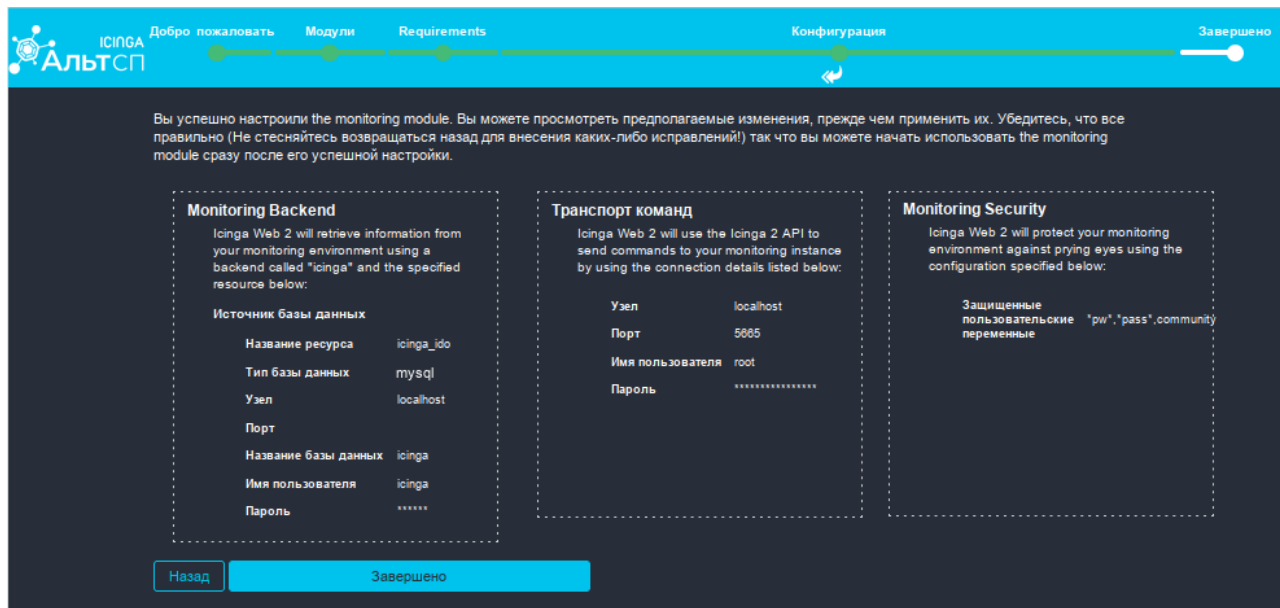


Рис. 98 – Icinga Web 2. Суммарная информация о конфигурации модуля мониторинга

После нажатия кнопки «Завершено» будет выведен краткий лог (рис. 99) и будет доступна кнопка перехода в веб-интерфейс («Login to Icinga Web 2»).

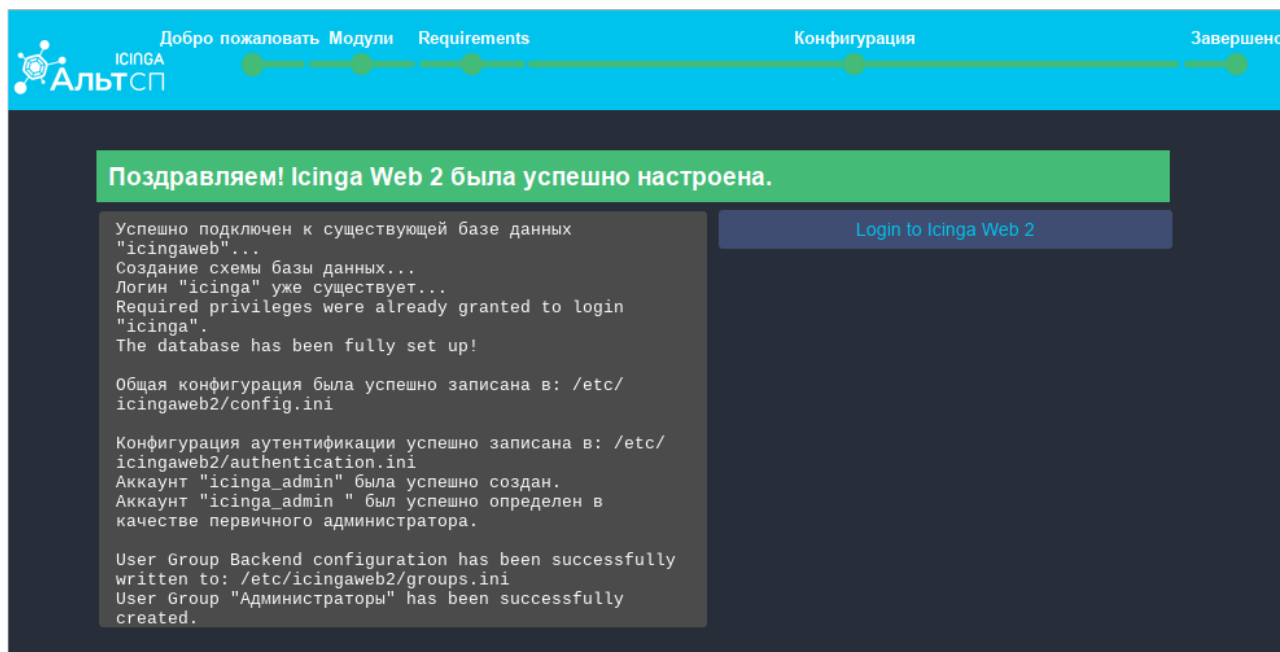


Рис. 99 – Icinga Web 2. Завершение настройки

Для входа в Icinga Web 2 (рис. 100) следует использовать учетные данные административного пользователя (в примере `icinga_admin`). В результате откроется сводная панель информации Icinga Web 2 (рис. 101) с информацией о состоянии базовых показателей мониторинга сервера.

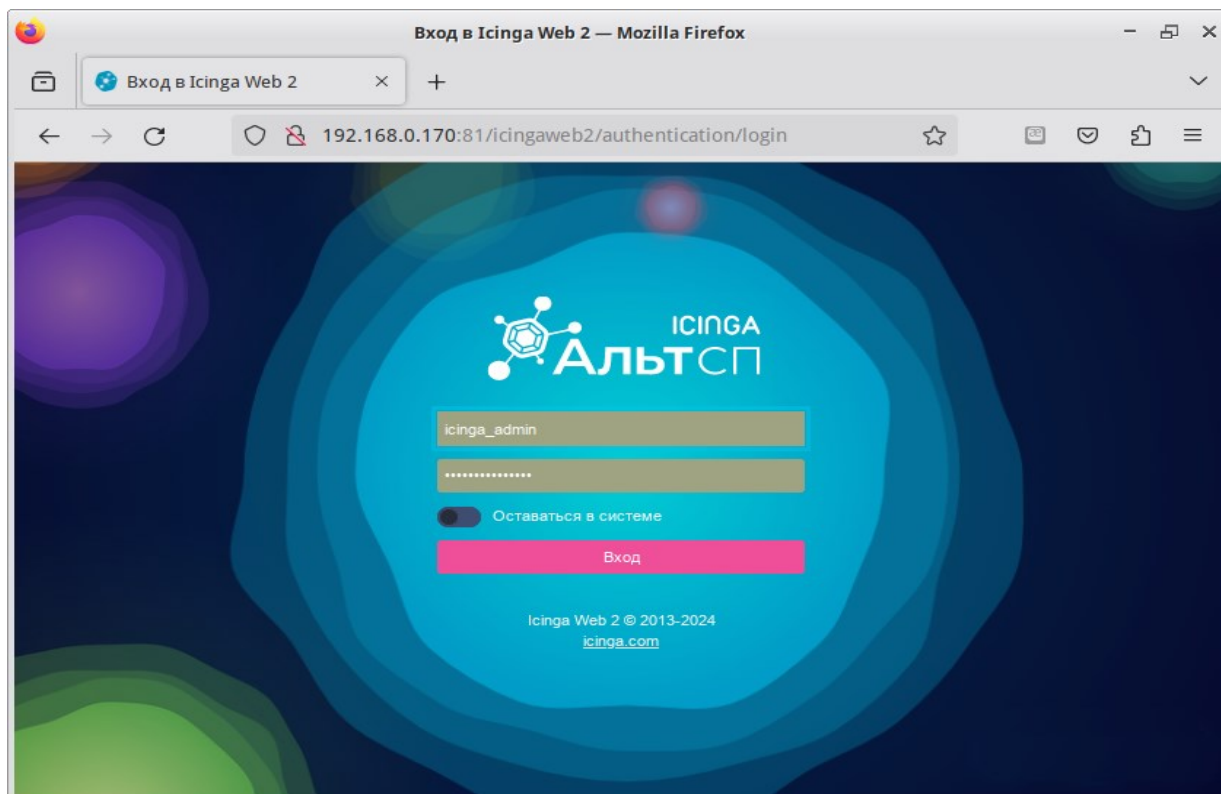


Рис. 100 – Вход в Icinga Web 2

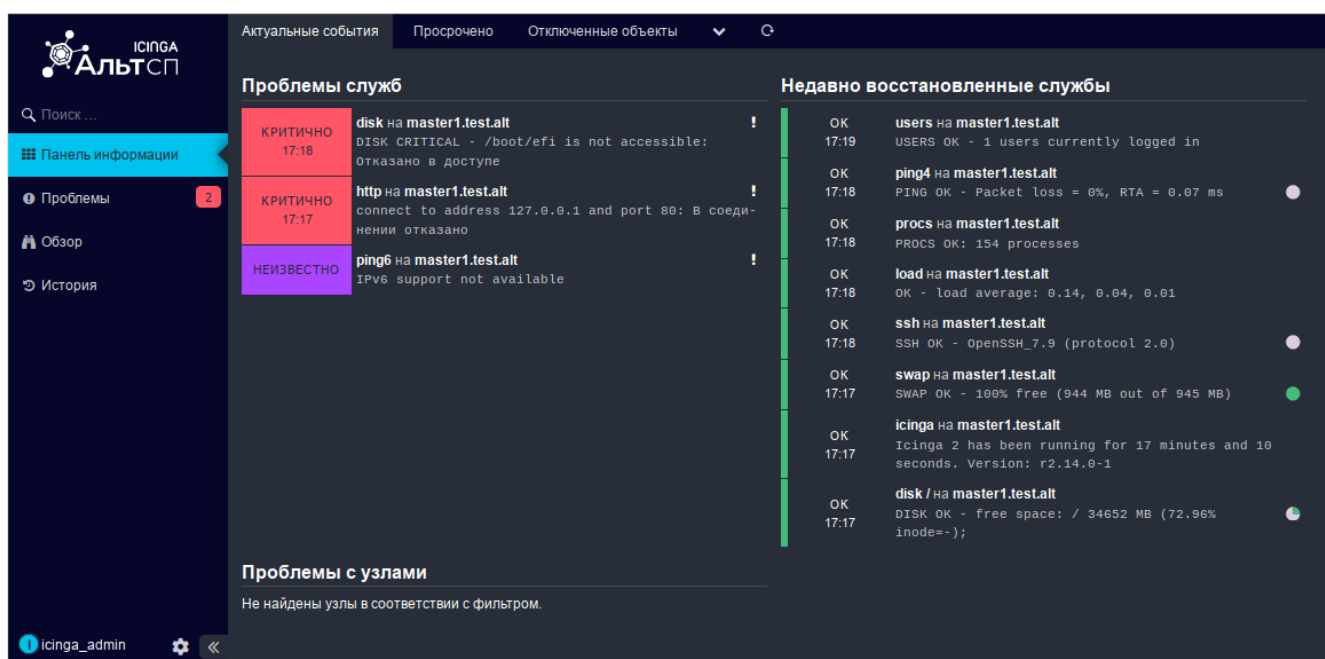


Рис. 101 – Панель информации Icinga Web 2

7.7.2. Настройка агентов

7.7.2.1. Установка пакетов

Установить пакеты `icinga2`, `nagwad-service`, `nagwad-audit` и `nagwad-icinga-agent`:

```
# apt-get install icinga2 nagwad-service nagwad-audit nagwad-icinga-agent
```

Включить в автозагрузку и запустить службу `nagwad.service`:

```
# systemctl enable --now nagwad.service
```

Включить в автозагрузку и запустить службу `icinga2.service`:

```
# systemctl enable --now icinga2.service
```

7.7.2.2. Настройка объектов наблюдения

Если для настройки объектов наблюдения используется Icinga Director (см. п. 7.7.3.2), то можно воспользоваться готовой корзиной (`basket`) шаблонов в формате JSON для наблюдения за событиями Nagwad из пакета `nagwad-icinga-master`.

Можно как добавлять конфигурацию каждого узла вручную, так и воспользоваться функцией API самообслуживания Icinga Director (см. п. 7.7.3.2.7).

В пакете `icinga2` также определены шаблоны конфигурации, пригодные для определения объектов наблюдения в конфигурационных файлах Icinga.

Шаблоны подготовлены для отслеживания следующих событий, фиксируемых `nagwad.service`:

- «Unauthorized file access» – несанкционированный доступ к файлам;
- «Unauthorized user or group change» – несанкционированное изменение файлов `/etc/passwd` и `/etc/group`;
- «Unauthorized device access» – несанкционированное подключение устройства;
- «Illegal login attempt» – неудачная попытка аутентификации;
- «System integrity violated» – нарушение целостности системы;
- «Printing policy violation attempt» – попытка нарушения политики печати.

7.7.2.2.1. Настройка политики печати

Поставляемый с пакетом nagwad фильтр событий печати `/etc/nagwad/print.regexp` рассчитан на то, что служба печати cups будет:

- проверять права доступа при печати;
- записывать в журнал сообщения об отказе по причине нехватки прав.

Для этого службу печати необходимо настроить следующим образом:

- в конфигурационном файле `/etc/cups/cups-files.conf` установить:

```
AccessLog syslog
```

- в главном конфигурационном файле `/etc/cups/cupsd.conf` ПОВЫСИТЬ уровень сообщений о нарушении доступа с `warn` до `info`:

```
LogLevel info
```

- в этом же файле ограничить доступ к операциям печати, например, разрешив их конкретному пользователю:

```
<Limit Create-Job Print-Job Print-URI Validate-Job>
```

```
    Require user имя-пользователя
```

```
    Order deny,allow
```

```
</Limit>
```

- перезапустить службу cups:

```
# systemctl restart cups
```

7.7.2.2.2. Сервис контроля целостности

Чтобы иметь возможность отслеживать нарушения целостности системных файлов, должен быть установлен пакет `integalert`.

Выполнить настройку наблюдаемых файлов и каталогов, проинициализировать базу данных, выполнив команду:

```
# integalert fix
```

Включить и запустить службу:

```
# systemctl enable --now integalert.service
```

7.7.2.3. Служба наблюдения за системным журналом Nagwad

7.7.2.3.1. Состав

Основными компонентами пакета nagwad являются:

- системная служба nagwad, сканирующая системный журнал с помощью набора фильтров `/etc/nagwad/*.regexp`, `/etc/nagwad/*.sed` (либо простые регулярные выражения для `grep`, либо полнофункциональные скрипты `sed`);
- сценарии пост-фильтрации событий в `/etc/nagwad/filter-event.d`;
- сценарии пост-обработки событий в `/etc/nagwad/process-event.d`;
- NRPE-скрипт `check_nagwad`, который проверяет файлы сигналов событий в каталогах `/var/log/nagwad/<boot_id>/<filter>/`, где `boot_id` это текущий системный идентификатор загрузки (`/proc/sys/kernel/random/boot_id`);
- служебный скрипт `nagwad`, который позволяет запрашивать, проверять и управлять сигнальными файлами событий.

Дополнения для различных систем мониторинга включают в себя следующие компоненты:

- шаблоны конфигурации для агента мониторинга Icinga2;
- шаблоны конфигурации для агента мониторинга Nagios;
- скрипты для интерфейса мониторинга Nagstamon;
- оболочка оболочки `nscs-shell` с ведением журнала, которую можно использовать для удаленного доступа.

7.7.2.3.2. Принцип работы

Как только какой-либо из настроенных фильтров определяет сообщение из системного журнала, nagwad генерирует событие, которое затем передается сценариям в каталоге `filter-event.d`. Сценарии могут дать ответный сигнал nagwad о том, нужно ли пропустить или проигнорировать данное событие. Сценарии также могут добавить произвольный текст к сообщению о событии.

Если событие не игнорируется, то соответствующий сигнальный файл записывается в каталог `/var/log/nagwad/<boot_id>/<filter>/`.

Имя сигнального файла соответствует шаблону `<filter>.<HASH>.<LEVEL>`.

NRPE-совместимый агент мониторинга может проверить этот файл с помощью сценария `check_nagwad`.

При проверке сигнальных файлов скрипт игнорирует файлы со специальным суффиксом `.FIXED`. Это позволяет помечать зарегистрированные события как разрешенные (либо с помощью команды `nagwad fix`, либо просто переименованием файла).

В дополнение к этому, данные о каждом событии передаются в скрипты в каталоге `process-event.d`.

7.7.2.3.3. Параметры конфигурации

Описание параметров конфигурации `nagwad` (файл `/etc/nagwad/nagwad.conf`) представлено в таблице 6.

Т а б л и ц а 6 – Описание конфигурационных параметров службы `nagwad`

Параметр	Описание	Значение по умолчанию
PIDFILE	Путь к PID-файлу, записываемому при запуске службы <code>nagwad</code>	<code>/run/nagwad.pid</code>
LOG_USER	Имя системного пользователя, которому принадлежат сигнальные файлы	<code>root</code>
LOG_GROUP	Имя системной группы, имеющей доступ на чтение для сигнальных файлов	<code>nagwad</code>
CONFDIR	Путь к каталогу конфигурации	<code>/etc/nagwad</code>
POSTFILTERS	Путь к каталогу для скриптов пост-фильтрации	<code>\$CONFDIR/filter-event.d</code>
POSTPROCESS	Путь к каталогу для скриптов пост-обработки	<code>\$CONFDIR/process-event.d</code>
LOGDIR	Путь к корневому каталогу журнала	<code>/var/log/nagwad</code>
MAXAGE	Количество дней, по истечении которых старые сигнальные файлы будут удалены	<code>30</code>
JOURNAL_TAIL	Количество сообщений, которые считываются из системного журнала при запуске и перезапуске <code>nagwad</code>	<code>5000</code>

Примечание. Если для параметра `MAXAGE` в файле `/etc/nagwad/nagwad.conf` установлено отличное от 0 значение, то при запуске `nagwad` удаляет все каталоги `/var/log/nagwad/*`, возраст которых превышает `MAXAGE`.

7.7.2.3.4. Команда nagwad

Синтаксис:

```
nagwad [опции] [команда]
```

Описание команд nagwad приведено в таблице 7.

Т а б л и ц а 7 – Описание команд nagwad

Команда	Описание
[list]	Просмотр списка зарегистрированных событий
[show] EVENT-ID	Просмотр информации о конкретном событии
fix EVENT-ID [EVENT-ID ...]	Пометить событие как исправленное
check [FILTER]	Проверить все события или события по определенному фильтру
status	Вывести статус службы nagwad
cleanup-old [DAYS]	Удалить события старше, указанного количества дней

Примеры использования команды nagwad:

- запуск в качестве системной службы:

```
# nagwad --service
```

- просмотр списка зарегистрированных событий:

```
# nagwad
```

```
2024-07-03+12:20:02.2161021330 login.c15459dac0fecba98fe27bfad170b3ba.WARNING
2024-07-03+12:20:35.7491051260
authdata.4d95e2fedcef82ca3e2dcbb062f3bd1c.CRITICAL
```

- просмотр информации о событии:

```
# nagwad show login.c15459dac0fecba98fe27bfad170b3ba.WARNING
WARNING: 2024-07-03T12:20:01+0200 agent4.test.alt audit[11506]:
USER_AUTH pid=11506 uid=0 auid=4294967295 ses=4294967295
msg='top=PAM:authentication grantors=? acct="?" exe="/bin/login"
hostname=agent4.test.alt addr=? terminal=/dev/tty2 res=failed'
```

- пометить событие как исправленное:

```
# nagwad fix authdata.4d95e2fedcef82ca3e2dcbb062f3bd1c.CRITICAL
```

- проверить события authdata:

```
# nagwad check authdata
```

```
CRITICAL: 2024-07-03T12:20:35+0200 agent4.test.alt audit[11815]:
SYSCALL arch=c000003e syscall=82 success=yes exit=0 a0=7fff2457ee60
a1=55873eafa900 a2=7fff2457edd0 a3=1f5 items=5 ppid=4114 pid=11815 auid=500
uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=5
comm="useradd" exe="/usr/sbin/useradd" key="usergroup-change"
```

- удалить события старше двух дней:

```
# nagwad cleanup-old 1
```

7.7.2.3.5. Некоторые скрипты пост-фильтрации

Скрипт фильтрации `/etc/nagwad/filter-event.d/10-eperm` используется для дополнительной фильтрации событий ошибочного доступа к файлам (EACCESS у процесса `systemd` при загрузке системы). Он использует файлы `.regex` из каталога `/etc/nagwad/filter-event.d/eperm-skip.d`, для определения того, какие события нужно пропустить. К событию, которое проходит пост-фильтр `10-eperm`, добавляется строка:

```
PATH=<путь>
```

где `<путь>` – это фактический путь к файлу, в доступе к которому было отказано.

7.7.2.3.6. Добавление новых проверок

7.7.2.3.6.1. Добавление новых фильтров журнала событий

Начиная с версии 0.10.0 `nagwad` автоматически обрабатывает все `*.regex` и `*.sed` файлы в каталоге `/etc/nagwad`.

В файлах формата `*.regex` определяются регулярные выражения для отслеживания сообщений системного журнала. Файл может содержать сразу несколько регулярных выражений – по одному выражению на строке. Событие формируется если обнаруживается совпадение с любым из определенных выражений. Базовое имя записываемого `nagwad` сигнального файла определяется базовым именем файла с суффиксом `.regex`. Оно же определяет имя фильтра, которое используется для проверки сигнального файла из Icinga2 или Nagios.

Файлы формата `*.sed` являются полноценными сценариями, предназначенными для программы `sed` (см. `man sed(1)` и `info sed`). В отличие от простого набора регулярных выражений, использование сценариев `sed` позволяет:

- модифицировать сообщения системного журнала;
- фиксировать различные «уровни критичности» события для различных сообщений.

Программа `sed` запускается из `nagwad` с аргументом `-n`, что позволяет использовать `sed` прежде всего как фильтр сообщений. Каждое отфильтрованное сценарием сообщение системного журнала должно после обработки принимать вид:

```
<имя_фильтра>:<ВАЖНОСТЬ>:<сообщение>
```

где «имя_фильтра» определяет базовое имя записываемого `nagwad` сигнального файла. Например, подстановку вида `s//myevent:CRITICAL:&/p` удобно использовать после предварительной фильтрации сообщений системного журнала для того, чтобы транслировать отфильтрованное сообщение без изменений как критическое событие, которое будет записано в сигнальный файл `/var/log/nagwad/<boot_id>/<filter>/filterXXX.CRITICAL`. В `Icinga2` это событие будет отражено как критичное.

При необходимости, вместо уровня `CRITICAL` можно использовать уровень `WARNING`, отображающийся в `Icinga` и `Nagios` как предупреждение. Другие уровни сообщений `Icinga` и `Nagios` не поддерживают.

7.7.2.3.6.2. Фильтры пост-обработки событий

Кроме фильтров для первичной обработки событий (то есть для их фильтрации из системного журнала), начиная с версии 0.10.1 `nagwad` поддерживает дополнительные фильтры для пост-обработки отфильтрованных событий. Сценарии для пост-обработки помещаются в каталог `/etc/nagwad/filter-event.d` и выполняются для каждого события в алфавитном порядке.

Каждый сценарий пост-обработки запускается с тремя аргументами:

```
<сценарий> FILTER STATUS MESSAGE
```

где:

- `FILTER` – имя фильтра, зафиксировавшего событие;
- `STATUS` – уровень критичности события (`CRITICAL` или `WARNING`);
- `MESSAGE` – сообщение.

На основе этих данных сценарий должен вынести решение пропустить данное событие дальше или «отбросить» его. Для этой цели используется код завершения работы сценария (`exit code`):

- 0 – означает, что событие можно пропускать дальше;

- `$NAGWAD_SKIP_EVENT` — означает, что событие должно быть отброшено (переменная `NAGWAD_SKIP_EVENT` передается из `nagwad` в окружение сценария);
- любое другое значение сигнализирует о сбое в работе сценария (однако событие пропускается дальше).

Если очередной сценарий из каталога `/etc/nagwad/filter-event.d` завершается со значением `$NAGWAD_SKIP_EVENT`, дальнейший вызов сценариев пост-обработки прекращается.

7.7.3. Управление конфигурацией

Управление конфигурацией клиентов Icinga может выполняться разными способами:

- с помощью веб-инструмента Icinga Director. Реализует управление всеми конфигурационными файлами через веб-интерфейс Icinga Web 2;
- ручная настройка посредством редактирования конфигурационных файлов (более гибкий способ).

Примечание. Настоятельно рекомендуется использовать файлы конфигурации или Director. Смешение вариантов может привести к конфликтам имен, труднообнаружимым проблемам или любому другому неожиданному поведению. Комбинирование данных способов возможно в некоторых нетривиальных сценариях, при этом необходимо учитывать:

- объекты из файлов конфигурации не видны и не редактируются внутри Director;
- наименование объектов, которые предназначены для ручной настройки и объектов, которые предназначены для Icinga Director должны различаться;
- если что-то было добавлено/изменено в файлах конфигурации, перед развертыванием нужно проверить конфигурацию, выполнив команду `icinga2 daemon -C`
- при создании объектов с одинаковыми именами в файлах конфигурации, и Director не предупредит о наличии дубликата, до момента разворачивания конфигурации.

Далее будут рассмотрены оба способа.

7.7.3.1. Ручная конфигурация

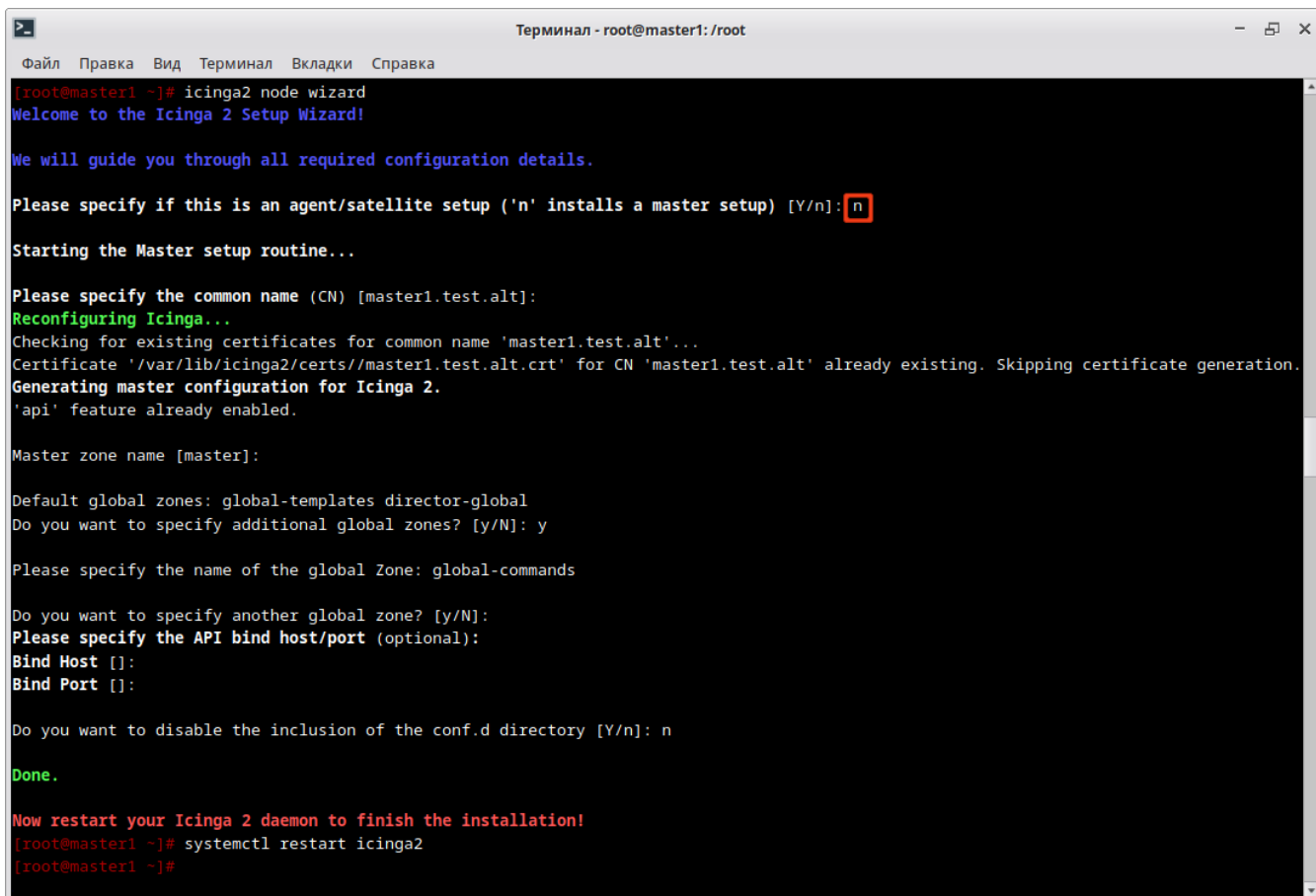
7.7.3.1.1. Конфигурирование Мастер-узла

На сервере, где развернуты Icinga2 и Icinga Web 2, необходимо запустить мастер конфигурирования узла, выполнив команду `icinga2 node wizard` (рис. 102).

В ответах можно принять значения по умолчанию (можно просто нажать клавишу Enter) или ввести свои ответы. Важно при ответе на первый вопрос ввести «n», чтобы перевести мастер настройки в режим настройки Мастер-узла. При ответе на вопрос `Do you want to specify additional global zones? [y/N]:` следует ответить «y» и при ответе на следующий вопрос `Please specify the name of the global Zone:` указать зону `global-commands`.

Описание остальных параметров приведено в таблице 8.

Примечание. Для возможности использования шаблонов `generic-host` нужно НЕ отключать чтение файлов из `conf.d` при первичной настройке узла (ответить «n» на вопрос «`Do you want to disable the inclusion of the conf.d directory [Y/n]:`»).



```
Терминал - root@master1: /root
Файл Правка Вид Терминал Вкладки Справка
[root@master1 ~]# icinga2 node wizard
Welcome to the Icinga 2 Setup Wizard!

We will guide you through all required configuration details.

Please specify if this is an agent/satellite setup ('n' installs a master setup) [Y/n]: n
Starting the Master setup routine...

Please specify the common name (CN) [master1.test.alt]:
Reconfiguring Icinga...
Checking for existing certificates for common name 'master1.test.alt'...
Certificate '/var/lib/icinga2/certs//master1.test.alt.crt' for CN 'master1.test.alt' already existing. Skipping certificate generation.
Generating master configuration for Icinga 2.
'api' feature already enabled.

Master zone name [master]:

Default global zones: global-templates director-global
Do you want to specify additional global zones? [y/N]: y

Please specify the name of the global Zone: global-commands

Do you want to specify another global zone? [y/N]:
Please specify the API bind host/port (optional):
Bind Host []:
Bind Port []:

Do you want to disable the inclusion of the conf.d directory [Y/n]: n

Done.

Now restart your Icinga 2 daemon to finish the installation!
[root@master1 ~]# systemctl restart icinga2
[root@master1 ~]#
```

Рис. 102 – Настройка ведущего узла

Т а б л и ц а 8 – Описание параметров

Параметр	Описание
Common name (CN)	Используется для генерации SSL-сертификата, который будет использоваться для защиты соединений между сервером и его клиентами. По умолчанию в качестве CN предлагается FQDN-имя сервера
Master zone name	Имя мастер-зоны. По умолчанию master
Global zones	Позволяет указать дополнительные глобальные зоны в дополнение к глобальным шаблонам и глобальному директору. По умолчанию N
API bind host	Адрес, к которому привязан ApiListener. Только для расширенного использования
API bind port	Порт, к которому привязан ApiListener. Только для расширенного использования
Disable conf.d	Позволяет отключить директиву include_recursive «conf.d», за исключением файла api-users.conf в файле icinga2.conf

Пример конфигурирования Мастер-узла:

```
# icinga2 node wizard

Welcome to the Icinga2 Setup Wizard!

We will guide you through all required configuration details.

Please specify if this is an agent/satellite setup ('n' installs
a master setup) [Y/n]: n

Starting the Master setup routine...

Please specify the common name (CN) [master1.test.alt]:
Reconfiguring Icinga...
Checking for existing certificates for common name
'master1.test.alt'...
Certificate '/var/lib/icinga2/certs//master1.test.alt.crt' for CN
'master1.test.alt' already existing. Skipping certificate generation.
Generating master configuration for Icinga2.
'api' feature already enabled.

Master zone name [master]:

Default global zones: global-templates director-global
Do you want to specify additional global zones? [y/N]: y

Please specify the name of the global Zone: global-commands

Please specify the API bind host/port (optional):
Bind Host []:
Bind Port []:
```

```
Do you want to disable the inclusion of the conf.d directory
[Y/n]: n
```

```
Done.
```

```
Now restart your Icinga2 daemon to finish the installation!
```

Примечание. Так как процедура активации Icinga API уже была запущена ранее (команда `icinga2 api setup`), то уже тогда был создан локальный центр сертификации (certificate authority) и сгенерирован SSL-сертификат для сервера (в каталоге `/var/lib/icinga2/certs/`). Поэтому в данном случае мастер конфигурирования узла обнаружит этот сертификат. Мастер также обнаружит, что поддержка API в Icinga уже включена.

После окончания конфигурации необходимо перезапустить сервис Icinga2:

```
# systemctl restart icinga2.service
```

Информация о мастер-узле будет добавлена в файл `/etc/icinga2/zones.conf`:

```
object Endpoint "master1.test.alt" {
}

object Zone "master" {
    endpoints = [ "master1.test.alt" ]
}

object Zone "global-templates" {
    global = true
}

object Zone "director-global" {
    global = true
}
object Zone "global-commands" {
    global = true
}
```

7.7.3.1.2. Конфигурирование агента

Все сертификаты агентов должны быть подписаны одним и тем же центром сертификации (CA). Это гарантирует, что все узлы доверяют друг другу в распределенной среде мониторинга.

Избежать подписания и развертывания сертификатов вручную можно, используя встроенные методы автоматического подписания запросов на подпись сертификатов (CSR):

- автоматическое подписание CSR – использует билет клиента (агента или спутника), сгенерированный на мастер-узле, в качестве идентификатора доверия;
- подписание CSR по требованию – позволяет подписывать ожидающие запросы сертификатов на мастер-узле.

7.7.3.1.2.1. Автоматическое подписание CSR

В этом сценарии агент отправляет запрос на подпись сертификата (CSR) и должен пройти аутентификацию доверенным способом. Мастер генерирует билет клиента, который включается в этот запрос. Таким образом, мастер может проверить, что запрос соответствует ранее доверенному билету, и подписать запрос.

Получить билет можно двумя способами:

- выполнить команду на мастер-узле;
- выполнить запрос REST API к мастер-узлу.

Пример генерации билета на мастер-узле:

```
# icinga2 pki ticket --cn 'agent1.test.alt'
84bffc6d33eccbbbd9b2ec6130031cef1d68ac01
```

где agent1.test.alt – FQDN добавляемого агента.

Пример генерации билета с выполнением запроса REST API:

```
# curl -k -s -u root:df0a9ffdbb104326 -H 'Accept: application/json' \
-X POST 'https://localhost:5665/v1/actions/generate-ticket' \
-d '{ "cn": "agent1.test.alt" }'
{"results":[{"code":200,"status":"Generated          PKI          ticket
'526ac5033f52716feddf1271eca8a18df2cd7584'          for          common          name
'agent1.test.alt'.", "ticket": "526ac5033f52716feddf1271eca8a18df2cd7584"}]}
```

где:

- root – имя пользователя для подключения к API;
- df0a9ffdbb104326 – пароль для подключения к API;
- agent1.test.alt – FQDN добавляемого агента.

Примечание. Для запроса API Icinga2 на мастер-узле требуется объект API User как минимум с разрешением на создание билета (actions/generate-ticket).

Создать данное разрешение можно, добавив следующие строки в файл `/etc/icinga2/conf.d/api-users.conf`:

```
object ApiUser "client-pki-ticket" {
    password = "333beabb8fd23e6e9" //change this
    permissions = [ "actions/generate-ticket" ]
}
```

После внесения изменений в файл `/etc/icinga2/conf.d/api-users.conf` необходимо перезапустить службу:

```
# systemctl restart icinga2
```

Сгенерированный на мастер-узле билет необходимо будет использовать на агенте во время установки.

Запустить мастер конфигурирования узла на агенте можно, выполнив команду (рис. 103):

```
# icinga2 node wizard
```

В ответах можно принять значения по умолчанию (можно нажать клавишу `<Enter>`) или ввести свои ответы. При ответе на первый вопрос можно нажать клавишу `<Enter>`, чтобы перевести мастер настройки в режим настройки агента. При ответе на вопрос `Do you want to specify additional global zones? [y/N]:` следует ответить «у» и при ответе на следующий вопрос `Please specify the name of the global Zone:` указать зону `global-commands`. Описание остальных параметров приведено в таблице 9.

```

Терминал - root@agent1:/root
Файл Правка Вид Терминал Вкладки Справка
[root@agent1 ~]# icinga2 node wizard
Welcome to the Icinga 2 Setup Wizard!

We will guide you through all required configuration details.

Please specify if this is an agent/satellite setup ('n' installs a master setup) [Y/n]:

Starting the Agent/Satellite setup routine...

Please specify the common name (CN) [agent1.test.alt]:

Please specify the parent endpoint(s) (master or satellite) where this node should connect to:
Master/Satellite Common Name (CN from your master/satellite node): master1.test.alt

Do you want to establish a connection to the parent node from this node? [Y/n]:
Please specify the master/satellite connection information:
Master/Satellite endpoint host (IP address or FQDN): master1.test.alt
Master/Satellite endpoint port [5665]:

Add more master/satellite endpoints? [y/N]:
Parent certificate information:

Version:                3
Subject:                 CN = master1.test.alt
Issuer:                  CN = Icinga CA
Valid From:              Jul  1 07:11:38 2024 GMT
Valid Until:             Aug  2 07:11:38 2025 GMT
Serial:                  c8:74:1e:c2:8f:6a:8b:bf:bc:61:97:3d:64:90:5a:bc:5d:54:62:9a

Signature Algorithm:    sha256WithRSAEncryption
Subject Alt Names:      master1.test.alt
Fingerprint:            19 07 D1 40 51 7B EE 74 6C C0 57 21 8C 90 52 73 7E F8 65 C6 3B 60 B0 46 4D B4 4C DC B5 C4 82 98

Is this information correct? [y/N]: y

Please specify the request ticket generated on your Icinga 2 master (optional).
(Hint: # icinga2 pki ticket --cn 'agent1.test.alt'): 84bffc6d33eccbbd9b2ec6130031cef1d68ac01
Please specify the API bind host/port (optional):
Bind Host []:
Bind Port []:

Accept config from parent node? [y/N]: y
Accept commands from parent node? [y/N]: y

Reconfiguring Icinga...
Disabling feature notification. Make sure to restart Icinga 2 for these changes to take effect.
Enabling feature api. Make sure to restart Icinga 2 for these changes to take effect.

Local zone name [agent1.test.alt]:
Parent zone name [master]:

Default global zones: global-templates director-global
Do you want to specify additional global zones? [y/N]: y

Please specify the name of the global Zone: global-commands

Do you want to specify another global zone? [y/N]:
Do you want to disable the inclusion of the conf.d directory [Y/n]:
Disabling the inclusion of the conf.d directory...

Done.

Now restart your Icinga 2 daemon to finish the installation!
[root@agent1 ~]#

```

Рис. 103 – Регистрация агента

Примечание. Для возможности использования шаблонов generic-host и nagwad-host с мастер-узла (см. п. 7.7.3.1.4), нужно отключить чтение файлов из conf.d (нажать Enter на вопрос Do you want to disable the inclusion of the conf.d directory [Y/n]:). Если же планируется использование шаблонов с агента, нужно НЕ отключать чтение файлов из conf.d при первичной настройке узла (ответить «n» на вопрос Do you want to disable the inclusion of the conf.d directory [Y/n]:). Данное значение можно будет изменить и после настройки узла.

Т а б л и ц а 9 – Описание параметров команды конфигурации агента

Параметр	Описание
Common name (CN)	Используется для генерации SSL-сертификата. По умолчанию используется FQDN-имя агента
Master/Satellite Common Name	Имя мастер-зоны. Необходимо указать имя, заданное на Мастер-узле
Establish connection to the parent node	Должен ли узел пытаться подключиться к родительскому узлу или нет. По умолчанию <code>y</code>
Master/Satellite endpoint host	Требуется, если агенту необходимо подключиться к Мастер-узлу/Спутнику. IP-адрес или полное доменное имя родительской конечной точки. Эта информация будет включена в конфигурацию объекта Endpoint в файле <code>Zones.conf</code>
Master/Satellite endpoint port	Необязательно, если агенту необходимо подключиться к Мастер-узлу/Спутнику. порт прослушивания родительских конечных точек. Эта информация включена в конфигурацию объекта Endpoint
Add more master/satellite endpoints	Если настроено несколько Мастер-узлов, необходимо указать их здесь
Parent Certificate information	Информация о Мастер-узле. Следует убедиться, что подключающийся хост действительно является запрошенным главным узлом. Отпечаток ключа мастер-узла можно узнать, выполнив на Мастер-узле команду: # openssl x509 -noout -fingerprint -sha256 -in \ "/var/lib/icinga2/certs/\$(hostname --fqdn).crt"
Request ticket	Билет, сгенерированный на мастере
API bind host	Адрес, к которому привязан ApiListener. Только для расширенного использования
API bind port	Порт, к которому привязан ApiListener. Только для расширенного использования
Accept config from parent node?	Принимает ли этот узел синхронизацию конфигурации от главного узла (требуется для режима синхронизации конфигурации). По соображениям безопасности по умолчанию установлено значение <code>n</code> .
Accept commands from parent node?	Принимает ли этот узел сообщения о выполнении команд от главного узла (требуется для режима конечной точки команды). По соображениям безопасности по умолчанию установлено значение <code>n</code>
Local zone name	Позволяет указать имя локальной зоны, когда этот экземпляр является спутником, а не агентом. По умолчанию используется FQDN-имя
Parent zone name	Позволяет указать имя родительской зоны. Это важно, если у агента родительским экземпляром является вспомогательный, а не главный. По умолчанию <code>master</code>
Global zones	Позволяет указать дополнительные глобальные зоны в дополнение к глобальным шаблонам и глобальному директору. По умолчанию <code>N</code>
Disable conf.d	Позволяет отключить включение каталога <code>conf.d</code> , в котором хранится локальный пример конфигурации. Клиенты должны получать свою конфигурацию от родительского узла или действовать как мост выполнения командной конечной точки. По умолчанию <code>y</code>

Пример конфигурации агента:

```
# icinga2 node wizard
Welcome to the Icinga2 Setup Wizard!
```

We will guide you through all required configuration details.

Please specify if this is an agent/satellite setup ('n' installs a master setup) [Y/n]:

Starting the Agent/Satellite setup routine...

Please specify the common name (CN) [agent1.test.alt]:

Please specify the parent endpoint(s) (master or satellite) where this node should connect to:

Master/Satellite Common Name (CN from your master/satellite node): master1.test.alt

Do you want to establish a connection to the parent node from this node? [Y/n]:

Please specify the master/satellite connection information:

Master/Satellite endpoint host (IP address or FQDN):
master1.test.alt

Master/Satellite endpoint port [5665]:

Add more master/satellite endpoints? [y/N]:

Parent certificate information:

```
Version:          3
Subject:          CN = master1.test.alt
Issuer:           CN = Icinga CA
Valid From:       Jul 1 07:11:38 2024 GMT
Valid Until:      Aug 1 07:11:38 2025 GMT
Serial:
```

```
c8:74:1e:c2:8f:6a:8b:bf:bc:61:97:3d:64:90:5a:bc:5d:54:62:9a
```

```
Signature Algorithm: sha256WithRSAEncryption
```

```
Subject Alt Names:  master1.test.alt
```

```
Fingerprint:       19 07 D1 40 51 7B EE 74 6C C0 57 21 8C 90
52 73 7E F8 65 C6 3B 60 B0 46 4D B4 4C DC B5 C4 82 98
```

Is this information correct? [y/N]: y

Please specify the request ticket generated on your Icinga2 master (optional).

ЛКНВ.11100-01 90 03

```
(Hint: # icinga2 pki ticket --cn 'agent1.test.alt'):
84bffc6d33eccbbbd9b2ec6130031cef1d68ac01
Please specify the API bind host/port (optional):
Bind Host []:
Bind Port []:
```

```
Accept config from parent node? [y/N]: Y
Accept commands from parent node? [y/N]: Y
```

Reconfiguring Icinga...

Disabling feature notification. Make sure to restart Icinga2 for these changes to take effect.

Enabling feature api. Make sure to restart Icinga2 for these changes to take effect.

```
Local zone name [agent1.test.alt]:
Parent zone name [master]: master1.test.alt
```

```
Default global zones: global-templates director-global
Do you want to specify additional global zones? [y/N]: y
```

```
Please specify the name of the global Zone: global-commands
```

```
Do you want to disable the inclusion of the conf.d directory
[Y/n]:
```

Disabling the inclusion of the conf.d directory...

Done.

Now restart your Icinga2 daemon to finish the installation!

После окончания конфигурации необходимо перезапустить сервис Icinga2:

```
# systemctl restart icinga2.service
```

Информация о мастер-узле и об агенте будет добавлена в файл

/etc/icinga2/zones.conf:

```
object Endpoint "master1.test.alt" {
    host = "master1.test.alt"
    port = "5665"
}

object Zone "master" {
    endpoints = [ "master1.test.alt" ]
}
```

```
object Endpoint "agent1.test.alt" {
}

object Zone "agent1.test.alt" {
  endpoints = [ "agent1.test.alt" ]
  parent = "master"
}

object Zone "global-templates" {
  global = true
}

object Zone "director-global" {
  global = true
}

object Zone "global-commands" {
  global = true
}
```

7.7.3.1.2.2. Подписание CSR по требованию (sign on demand)

В данном разделе рассмотрен вариант с подписыванием сертификата агента на мастере (sign on demand).

В этом сценарии не требуется предварительное получение билета на мастере. Агент отправляет запрос на подпись сертификата указанному родительскому узлу (это может быть либо непосредственно мастер, либо спутник, который пересылает запрос подписывающему мастеру). Администратор основного мастера отвечает за проверку и подписание запросов с помощью закрытого ключа СА.

Для регистрации агента в режиме sign on demand после запуска мастера конфигурирования узла (команда `icinga2 node wizard`) следует пропустить вопрос с указанием билета (рис. 104) и подписать запрос позже на мастере. Описание остальных параметров приведено в таблице 9.

Примечание. Для возможности использования шаблонов `generic-host` и `nagwad-host` с мастер-узла (см. п. 7.7.3.1.4), нужно отключить чтение файлов из `conf.d` (нажать клавишу `Enter` на вопрос `Do you want to disable the inclusion of the conf.d directory [Y/n]:`). Если же планируется использование шаблонов с агента, нужно НЕ отключать чтение файлов из `conf.d` при первичной настройке узла (ответить «n» на вопрос `Do you want to disable the inclusion of the conf.d directory [Y/n]`). Данное значение можно будет изменить и после настройки узла.

```

Терминал - root@agent3: /root
Файл Правка Вид Терминал Вкладки Справка
[root@agent3 ~]# icinga2 node wizard
Welcome to the Icinga 2 Setup Wizard!

We will guide you through all required configuration details.

Please specify if this is an agent/satellite setup ('n' installs a master setup) [Y/n]:

Starting the Agent/Satellite setup routine...

Please specify the common name (CN) [agent3.test.alt]:

Please specify the parent endpoint(s) (master or satellite) where this node should connect to:
Master/Satellite Common Name (CN from your master/satellite node): master1.test.alt

Do you want to establish a connection to the parent node from this node? [Y/n]:
Please specify the master/satellite connection information:
Master/Satellite endpoint host (IP address or FQDN): 192.168.0.194
Master/Satellite endpoint port [5665]:

Add more master/satellite endpoints? [y/N]:
Parent certificate information:

Version:          3
Subject:          CN = master1.test.alt
Issuer:           CN = Icinga CA
Valid From:       Jul  1 07:11:38 2024 GMT
Valid Until:      Aug  2 07:11:38 2025 GMT
Serial:           c8:74:1e:c2:8f:6a:8b:bf:bc:61:97:3d:64:90:5a:bc:5d:54:62:9a

Signature Algorithm: sha256WithRSAEncryption
Subject Alt Names:   master1.test.alt
Fingerprint:        19 07 D1 40 51 7B EE 74 6C C0 57 21 8C 90 52 73 7E F8 65 C6 3B 60 B0 46 4D B4 4C DC B5 C4 82 98

Is this information correct? [y/N]: y

Please specify the request ticket generated on your Icinga 2 master (optional).
(Hint: # icinga2 pki ticket --cn 'agent3.test.alt'):

No ticket was specified. Please approve the certificate signing request manually
on the master (see 'icinga2 ca list' and 'icinga2 ca sign --help' for details).
Please specify the API bind host/port (optional):
Bind Host []:
Bind Port []:

Accept config from parent node? [y/N]: y
Accept commands from parent node? [y/N]: y

Reconfiguring Icinga...
Disabling feature notification. Make sure to restart Icinga 2 for these changes to take effect.
Enabling feature api. Make sure to restart Icinga 2 for these changes to take effect.

Local zone name [agent3.test.alt]:
Parent zone name [master]:

Default global zones: global-templates director-global
Do you want to specify additional global zones? [y/N]: y

Please specify the name of the global Zone: global-commands

Do you want to specify another global zone? [y/N]:
Do you want to disable the inclusion of the conf.d directory [Y/n]:
Disabling the inclusion of the conf.d directory...

Done.
Now restart your Icinga 2 daemon to finish the installation!
[root@agent3 ~]#

```

Рис. 104 – Регистрация агента в режиме sign on demand

Пример конфигурации агента в режиме sign on demand:

```
# icinga2 node wizard
Welcome to the Icinga2 Setup Wizard!
```

We will guide you through all required configuration details.

Please specify if this is an agent/satellite setup ('n' installs a master setup) [Y/n]:

Starting the Agent/Satellite setup routine...

Please specify the common name (CN) [agent3.test.alt]:

Please specify the parent endpoint(s) (master or satellite) where this node should connect to:

Master/Satellite Common Name (CN from your master/satellite node): master1.test.alt

Do you want to establish a connection to the parent node from this node? [Y/n]:

Please specify the master/satellite connection information:

Master/Satellite endpoint host (IP address or FQDN):
master1.test.alt

Master/Satellite endpoint port [5665]:

Add more master/satellite endpoints? [y/N]:

Parent certificate information:

```
Version:          3
Subject:          CN = master1.test.alt
Issuer:           CN = Icinga CA
Valid From:       Jul 1 07:11:38 2024 GMT
Valid Until:      Aug 1 07:11:38 2025 GMT
Serial:
```

```
c8:74:1e:c2:8f:6a:8b:bf:bc:61:97:3d:64:90:5a:bc:5d:54:62:9a
```

```
Signature Algorithm: sha256WithRSAEncryption
```

```
Subject Alt Names:  master1.test.alt
```

```
Fingerprint:       19 07 D1 40 51 7B EE 74 6C C0 57 21 8C 90
52 73 7E F8 65 C6 3B 60 B0 46 4D B4 4C DC B5 C4 82 98
```

Is this information correct? [y/N]: y

Please specify the request ticket generated on your Icinga2 master (optional).

(Hint: # icinga2 pki ticket --cn 'agent3.test.alt'):

No ticket was specified. Please approve the certificate signing request manually

on the master (see `icinga2 ca list` and `icinga2 ca sign -help` for details).

ЛКНВ.11100-01 90 03

Please specify the API bind host/port (optional):

Bind Host []:

Bind Port []:

Accept config from parent node? [y/N]: Y

Accept commands from parent node? [y/N]: Y

Reconfiguring Icinga...

Disabling feature notification. Make sure to restart Icinga2 for these changes to take effect.

Enabling feature api. Make sure to restart Icinga2 for these changes to take effect.

Local zone name [agent3.test.alt]:

Parent zone name [master]: master

Default global zones: global-templates director-global

Do you want to specify additional global zones? [y/N]: y

Please specify the name of the global Zone: global-commands

Do you want to disable the inclusion of the conf.d directory [Y/n]:

Disabling the inclusion of the conf.d directory...

Done.

Now restart your Icinga2 daemon to finish the installation!

После окончания конфигурации необходимо перезапустить сервис:

```
# systemctl restart icinga2.service
```

Информация о мастер-узле и об агенте будет добавлена в файл

/etc/icinga2/zones.conf:

```
object Endpoint "master1.test.alt" {
    host = "master1.test.alt"
    port = "5665"
}

object Zone "master" {
    endpoints = [ "master1.test.alt" ]
}

object Endpoint "agent3.test.alt" {
}

object Zone "agent3.test.alt" {
    endpoints = [ "agent3.test.alt" ]
}
```

```

        parent = "master"
    }

    object Zone "global-templates" {
        global = true
    }

    object Zone "director-global" {
        global = true
    }

    object Zone "global-commands" {
        global = true
    }

```

Созданный запрос необходимо подписать на мастер-узле.

На мастер-узле посмотреть запросы, ожидающие подпись сертификата, можно

с помощью команды:

```

# icinga2 ca list
Fingerprint          | Timestamp                | Signed | Subject
-----|-----|-----|-----
77a930d263ed2...8067| Jul 02 09:03:51 2024 GMT|        | CN = agent3.test.alt

```

Чтобы отобразить все запросы, используется параметр `all`:

```
# icinga2 ca list --all
```

Примечание. Запросы на подпись сертификата старше 1 недели автоматически удаляются.

Примечание. Чтобы получить подробную информацию о запросе в формате JSON, необходимо добавить в команду параметр `json`.

Для подписания запроса, используется команда `icinga2 ca sign` с отпечатком запроса (`fingerprint`) в качестве аргумента (рис. 105):

```
# icinga2 ca sign 77a930d263ed2...8067
```

Для удаления нежелательного запроса используется команда `icinga2 ca remove`:

```
# icinga2 ca remove 77a930d263ed2...9195e146098067
```

Восстановить удаленный сертификат, можно с помощью команды `icinga2 ca restore`.

```

Терминал - root@master1: /root
Файл  Правка  Вид  Терминал  Вкладки  Справка
[root@master1 ~]# icinga2 ca list
Fingerprint                                     | Timestamp                               | Signed | Subject
-----|-----|-----|-----
77a930d263ed231382a1958099660535edca75c9a77ba3f5f59195e146098067 | Feb 18 09:03:51 2024 GMT |         | CN = agent3.test.alt
[root@master1 ~]# icinga2 ca sign 77a930d263ed231382a1958099660535edca75c9a77ba3f5f59195e146098067
information/cli: Signed certificate for 'CN = agent3.test.alt'.
[root@master1 ~]#

```

Рис. 105 – Список запросов и подпись запроса на сертификат

7.7.3.1.3. Настройка взаимодействия мастера с агентами

Существуют разные способы гарантировать, что узлы кластера Icinga2 выполняют проверки, отправляют уведомления и т. д.

Предпочтительный метод – настроить объекты мониторинга на мастере и распространить конфигурацию на спутники и агенты.

В режиме Top Down Command Endpoint узел Icinga2 удаленно выполняет команды на указанной конечной точке. Конфигурация объекта host/service находится на мастере/спутнике, и агенту нужны только доступные определения объекта CheckCommand (см. п. 7.7.3.1.4).

Примечание. Не требуется никакой локальной настройки агента, за исключением определений CheckCommand, которые можно синхронизировать с помощью глобальной зоны. Поэтому следует закомментировать строку `include_recursive conf.d в /etc/icinga2/icinga2.conf` на агенте.

В примере, рассматриваемом ниже:

- master1.test.alt – мастер конфигурации;
- agent1.test.alt, agent2.test.alt – агенты.

Примечание. Конфигурация зон и Endpoint (конечных точек) на агенте выполняется при конфигурировании узла.

Примечание. Каждому агенту требуется собственная конфигурация зоны и конечной точки (Endpoint). Лучше всего использовать FQDN имя агента для всех имен объектов.

На Мастер-узле необходимо выполнить следующие действия:

- 1) включить конфигурации конечной точки и определить две зоны. Для этого в файл `/etc/icinga2/zones.conf` добавить информацию об агенте (в поле `host` должен быть указан адрес клиентского узла, зона `master` является родительской для зон клиентских узлов):

```
object Endpoint "master1.test.alt" {
    host = "192.168.0.170"
}
object Endpoint "agent1.test.alt" {
    host = "192.168.0.151"
    log_duration = 0 // Отключить ротацию журнала
}
object Endpoint "agent2.test.alt" {
    host = "192.168.0.152"
    log_duration = 0 // Отключить ротацию журнала
}
object Zone "master" {
    endpoints = [ "master1.test.alt" ]
}
object Zone "agent1.test.alt" {
    endpoints = [ "agent1.test.alt" ]
    parent = "master"
}
object Zone "agent2.test.alt" {
    endpoints = [ "agent2.test.alt" ]
    parent = "master"
}
object Zone "global-templates" {
    global = true
}

object Zone "director-global" {
    global = true
}

object Zone "global-commands" {
    global = true
}
```

- 2) создать файл конфигурации для мониторинга машин, входящих в зону `master`. Для этого создать каталог `/etc/icinga2/zones.d/master`:

```
# mkdir -p /etc/icinga2/zones.d/master
```


В этом каталоге создать файл `hosts.conf`, в который добавить информацию об агентах:

```
object Host "agent1.test.alt" {
    import "generic-host"
    import "nagwad-host"
    address = "192.168.0.151"
    vars.agent_endpoint = name //follows the convention that host
name == endpoint name
}
object Host "agent2.test.alt" {
    import "generic-host"
    import "nagwad-host"
    address = "192.168.0.152"
    vars.agent_endpoint = name //follows the convention that host
name == endpoint name
}
```

где:

- `import "generic-host"` – импорт стандартной конфигурации из шаблона `generic-host`;
- `import "nagwad-host"` – импорт конфигурации `nagwad` из шаблона `nagwad-host`;
- `address` – IP-адрес клиентского узла;
- `agent_endpoint` – пользовательская переменная, которая служит двум целям:

а) ей могут соответствовать правила применения службы;

б) правила применения могут получать его значение и присваивать его атрибуту `command_endpoint`;

3) проверить целостность конфигурации `Icinga2`, выполнив команду:

```
# icinga2 daemon -C
```

4) перезапустить сервис `Icinga2` на мастер-узле:

```
# systemctl restart icinga2
```

В веб-интерфейсе Icinga2 (раздел «Обзор» → «Узлы») агент сначала появится в статусе «Рассматриваемый» (рис. 106), а затем, если все настроено правильно, перейдет в статус «Включен» (рис. 107).



Рис. 106 – Статус узла «Рассматриваемый»



Рис. 107 – Статус узла «Включен»

После окончания настройки мониторинга клиентов, они будут отображаться в веб-интерфейсе Icinga2 (рис. 108).

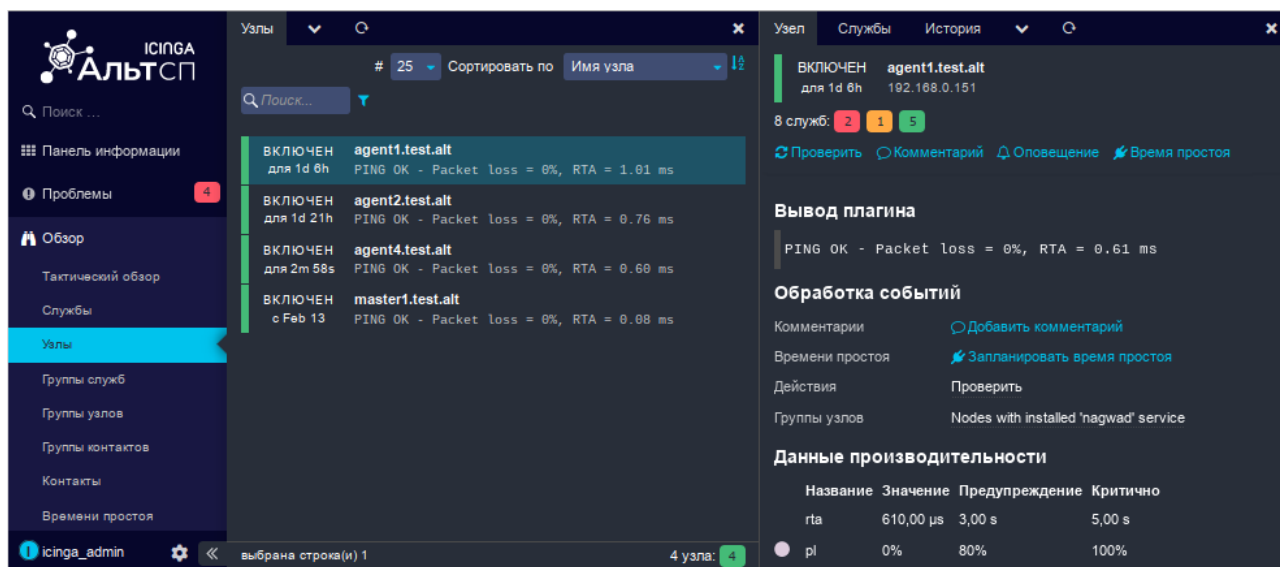


Рис. 108 – Клиенты мониторинга

7.7.3.1.4. Глобальные зоны

Глобальные зоны можно использовать для синхронизации универсальных объектов конфигурации со всеми зависящими от них узлами.

Примечание. Проверяемые объекты (хосты и службы) нельзя поместить в глобальную зону.

Конфигурация объекта зоны должна быть развернута на всех узлах, которые должны получать файлы глобальной конфигурации.

Примечание. Глобальные зоны по умолчанию, созданные мастерами установки, называются `global-templates` и `director-global`. Зона `director-global` зарезервирована для использования Icinga Director, в этой зоне нельзя размещать какие-либо конфигурации вручную.

Глобальная зона `global-commands`, в которой определен объект `CheckCommand` `check_nagwad`, должна быть добавлена на этапе конфигурирования узлов (см. выше). Если это не сделано на мастере и на агентах, в файл `/etc/icinga2/zones.conf` необходимо добавить информацию о глобальной зоне `global-commands`:

```
object Zone "global-commands" {
    global = true
}
```

7.7.3.2. Веб-интерфейс Icinga Director

Icinga Director предоставляет веб-интерфейс для управления конфигурацией Icinga2. Данный модуль позволяет описывать объекты Icinga (Services, Commands, Hosts) в веб-интерфейсе, используя гибкое и понятное меню.

Icinga Director не вносит никаких правок в классические конфигурационные файлы Icinga (в каталоге `/etc/icinga2`), а имеет свою независимую конфигурацию. Конфигурация хранится в БД и выгружается в текстовый вид, для чтения серверной частью Icinga, по требованию (при развертывании). Director ведет журнал всех изменений и предоставляет возможность отката на предыдущие версии конфигурации.

В файловой системе текущую и последнюю конфигурации можно найти в каталоге `/var/lib/icinga2/api/packages/director`. В веб-интерфейсе Director для просмотра выгруженных файлов конфигурации (рис. 109) необходимо перейти в раздел «Управление Icinga» → «Развертывания» и нажать кнопку «Render Config».

Примечание. Не следует напрямую редактировать выгруженные файлы конфигурации в файловой системе. Для работы нужно использовать только графический интерфейс или API.

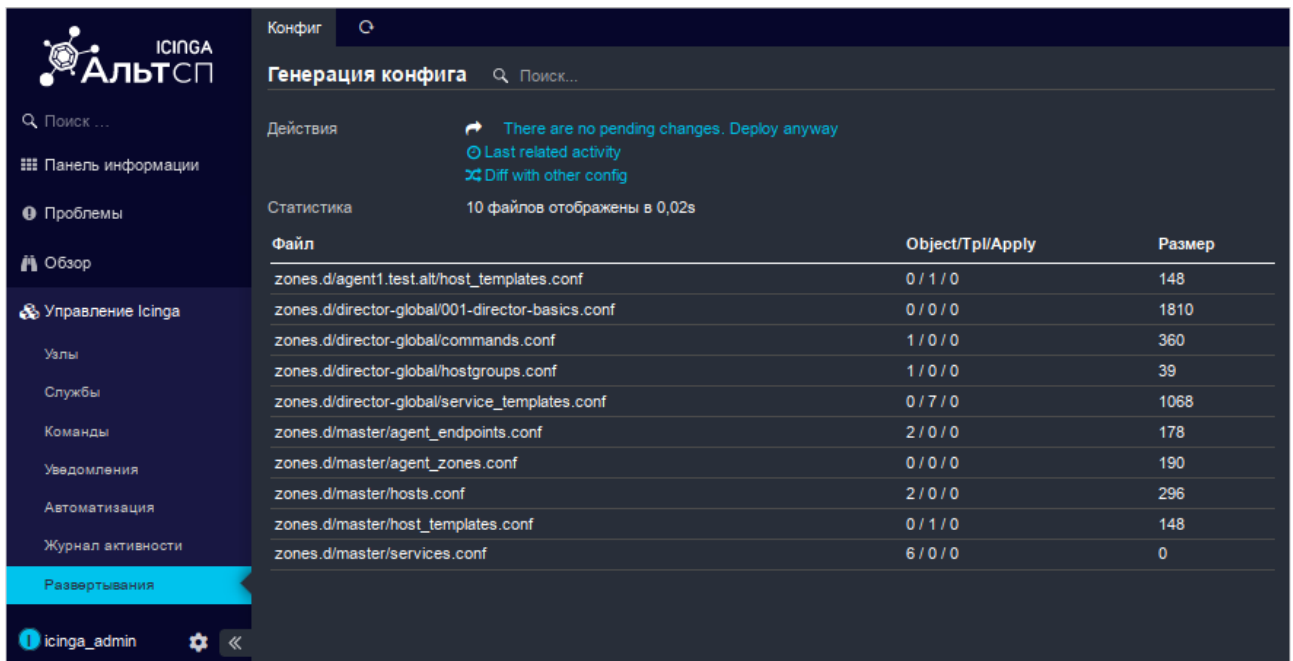


Рис. 109 – Файлы конфигурации Icinga Director

7.7.3.2.1. Установка Icinga Director

7.7.3.2.1.1. Установка пакетов

Для управления конфигурацией посредством веб-интерфейса, необходимо на мастер-узле установить пакет:

```
# apt-get install icingaweb2-module-director
```

7.7.3.2.1.2. Создание базы данных

MySQL/MariaDB

Создать пользователя director и базу данных director (пароль необходимо запомнить):

```
$ mysql -uroot -p
Enter password:
MariaDB [(none)]> create database director character set 'utf8'
collate utf8_general_ci;
MariaDB [(none)]> grant all privileges on director.* to
director@localhost identified by '<пароль>';
MariaDB [(none)]> quit;
```

PostgreSQL

Установить пакет:

```
# apt-get install postgresql16-contrib
```

Создать пользователя `director` и базу данных `director` (потребуется также ввести пароль пользователя `postgres`):

```
# su - postgres -s /bin/sh -c 'createuser --no-superuser --no-createdb --no-createrole --encrypted --pwprompt director'
```

Введите пароль для новой роли:

Повторите его:

Пароль:

```
# su - postgres -s /bin/sh -c 'createdb -E utf8 -O director director'
```

Пароль:

Включить расширение `pgcrypto`:

```
# psql -U postgres
```

Пароль пользователя `postgres`:

```
psql (16.3)
```

Введите "help", чтобы получить справку.

```
postgres=# create extension pgcrypto;
```

```
CREATE EXTENSION
```

```
postgres=# \q
```

7.7.3.2.1.3. Подключение базы данных для Icinga Director

В Icinga необходимо создать запись о новом ресурсе с типом «База данных SQL», который будет ссылаться на базу данных `director`. Для этого в веб-интерфейсе Icinga Web 2 следует выбрать пункт «Настройки» → «Приложение», перейти на вкладку «Ресурсы» (рис. 110) и нажать кнопку «Создание нового ресурса».

В открывшемся окне введите данные подключения к базе данных `director` (рис. 111), проверить конфигурацию, нажав кнопку «Проверить конфигурацию», и, если проверка прошла успешно, сохранить новый ресурс, нажав кнопку «Сохранить изменения».

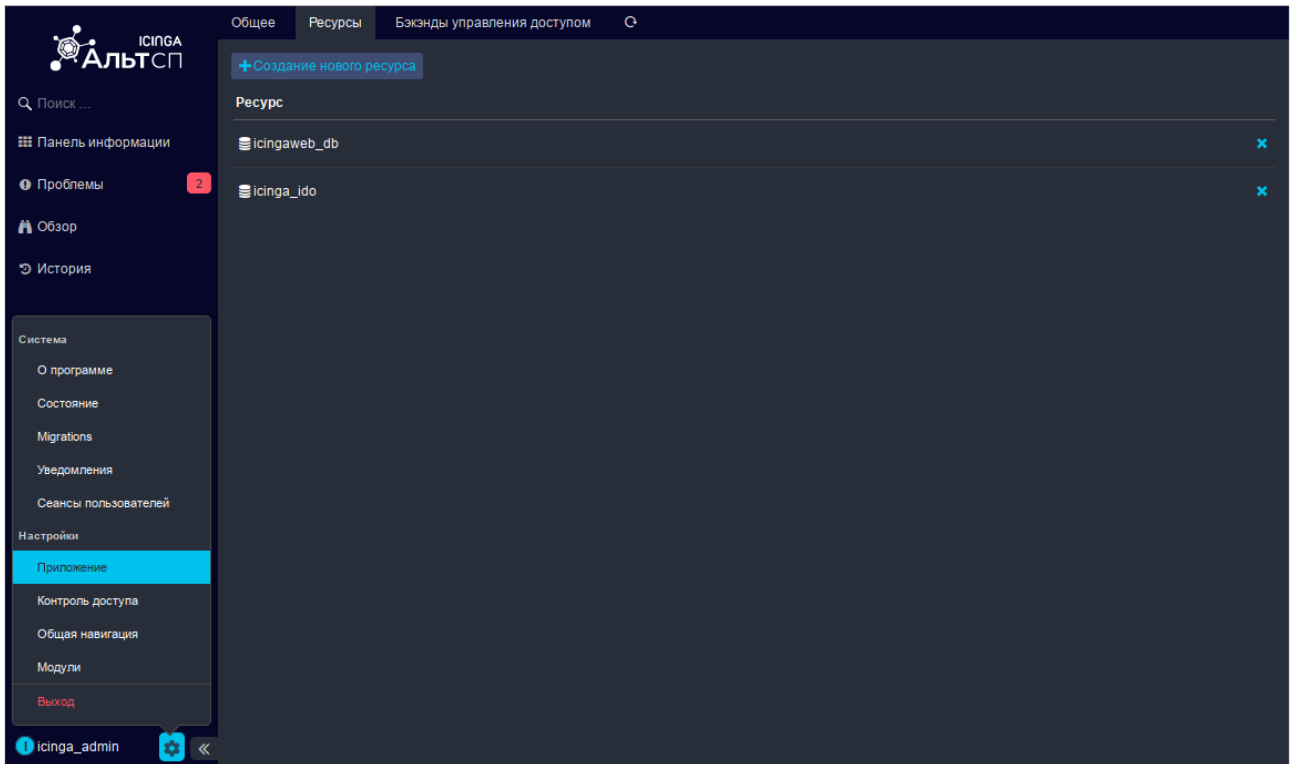


Рис. 110 – Список ресурсов

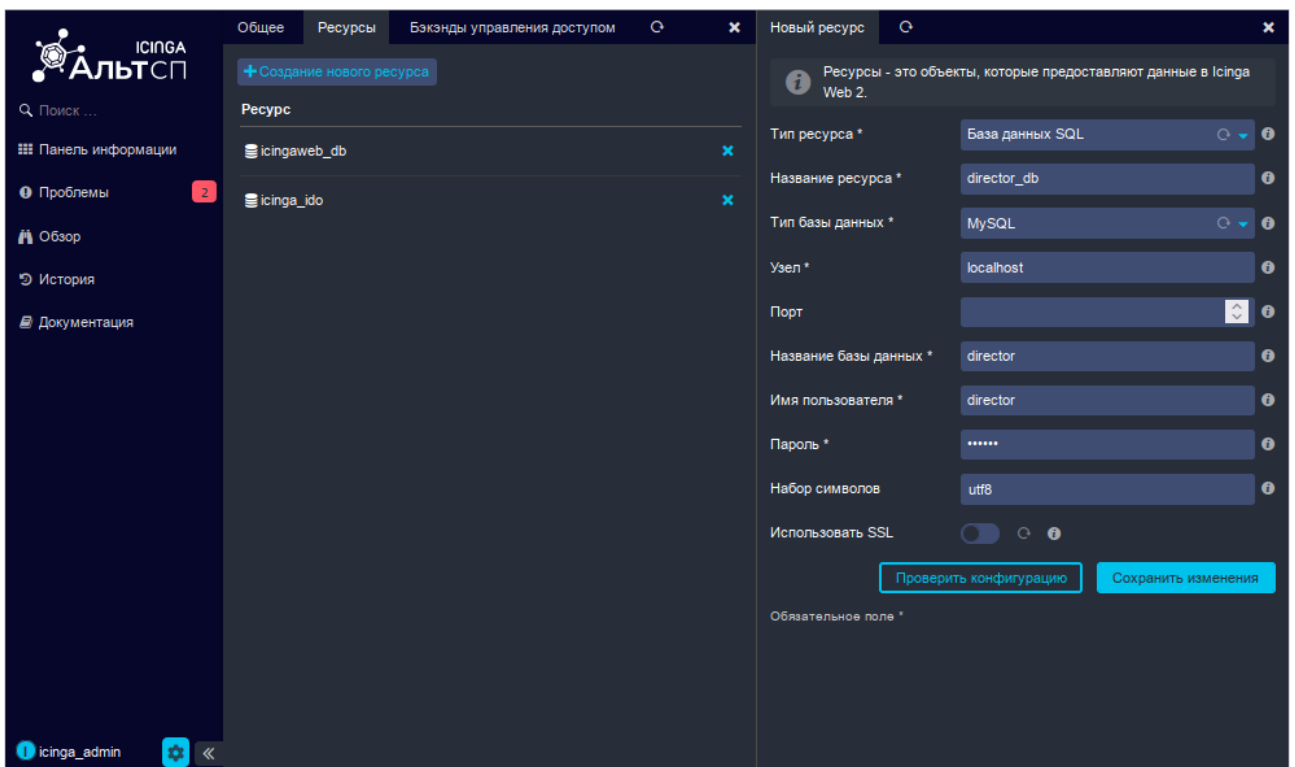


Рис. 111 – Создание нового ресурса

7.7.3.2.1.4. Включение модуля Icinga Director

Для просмотра списка модулей перейти в раздел «Настройки» → «Модули» (рис. 112).

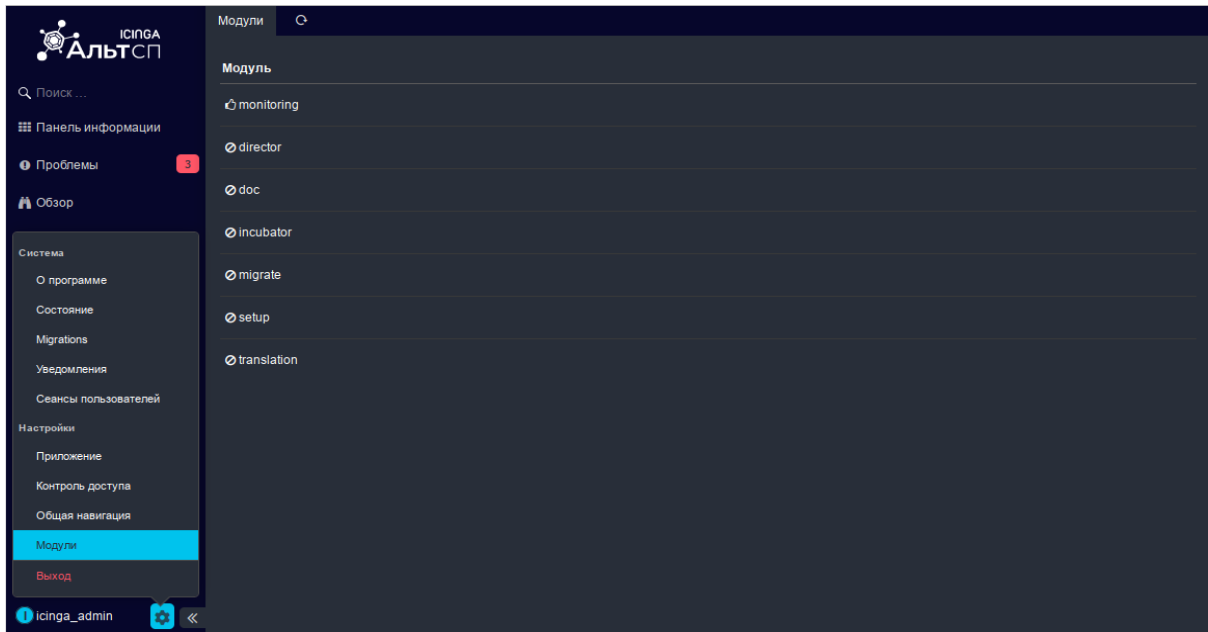


Рис. 112 – Список модулей

Предварительно необходимо включить модуль `incubator`. Для этого следует выбрать данный модуль в списке модулей, и, в открывшейся справа форме, нажать на значок «Обновить» справа от слова «disabled» в строке «Состояние» (рис. 113).

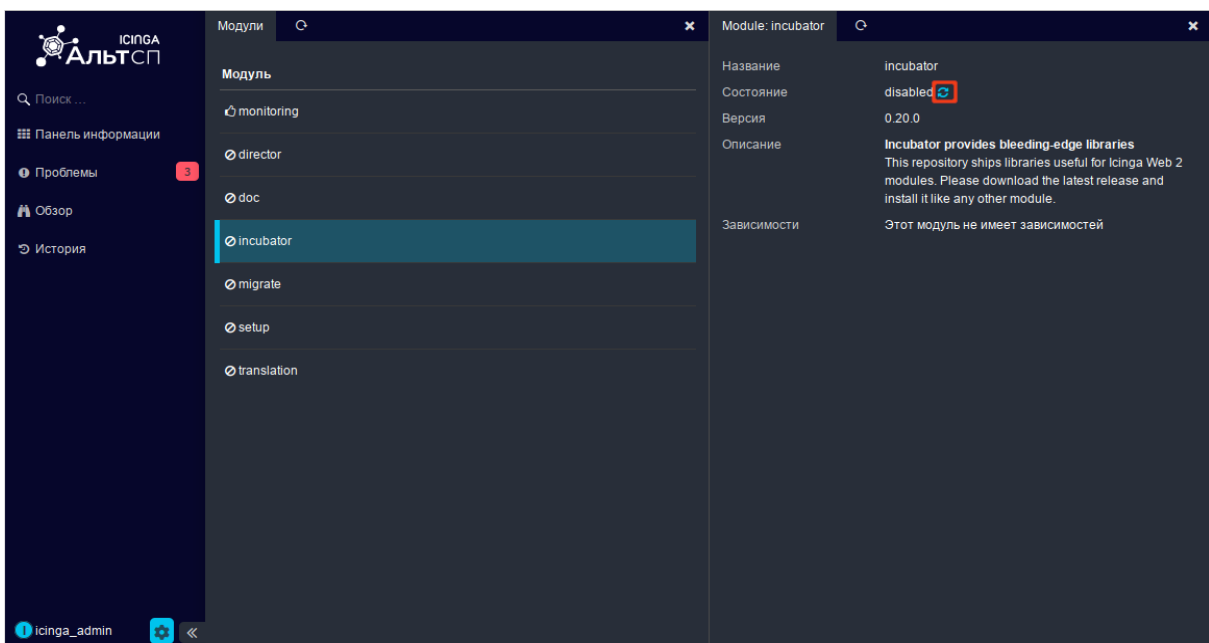


Рис. 113 – Модуль `incubator`

Состояние модуля должно измениться с disabled на enabled. Далее нужно повторить эти действия для модуля director (рис. 114).

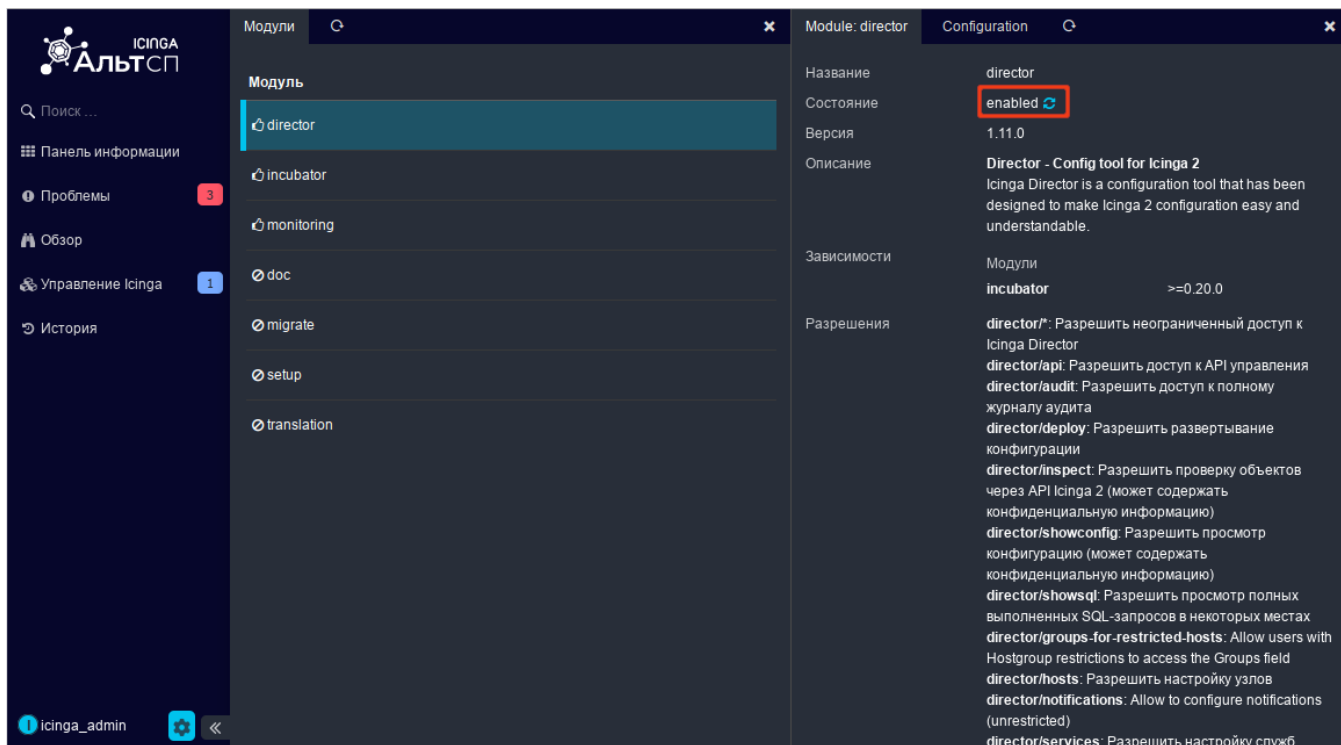


Рис. 114 – Модуль director

После того как модуль director включен, необходимо перейти на вкладку «Configuration» (рис. 115) и выполнить настройку модуля. Для этого выбрать из выпадающего списка «Источник БД» ресурс director_db. Будет выведено сообщение о том, что ассоциированная база данных пуста и не имеет схемы (рис. 116). Для создания схемы необходимо нажать кнопку «Создание схемы базы данных».

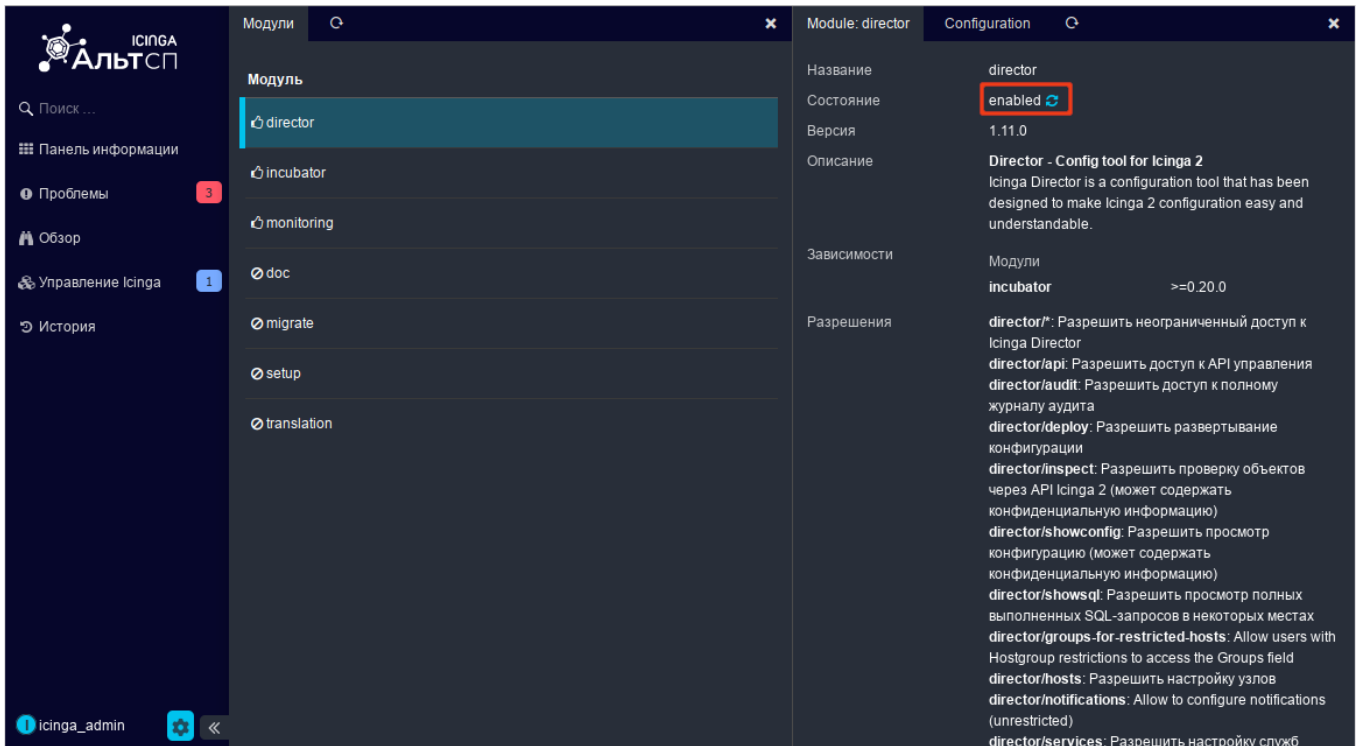


Рис. 115 – Модуль director вкладка «Configuration»

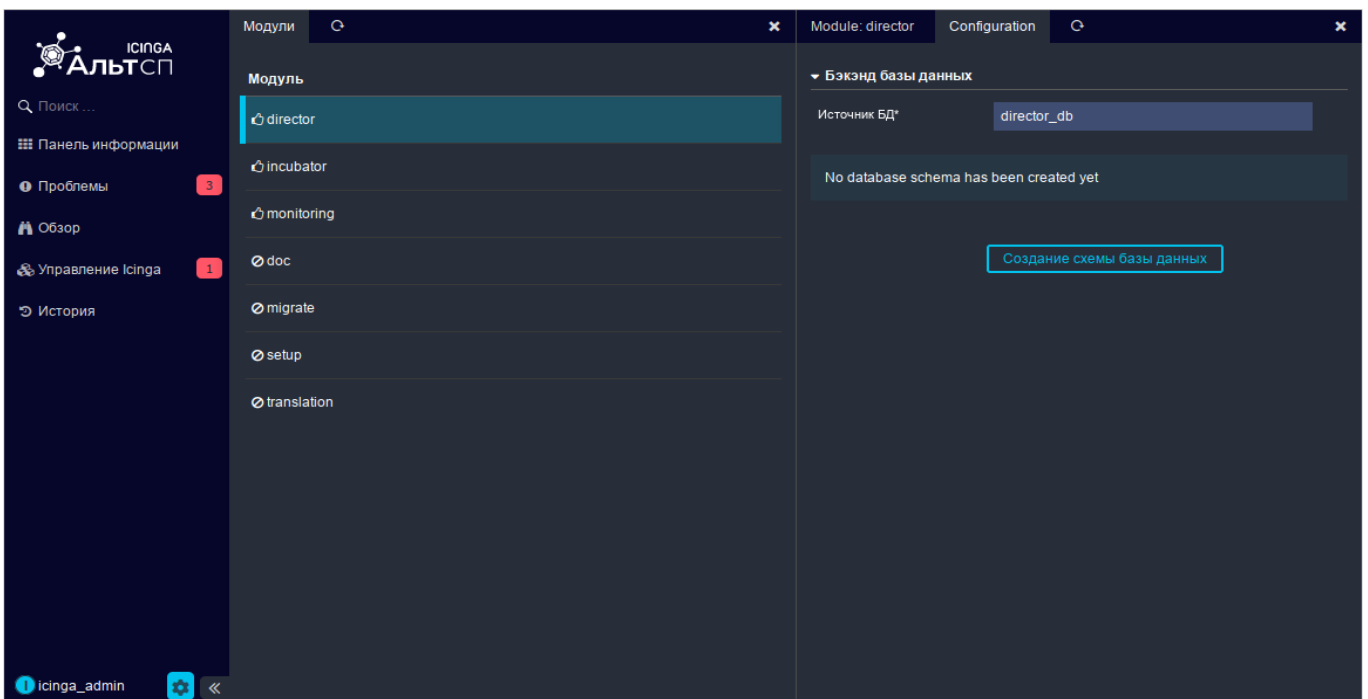


Рис. 116 – Ассоциированная база данных пуста и не имеет схемы

В открывшейся форме необходимо настроить параметры подключения модуля Director к серверу Icinga (рис. 117):

- «Имя конечной точки» – имя Common Name (CN) из SSL-сертификата, который был сгенерирован в процессе включения Icinga API. По умолчанию в качестве CN для SSL-сертификата используется FQDN-имя сервера, на котором выполняется включение Icinga API;
- «Icinga Host» – имя сервера Icinga;
- «Порт» – порт Icinga API по умолчанию (5665);
- «Имя пользователя API» – имя пользователя для подключения к API (root);
- «Пароль API» – пароль для подключения к API.

Примечание. Имя и пароль пользователя для подключения к API указаны в файле `/etc/icinga2/conf.d/api-users.conf`.

Примечание. Если в дальнейшем планируется делегирование прав доступа к API можно создать отдельного пользователя API Icinga2 для Director с полным доступом к API, добавив следующие строки в файл `/etc/icinga2/conf.d/api-users.conf`:

```
object ApiUser "director" {  
    password = "aaabea888fd23e777" //change this  
    permissions = [ "*" ]  
}
```

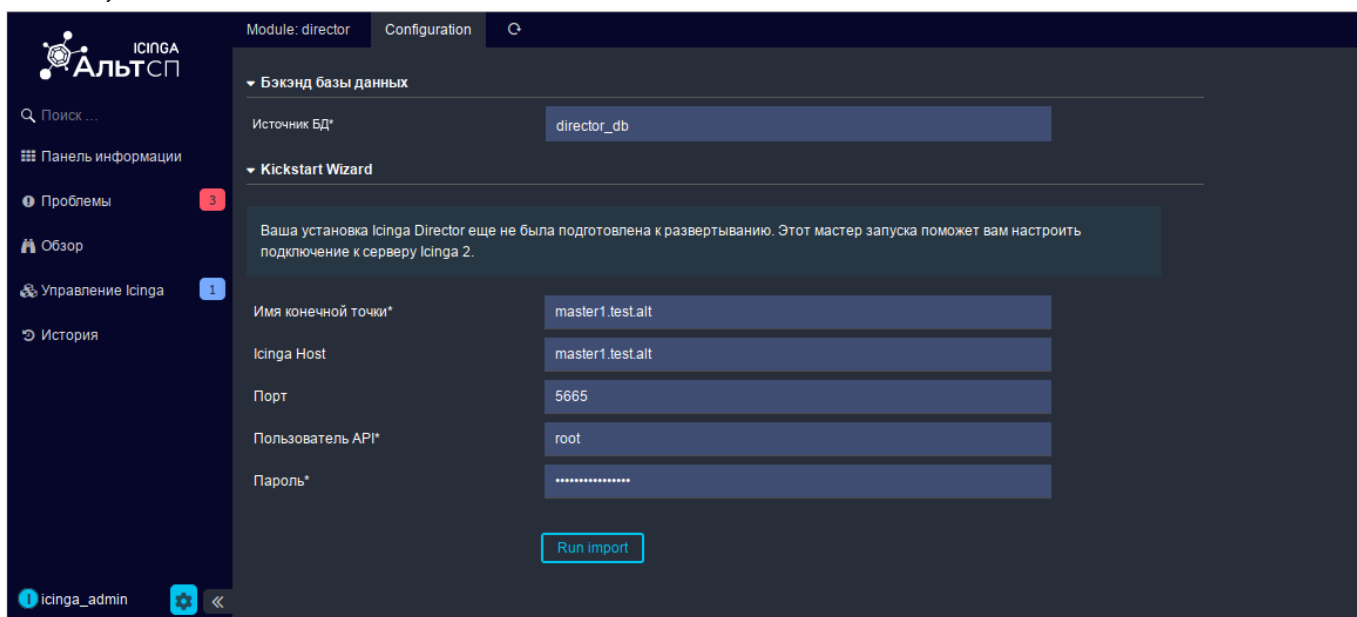


Рис. 117 – Настройка подключения к серверу Icinga

После внесения изменений в файл `/etc/icinga2/conf.d/api-users.conf` необходимо перезапустить службу `icinga2`:

```
# systemctl restart icinga2
```

Запустить подключение, нажав на кнопку «Run Import». В случае успешного подключения будет выведено сообщение «Ваша база данных выглядит хорошо» (рис. 118).

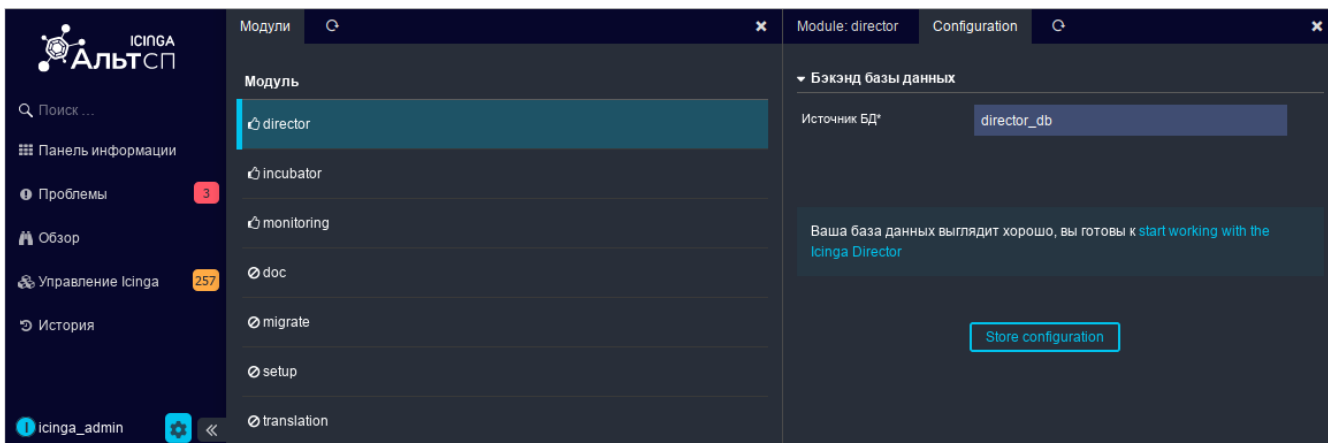


Рис. 118 – Подключение к Icinga

Включить и добавить в автозагрузку службу `icinga-director`:

```
# systemctl enable --now icinga-director.service
```

Для доступа к функциям подключенного модуля в главном меню навигации Icinga Web 2 используется пункт «Управление Icinga» (рис. 119).

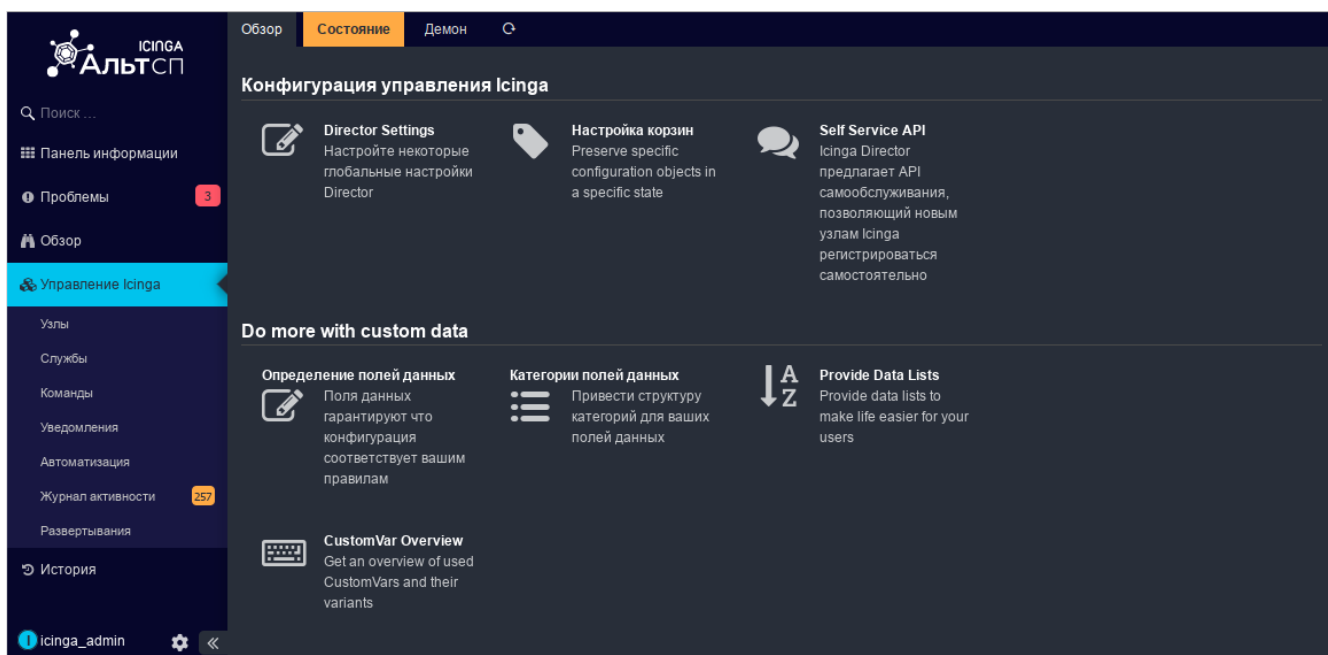


Рис. 119 – Управление Icinga

Примечание. В файле `/etc/icinga2/zones.conf` должна присутствовать запись о глобальной зоне `director-global`. Эта зона нужна для хранения общих объектов конфигурации, которые Icinga Director будет распространять на клиентов. Если записи о зоне нет, ее необходимо добавить, добавив в файл строки:

```
object Zone "director-global" {
    global = true
}
```

и перезапустить службу `icinga2`:

```
# systemctl restart icinga2
```

Для возможности запрашивания билетов для агента необходимо сгенерировать секретный ключ и записать его в файл `/etc/icinga2/constants.conf`:

- сгенерировать `TicketSalt`:

```
# openssl rand -base64 30
FbatRmRfzLccmuXQKQbZOapCoNLkYSEWs9eQkl0c
```

- записать полученный `TicketSalt` в файл `/etc/icinga2/constants.conf` в строку `const TicketSalt = ""`:

```
const TicketSalt = "FbatRmRfzLccmuXQKQbZOapCoNLkYSEWs9eQkl0c"
```

- и перезапустить службу `icinga2`:

```
# systemctl restart icinga2
```

7.7.3.2.2. Основные объекты конфигурации

Одним из основных принципов взаимосвязей объектов в Icinga2 является то, что сначала создаются шаблоны того-или иного вида объекта, а потом создаются сами объекты с привязкой к этим шаблонам. Шаблоны описывают одно или несколько схожих для некоего множества объектов значений свойств. Для объекта может быть создано любое необходимое количество шаблонов. Основное назначение шаблона – это определить параметры, характерные для некоторого массива объектов, чтобы в дальнейшем можно было применить эти параметры к этому массиву объектов.

Основные объекты конфигурации:

1) Команды (`Command`) и шаблоны команд (`Command Templates`). Команда – это предопределенное действие, которое выполняется на проверяемой системе или удаленно проверяет систему.

Атрибуты команды:

- описание базовых параметров и пути запуска скрипта или утилиты, выполняющих проверку (например, скрипты удаленной и локальной проверки);
- аргументы команды, то есть сопоставление ключей запуска или с переменными среды Icinga, например, \$address\$ (адрес хоста, к которому применяется проверка), или с вычисляемыми значениями;
- переменные команды, то есть определенные пользователем переменные, задающие значение переменных.

Основные типы команд:

- Check command – команды проверок;
- Notification command – команды отсылки уведомлений (e-mail, SMS, службы сообщений);
- Event command – команды действий по отношению к узлу или сервису (перезагрузка, запуск дополнительных утилит и т. д.)

Шаблоны команд используются в том случае, когда необходимо задать некие общие параметры проверок или переменные для группы команд.

2) Служба (Service) – это сущность, описывающая проверку того или иного параметра системы указанной командой с некоторым набором параметров, определяющих среду вызова и исполнения этой команды. В частности, в свойствах службы задается то, где выполняется команда – на стороне сервера или на стороне агента. Также в свойствах службы может быть задано количество попыток выполнения команды, интервалы между попытками и другие параметры. Здесь можно выделить такие сущности, как:

- шаблоны служб (Service Templates) используются чтобы задать общие групповые характеристики. Это может быть частота проверок, общие переменные или назначение определенной функциональности (агент Icinga);
- правила применений служб (Service Apply Rules) – применение определенной службы к узлу или группе узлов на основе набора признаков. Это могут быть, как свойства узла (имя, адрес, принадлежность к группе), так и набор пользовательских переменных;

- группа служб (Service Groups) – может применяется для визуализации однотипных сервисов, определения прав пользователей Служб, или упрощения управления ими через API;
- наборы служб (Service Sets) – используется для назначения группы команд к группе хостов.

3) Узлы (Host) – это конечные компьютеры или сетевые устройства, однозначно идентифицируемые при помощи адреса, которые добавляются в систему мониторинга. Вспомогательные сущности:

- шаблоны узла (Host Templates) – представляют собой те или иные параметры настройки, которые могут быть применимы к одному или множеству узлов, а также могут содержать в себе привязку служб;
- группы узлов (Host Groups) – применяются для группировки узлов, настройки разграничения доступа или управления через API.

7.7.3.2.3. Пример настройки конфигурации Icinga

В данном разделе рассмотрен пример создания шаблона служб, набора служб на его основе и шаблона узла.

Этот раздел можно пропустить и развернуть готовую конфигурацию из корзины (см. п. 7.7.3.2.4).

7.7.3.2.3.1. Создание шаблона служб (Service Templates)

В первую очередь необходимо настроить шаблон службы, который будет использоваться для мониторинга систем и служб. В шаблоне определяется служба и часть системы, которая будет отслеживаться.

В данном примере создадим шаблон, который отслеживает доступность системы по ssh и использование диска.

Для создания шаблона служб перейти в веб-интерфейсе «Управление Icinga» в раздел «Службы», выбрать «Шаблоны служб» и на вкладке «Шаблоны» нажать ссылку «Добавить» (рис. 120).

В открывшейся справа форме создания шаблона службы (рис. 121) указать следующие данные:

- «Название» – произвольное имя службы;

- «Команда проверки» – команда, которая будет использоваться для проверки мониторинга, например, ssh, ping (можно начать вводить символы и выбрать из предложенного списка);

- «Run on Agent» – разрешить запуск команды проверки на стороне клиента.

Нажать кнопку «Добавить», чтобы сохранить шаблон службы.

Аналогичным способом создать шаблон службы проверки диска.

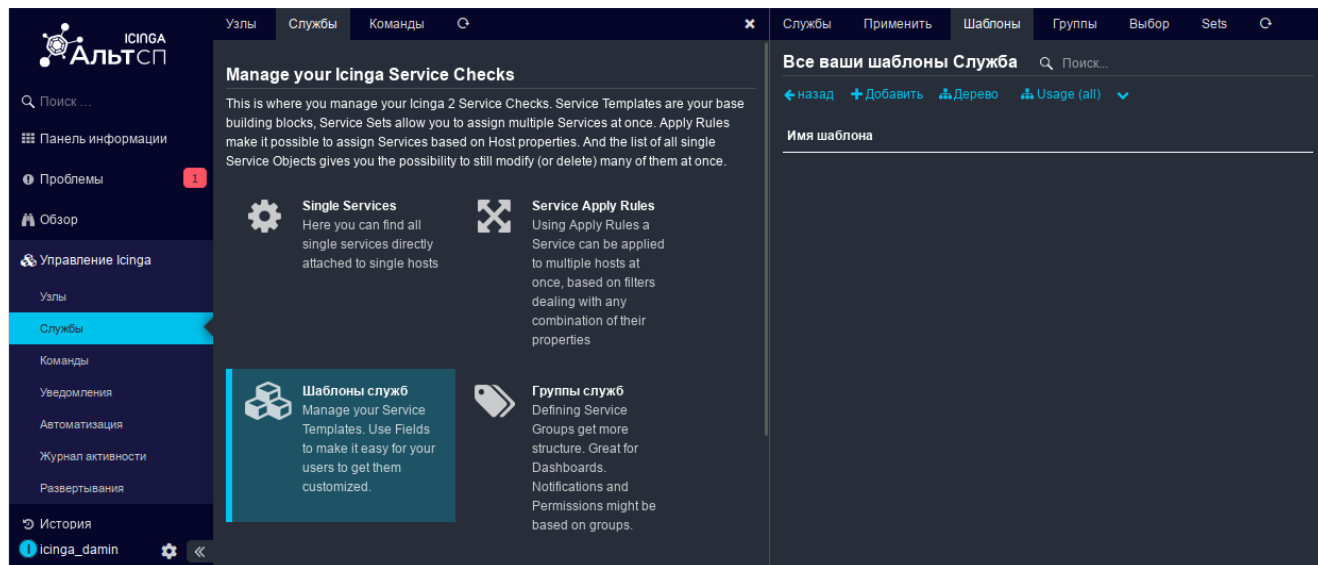


Рис. 120 – Раздел «Шаблоны служб»

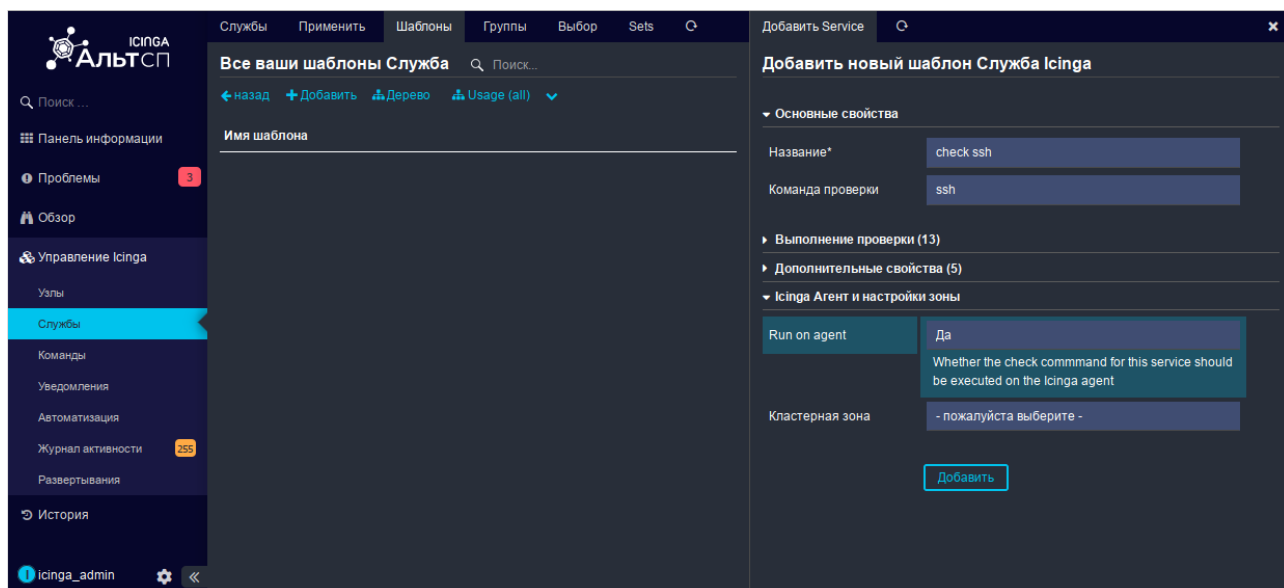


Рис. 121 – Создание шаблона службы

7.7.3.2.3.2. Создание набора служб (Service Set)

Следующий шаг – создание набора служб и добавление в него шаблонов служб. Для этого перейти в веб-интерфейсе «Управление Icinga» в раздел «Службы», выбрать «Наборы служб» и на вкладке «Sets» нажать ссылку «Добавить» (рис. 122).

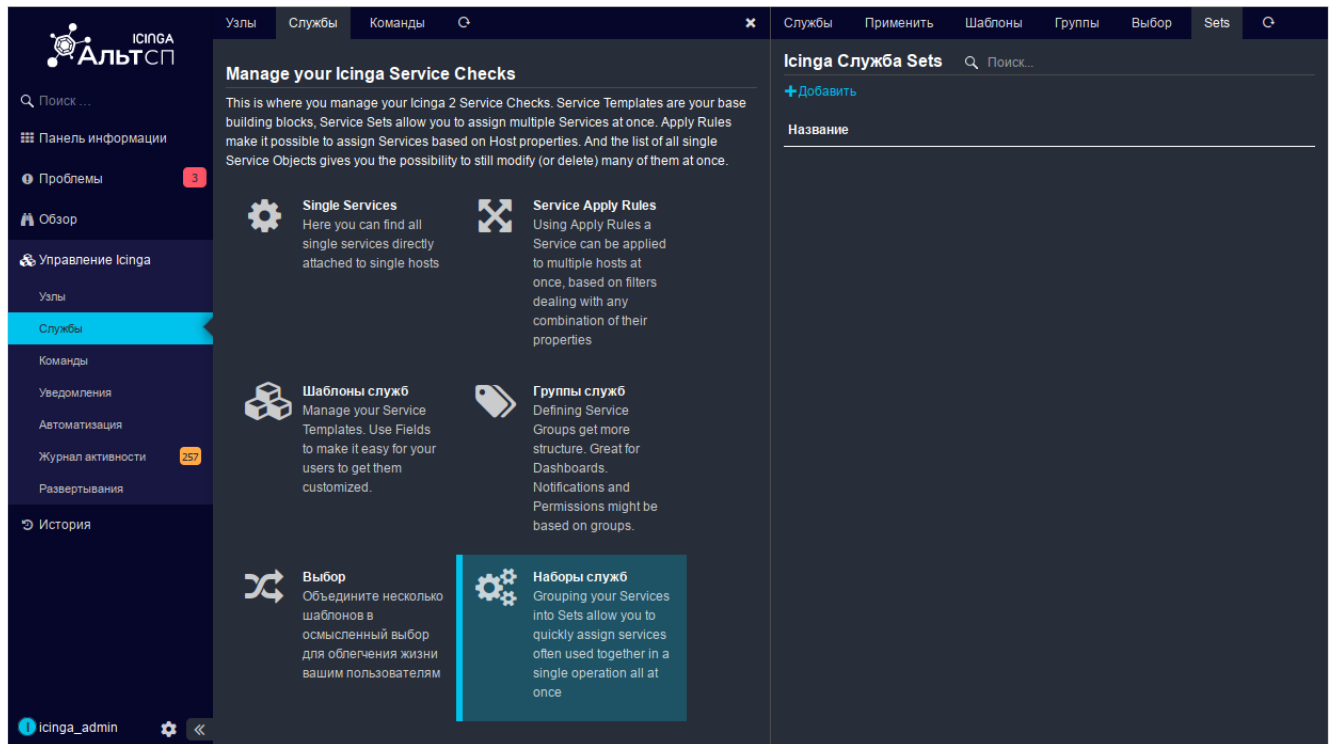


Рис. 122 – Раздел «Наборы служб»

В открывшейся справа форме создания шаблона службы (рис. 123) указать параметры:

- «Service set name» – краткое название, идентифицирующее этот набор служб;
- «Описание» – содержательное описание, объясняющее пользователям чего следует ожидать при назначении этого набора служб.

Нажать кнопку «Добавить», чтобы сохранить набор служб.

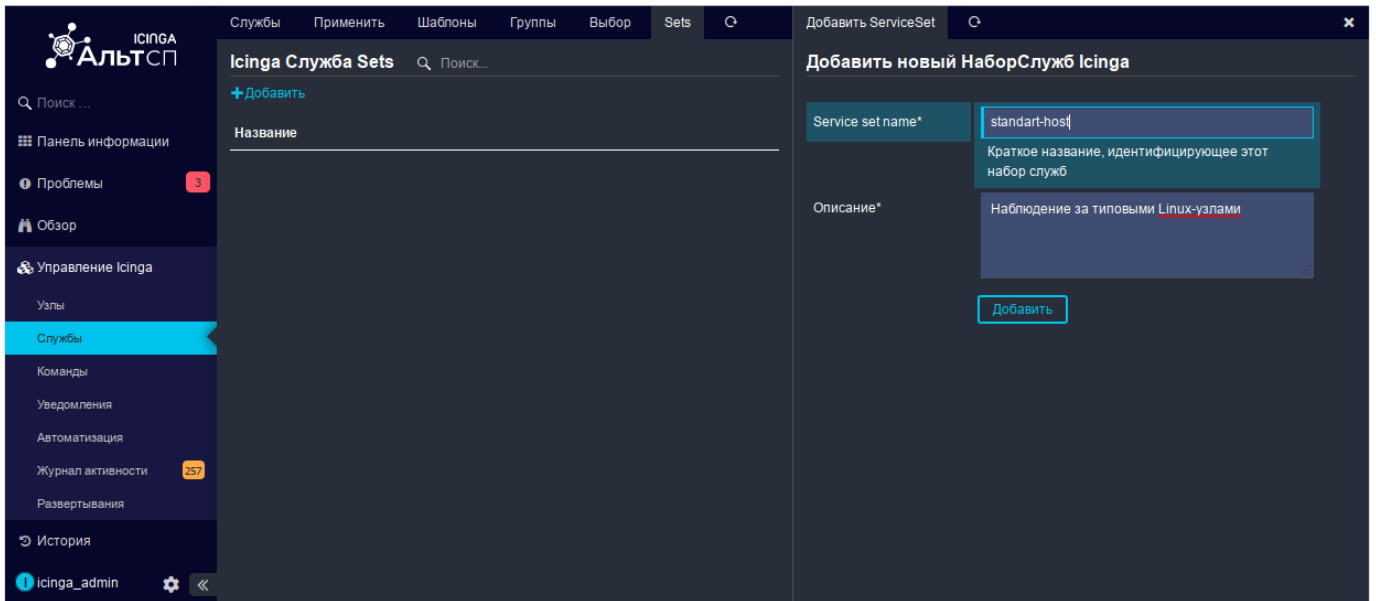


Рис. 123 – Новый набор служб

Далее следует добавить шаблоны служб в созданный набор сервисов. Для этого выбрать набор служб в списке на левой панели, перейти на вкладку «Services» на правой панели (рис. 124) и нажать ссылку «Добавить службу».

Выбрать имя службы в раскрывающемся списке «Imports» и нажать кнопку «Добавить» (рис. 125).

Повторить это действие для второго шаблона.

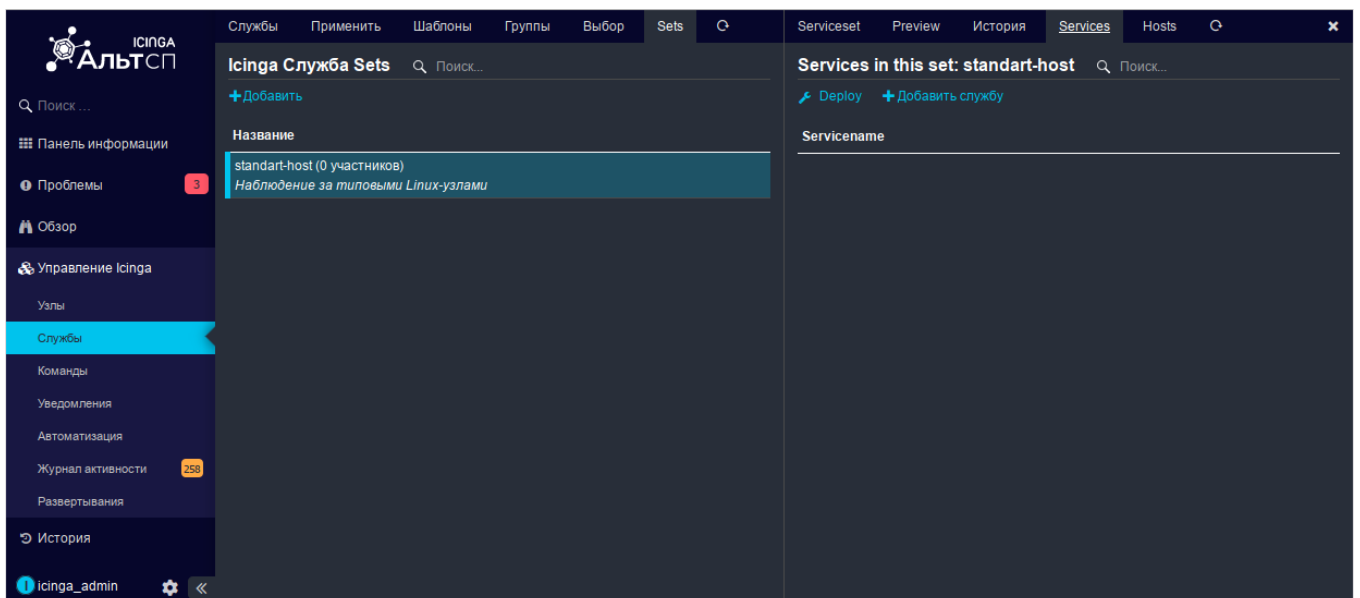


Рис. 124 – Список шаблонов в наборе служб

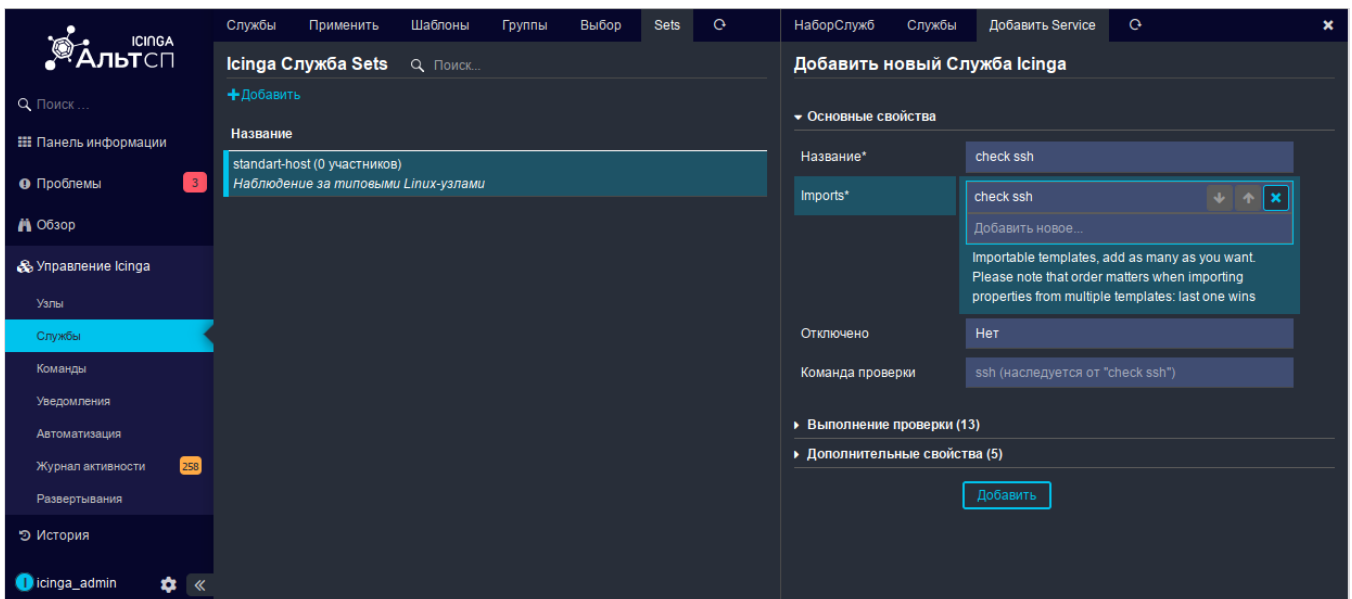


Рис. 125 – Добавление шаблона в набор служб

7.7.3.2.3.3. Создание шаблона узла (Host Templates)

На этом шаге необходимо создать шаблон узла и подключить к нему созданный выше набор служб.

Перейти в веб-интерфейсе «Управление Icinga» в раздел «Узлы», выбрать «Шаблоны узла» и на вкладке «Шаблоны» нажать ссылку «Добавить» (рис. 126).

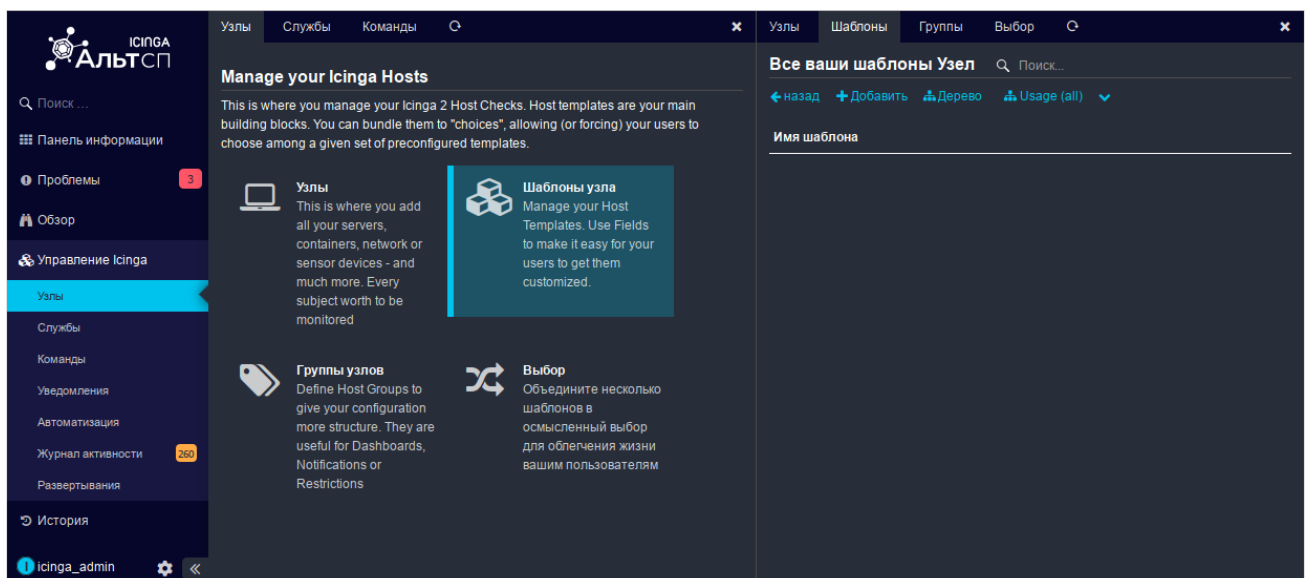


Рис. 126 – Вкладка «Шаблоны узла»

В открывшейся форме (рис. 127) необходимо заполнить следующие поля:

- «Название» – описательное имя шаблона узла (рекомендуется использовать значимые имена для шаблонов);
- «Команда проверки» – определение команды проверки (hostalive);
- «Icinga2 Агент» – установлен ли на этом узле агент Icinga2 (да);
- «Establish connection» – должен ли мастер активно пытаться подключиться к этому агенту (да);
- «Принять конфигурацию» – настроен ли агент на прием конфигурации (да).

Нажать кнопку «Добавить», чтобы сохранить шаблон узла.

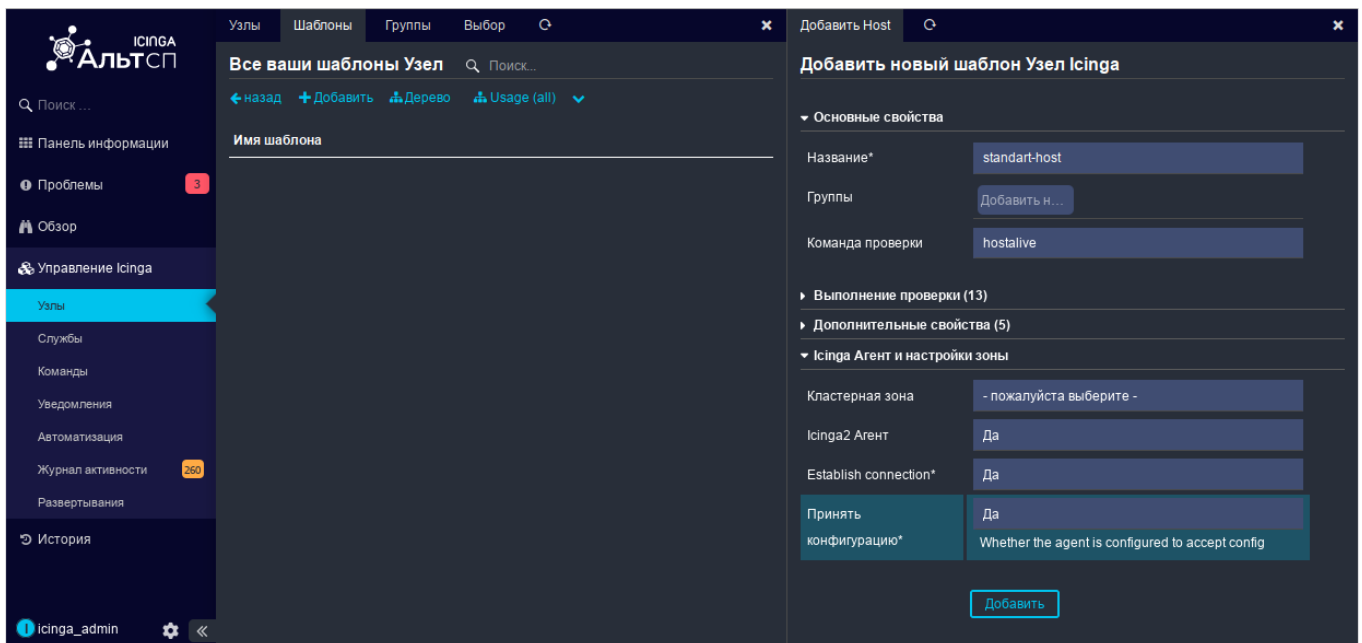


Рис. 127 – Создание шаблона узла

Для добавления набора служб в шаблон, следует выделить, созданный шаблон узла, затем на вкладке «Службы» нажать ссылку «Добавить набор служб» (рис. 128).

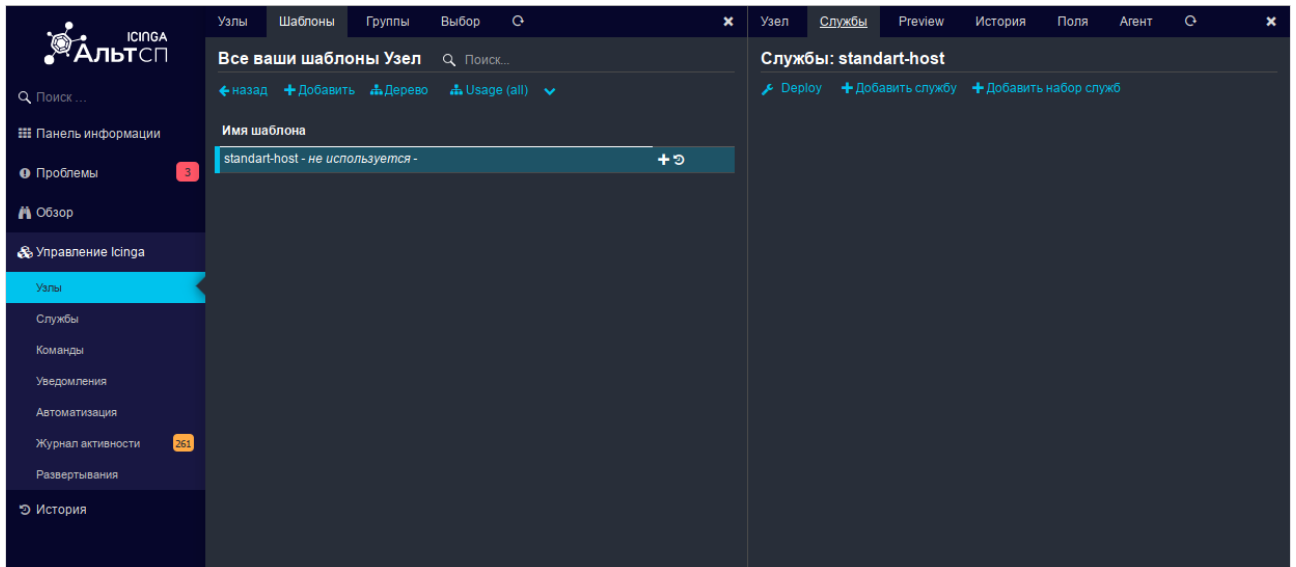


Рис. 128 – Ссылка «Добавить набор служб»

Нажмите кнопку «Добавить набор служб», чтобы добавить набор служб.

В открывшейся форме (рис. 129) необходимо выбрать созданный ранее набор услуг (standart-host) и нажать кнопку «Добавить».

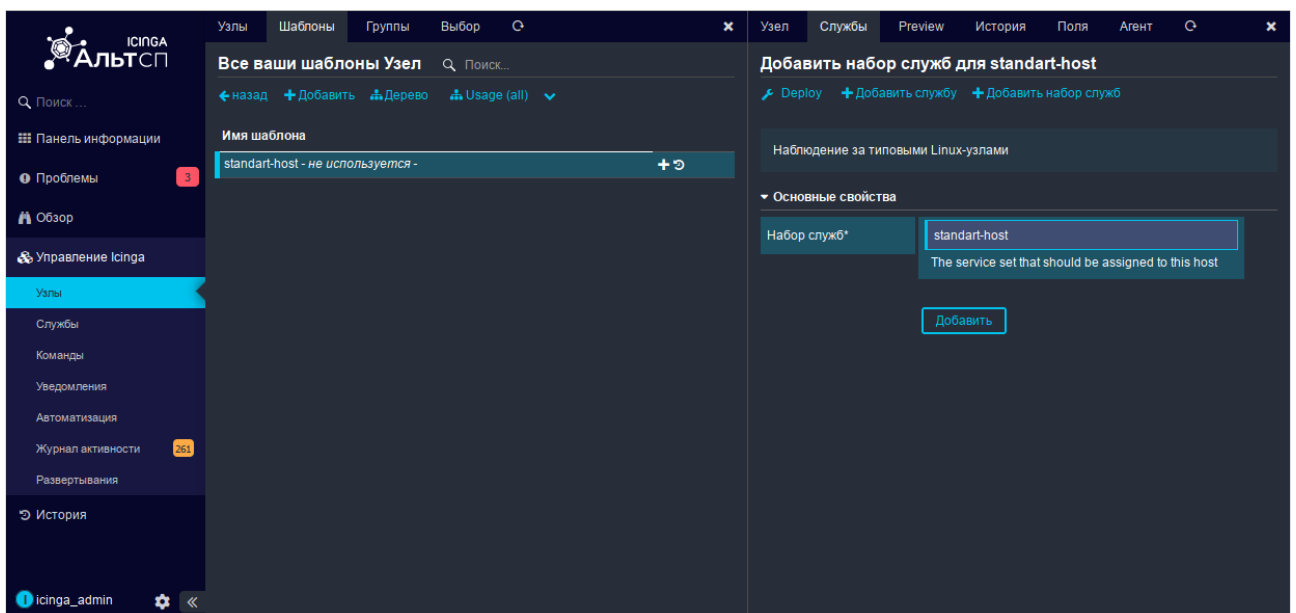


Рис. 129 – Добавление набора служб шаблону узла

На этом этапе шаблон узла создан и к нему добавлен набор служб. Теперь можно переходить к добавлению узла (агента) к Icinga2, с помощью Icinga Director (см. п. 7.7.3.2.5).

7.7.3.2.4. Импорт конфигурации Director из корзины

Корзины конфигурации позволяют экспортировать, импортировать, восстанавливать всю или часть конфигурации Icinga.

В пакете nagwad-icinga в каталоге `/usr/share/doc/nagwad-icinga-master*/` есть готовая корзина (basket) шаблонов в формате JSON для наблюдения за событиями Nagwad. Шаблон для добавления узла называется `d-nagwad-node`.

Для импорта конфигурации необходимо перейти в раздел «Управление Icinga», выбрать ссылку «Настройка корзин» и в открывшейся справа форме нажать ссылку «Загрузка» (рис. 130). Указать имя корзины, выбрать файл шаблонов в формате JSON, нажав кнопку «Обзор» (рис. 131) и нажать кнопку «Загрузка».

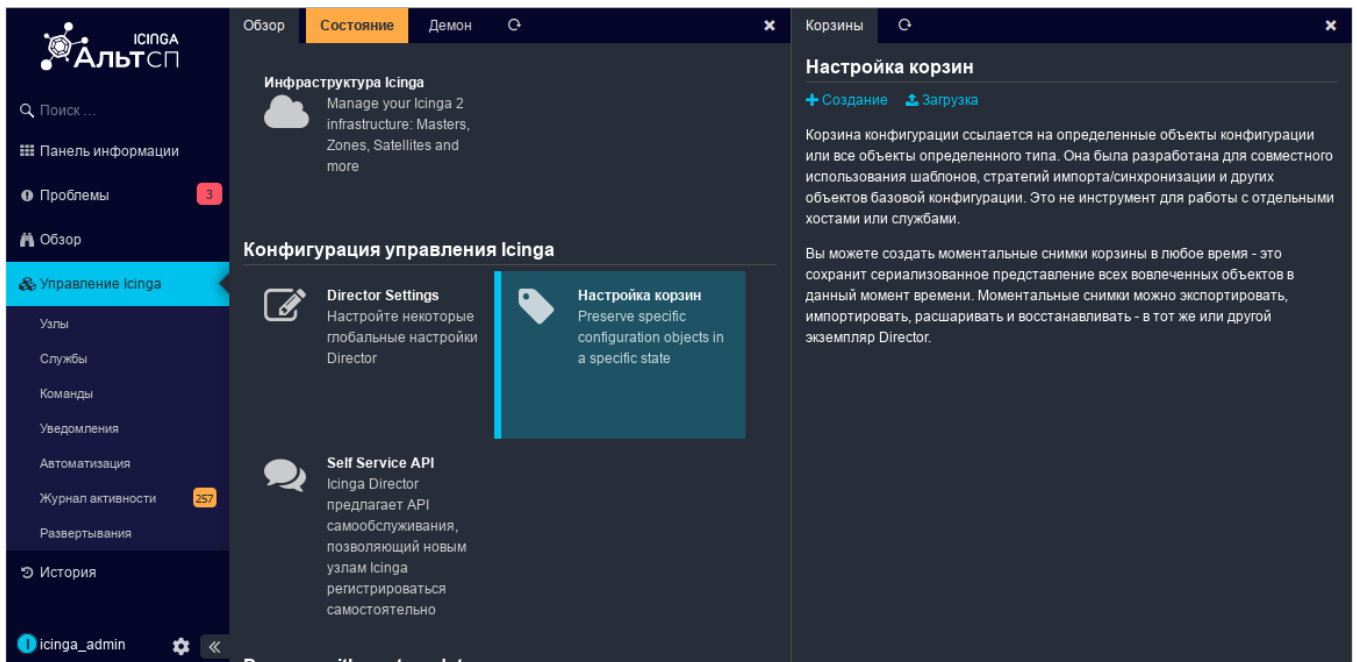


Рис. 130 – Настройка корзин

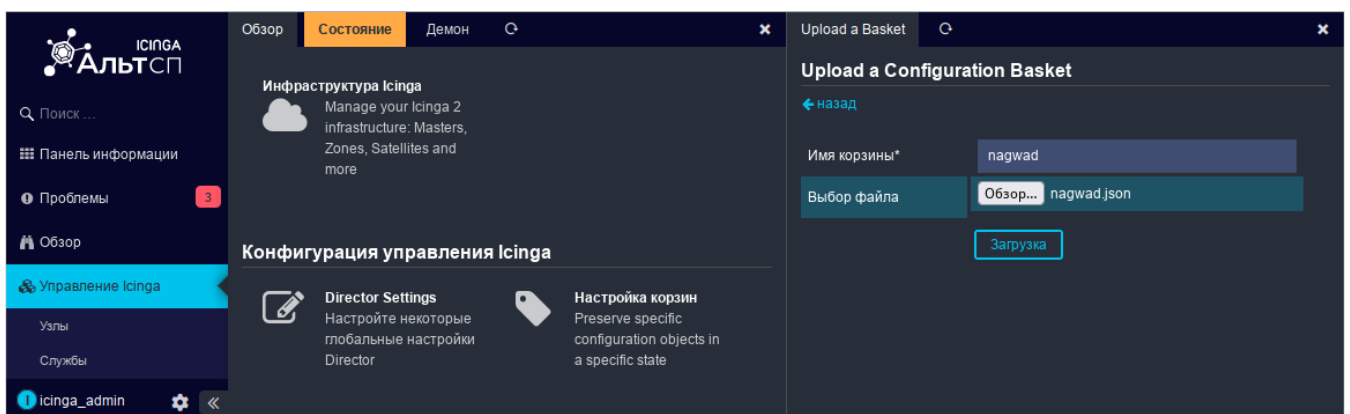


Рис. 131 – Загрузка корзины

Далее следует выбрать, должен ли каждый из элементов конфигурации отображаться в снимках этой корзины. Для каждого типа элемента доступны следующие варианты (рис. 132):

- «Все из них» – помещать все элементы этого типа в снимки (например, все шаблоны хостов);
- «Игнорировать» («Ignore») – не помещать этот элемент в снимки (например, не включать правила синхронизации);
- «Настраиваемый выбор» – помещать в снимок только указанные элементы этого типа. В этом случае нужно вручную отмечать каждый элемент. Например, если отмечены шаблоны хостов, то нужно перейти к каждому из нужных шаблонов хостов и выбрать действие «Добавить в корзину». Это приведет к тому, что эти конкретные шаблоны хостов будут включены в следующий снимок.

Оставить значения по умолчанию и нажать кнопку «Применить». Будет создана корзина (рис. 133).

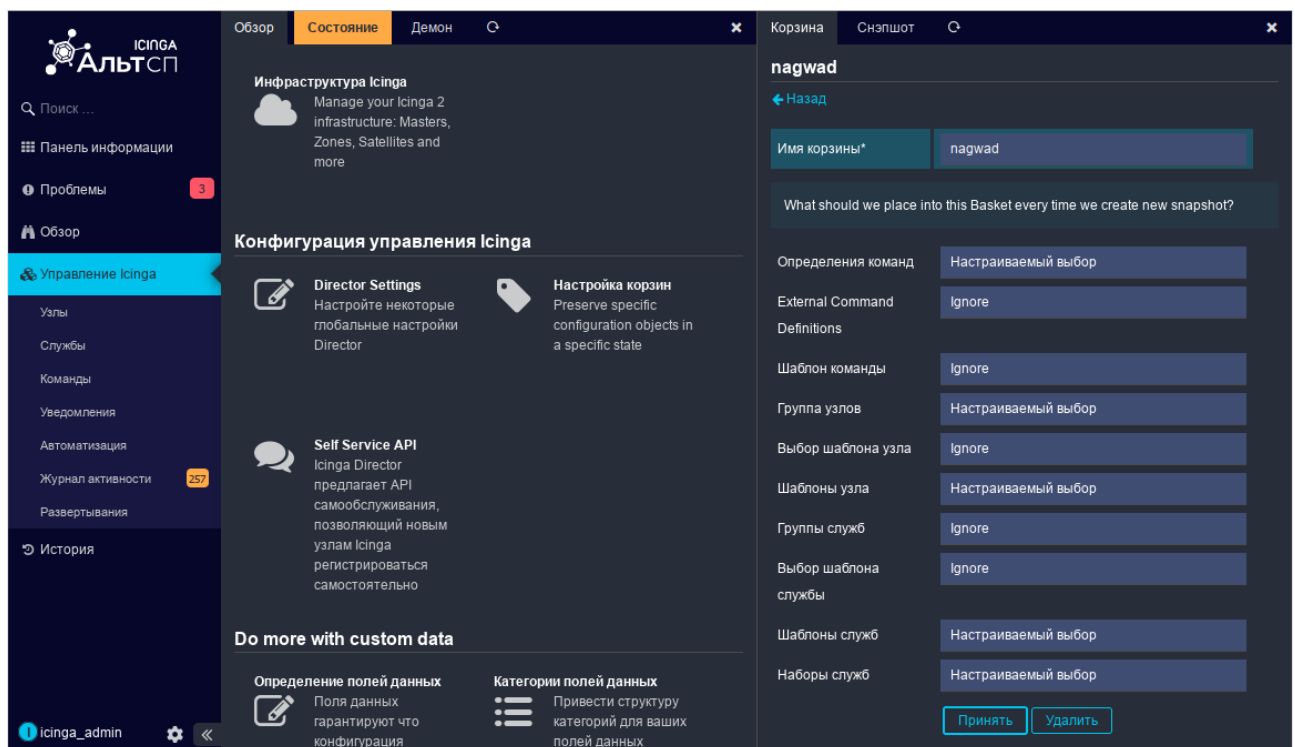


Рис. 132 – Выбор элементов конфигурации для корзины

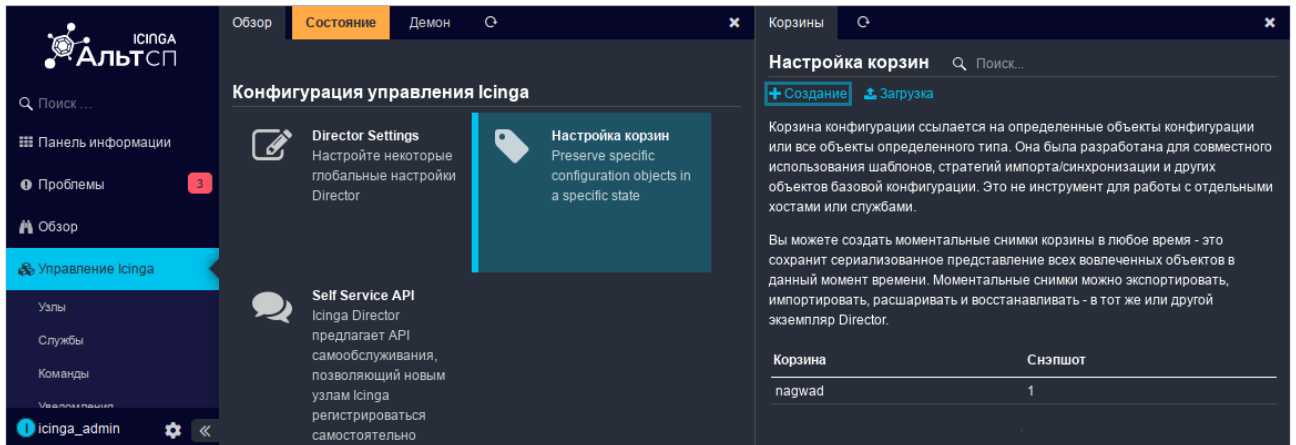


Рис. 133 – Корзина nagwad

Выбрать корзину из списка, перейти на вкладку «Снэпшот» (рис. 134) и выбрать снимок. В открывшейся справа форме нажать ссылку «Восстановление» (рис. 135), выбрать целевую базу данных и нажать кнопку «Восстановление». В результате будут созданы:

- команда (d_check_nagwad);
- шаблон группы (d-check-nodes);
- шаблон узла (d-nagwad-host);
- шаблоны служб (d-nagwad-service, d-nagwad-eperm, d-nagwad-login, d-nagwad-integralert, d-nagwad-print, d-nagwad-device, d-nagwad-authdata, d-nagwad-status);
- набор служб (d-nagwad-service-set).

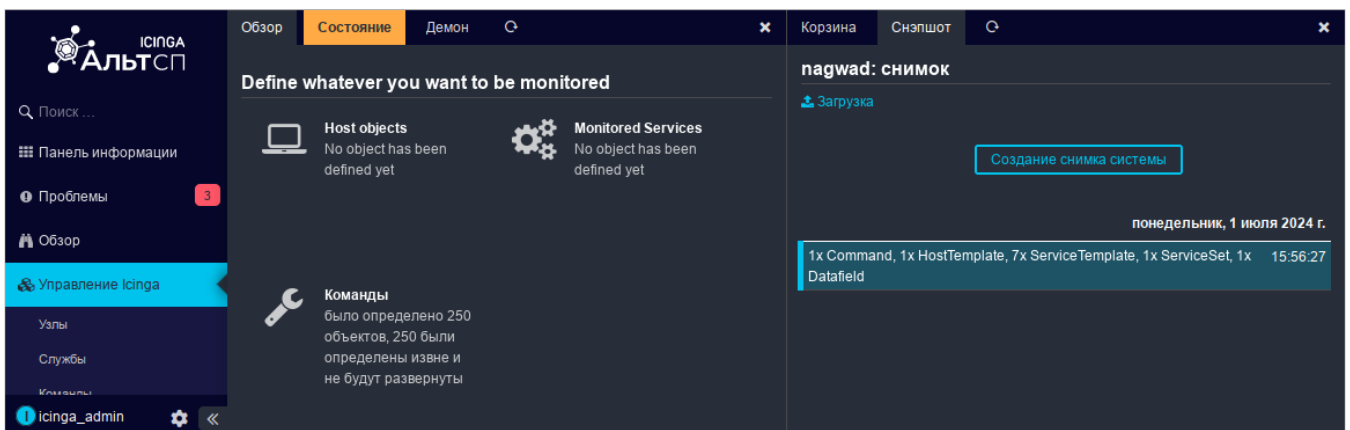


Рис. 134 – Вкладка «Снэпшот»

Далее необходимо убедиться, что шаблону узла добавлен набор служб. Для этого в разделе «Управление Icinga» → «Узлы» → «Шаблоны узла» выбрать шаблон d-nagwad-host, перейти на вкладку «Службы». Шаблону узла должны быть добавлены 7 служб из набора d-nagwad-service-set (рис. 136).

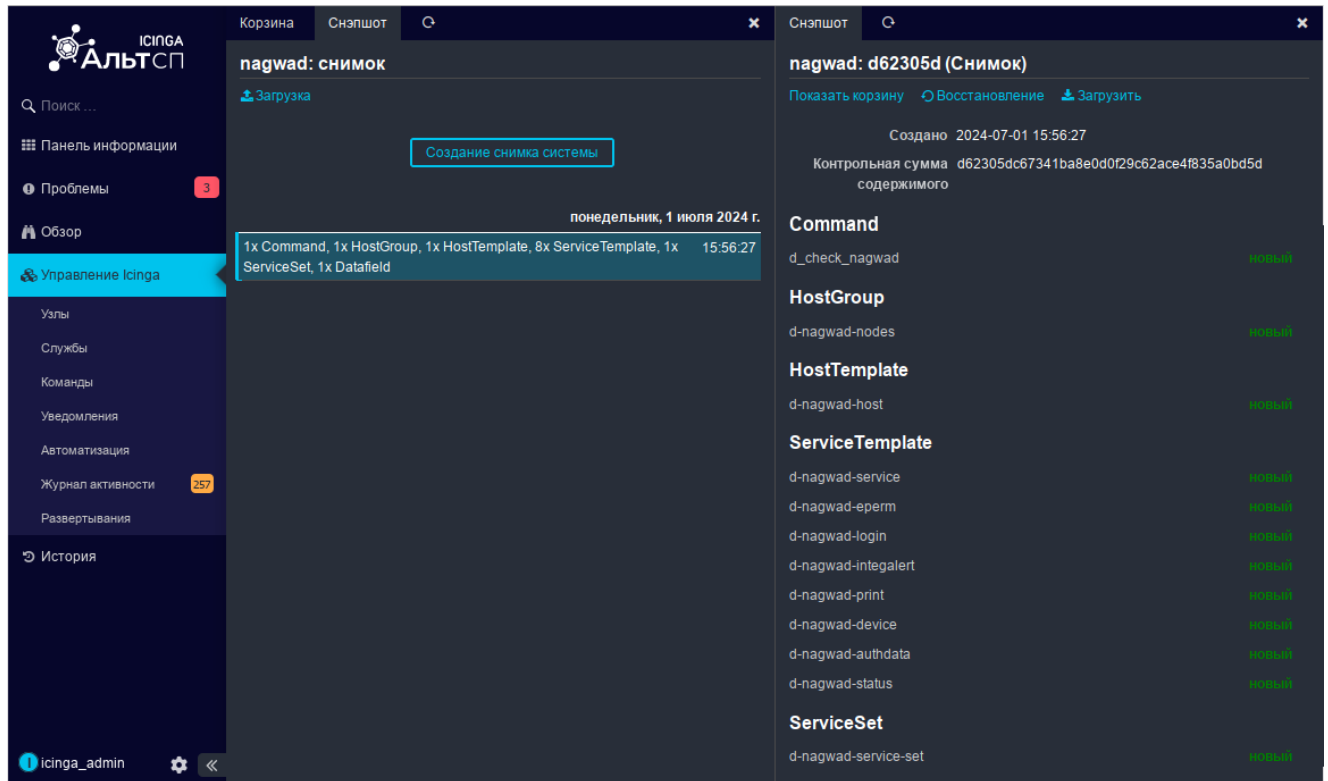


Рис. 135 – Просмотр снимка

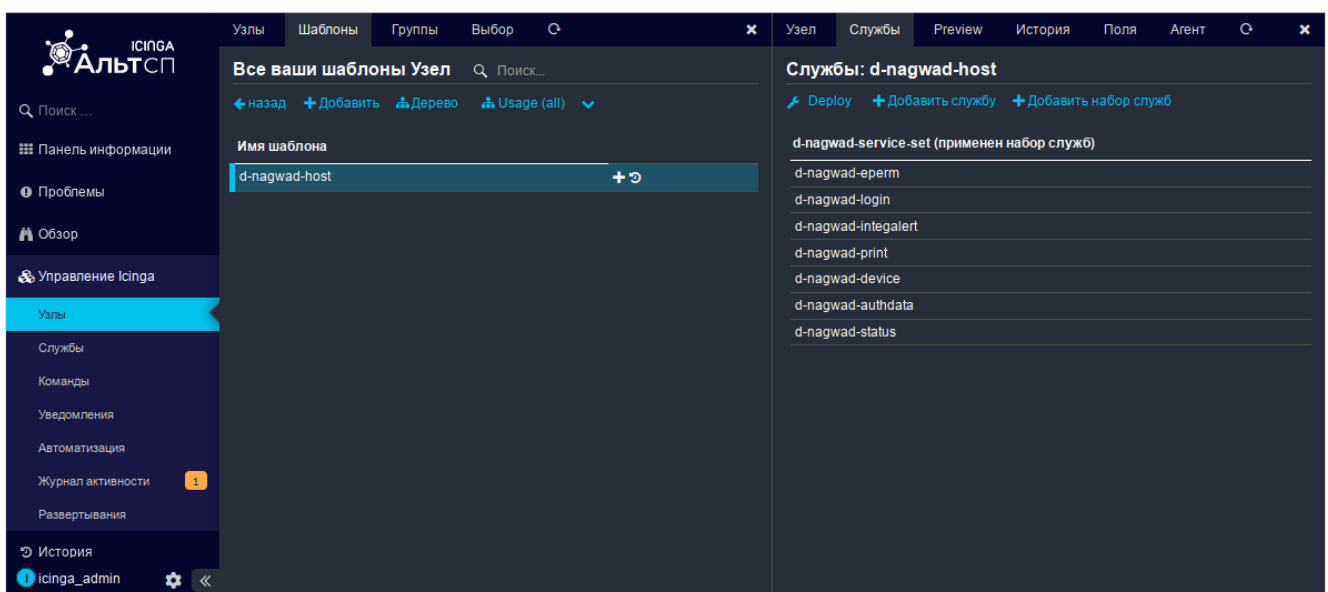


Рис. 136 – Службы, назначенные шаблону узла

7.7.3.2.5. Создание записи об агенте

Для создания записи об агенте с помощью Icinga Director перейти в раздел «Управление Icinga» → «Узлы» и на вкладке «Узлы» нажать ссылку «Добавить». В открывшейся справа форме добавления узла (рис. 137) заполнить следующие поля:

- «Host Template» – выбрать шаблон узла (можно выбрать несколько шаблонов, при этом если в разных шаблонах имеются одни и те же конфликтующие параметры, то к агенту будет применен тот параметр, который находится самым последним в этом списке шаблонов);
- «Имя узла» – FQDN-имя добавляемого узла;
- «Отображаемое имя» – имя имя агента, так как оно будет отображаться на веб-консоли;
- «Адрес узла» – IPv4-адрес добавляемого узла;
- «Группы» – группа, в которую будет добавлен узел.

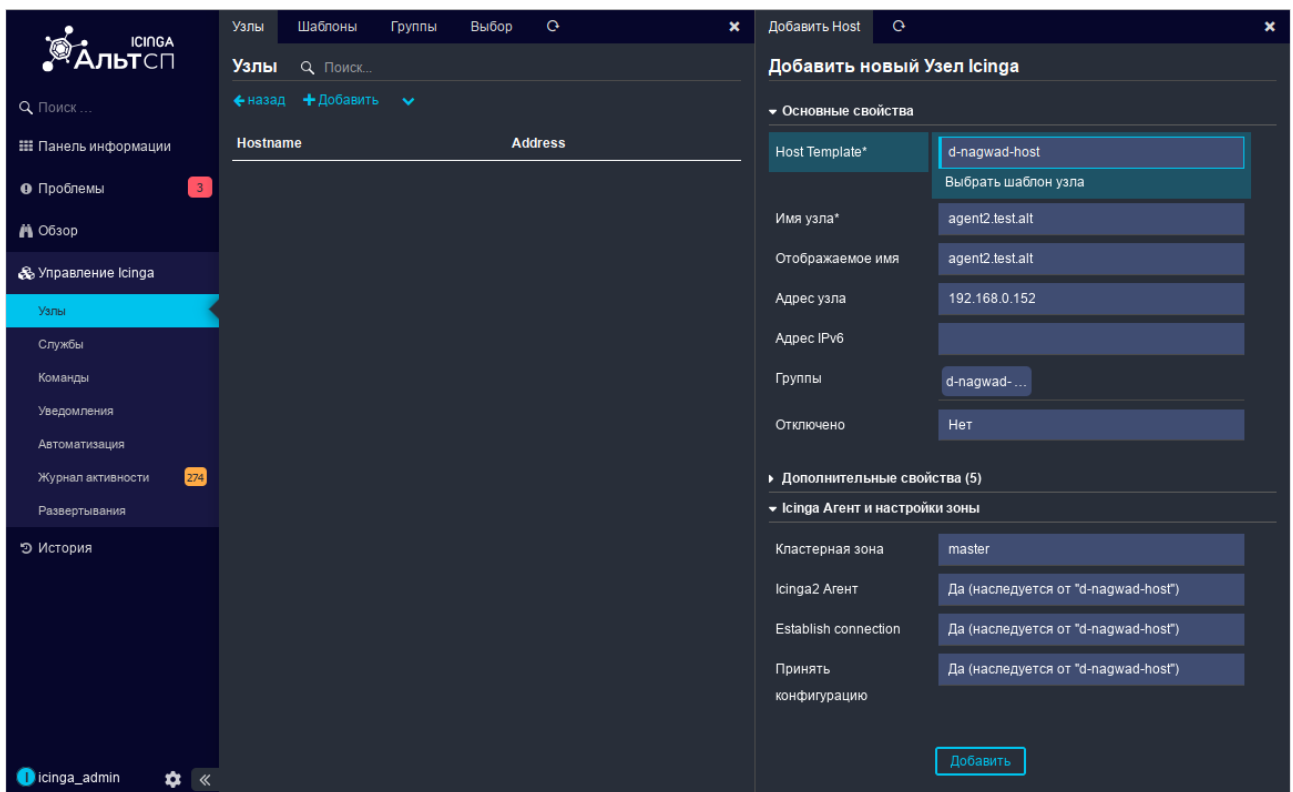


Рис. 137 – Добавление нового агента

После создания новой записи о агенте, как и после прочих операций по созданию и изменению объектов в Icinga Director, необходимо применить сделанные изменения в действующую конфигурацию Icinga, то есть выполнить развертывание (Deploy) обновленной конфигурации. Для этого необходимо нажать ссылку «Deploy» (рис. 138). После добавления новый агент перейдет сначала в состояние «Рассматриваемый» (PENDING), а после проверки его сетевой доступности, в состояние «Включен» (UP). Службы же этого агента будут иметь статус UNKNOWN с сообщением об отсутствии настроенного соединения клиента с сервером.

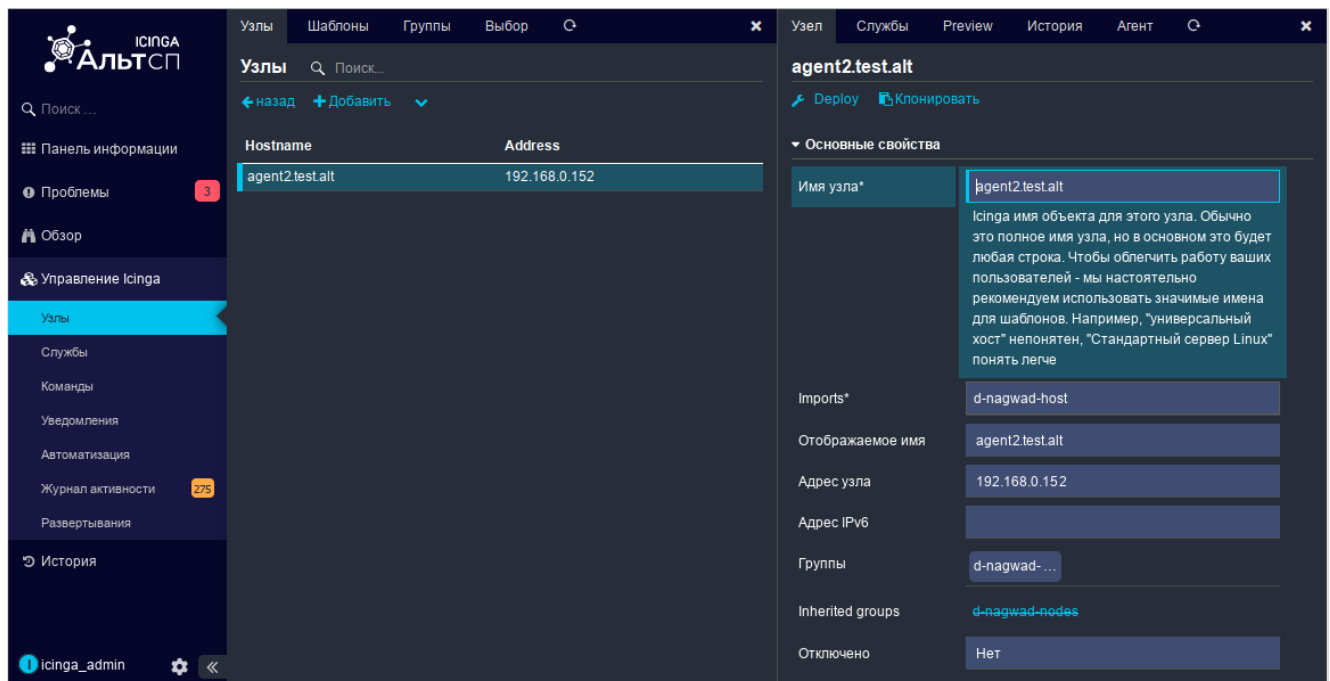


Рис. 138 – Созданный агент

Переключиться на вкладку «Агент» (рис. 139). Здесь можно найти билет (ticket) для настройки агента.

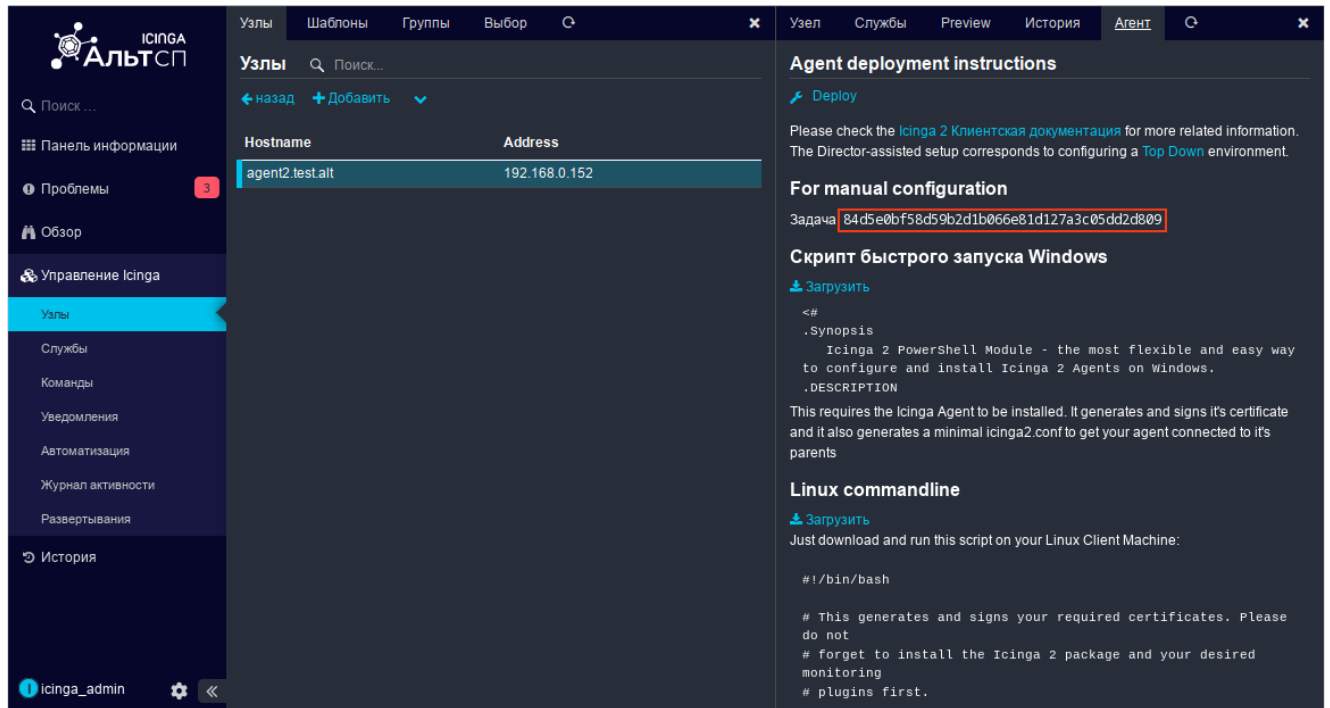


Рис. 139 – Вкладка «Агент»

7.7.3.2.6. Регистрация агента

Для регистрации агента может использоваться команда `icinga2-register-host`.

Синтаксис:

```
icinga2-register-host [options] [<Icinga Web 2 URL> <host-template-key>]
```

Возможные опции:

- `--name` – имя добавляемого узла (по умолчанию `hostname`);
- `--zone` – имя зоны (по умолчанию имя узла);
- `--address` – адрес добавляемого узла (по умолчанию `hostname`);
- `--remote` – адрес удаленной конечной точки в формате `CN[,HOST[,PORT]]` (по умолчанию адрес извлекается из указанного URL-адреса Icinga Web 2);
- `--parent-zone` – имя родительской зоны (по умолчанию `master`);
- `--trustedcert` – файл доверенного сертификата для проверки родительского узла (по умолчанию загрузка и проверка в интерактивном режиме);
- `--ticket` – билет Icinga2 для настройки узла (если этот параметр указан, то URL-адрес Icinga Web 2 не используется);

- `--web-ca` – файл CA для проверки URL-адреса Icinga Web 2;
- `--no-web-ca` – пропустить проверку URL-адреса Icinga Web 2.

Для настройки наблюдаемого узла с помощью билета следует запустить скрипт регистрации на агенте, выполнив команду:

```
# icinga2-register-host --name agent2.test.alt --remote
master1.test.alt --ticket 84d5e0bf58d59b2d1b066e81d127a3c05dd2d809
```

где `84d5e0bf58d59b2d1b066e81d127a3c05dd2d809` – билет для настройки агента.

7.7.3.2.7. Регистрация агента через API самообслуживания Icinga Director (Self Service API)

Icinga Director предлагает API самообслуживания, позволяющий новым хостам, на которых работает агент Icinga, безопасно регистрироваться.

7.7.3.2.7.1. Конфигурация Icinga Director

Для настройки API самообслуживания необходимо перейти в раздел «Управление Icinga» и выбрать ссылку «Self Service API». Справа появится форма настроек API самообслуживания (рис. 140).

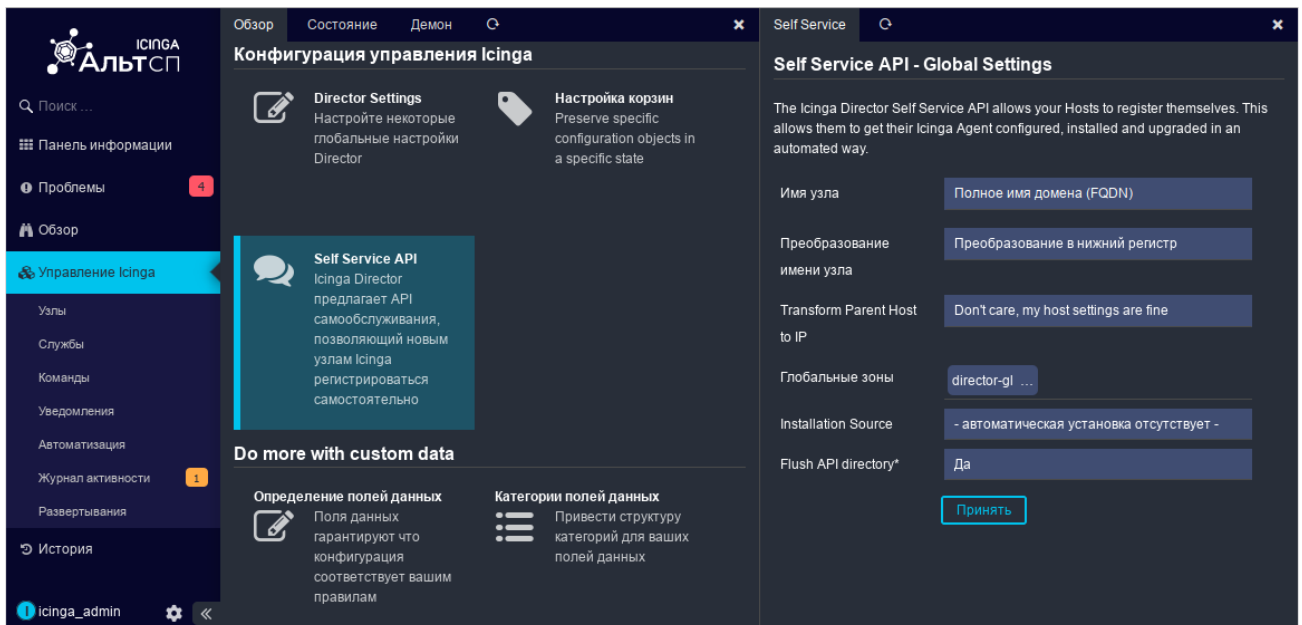


Рис. 140 – Настройка автоподключения

Для создания API ключа самообслуживания необходимо перейти в раздел «Управление Icinga» → «Узлы» → «Шаблоны узла», выбрать шаблон и в

открывшейся справа форме перейти на вкладку «Агент» и нажать кнопку «Создание API ключа самообслуживания» (рис. 141). В результате будет создан API ключ самообслуживания (рис. 142).

В шаблоне можно определить все виды пользовательских переменных, которые будут применяться автоматически.

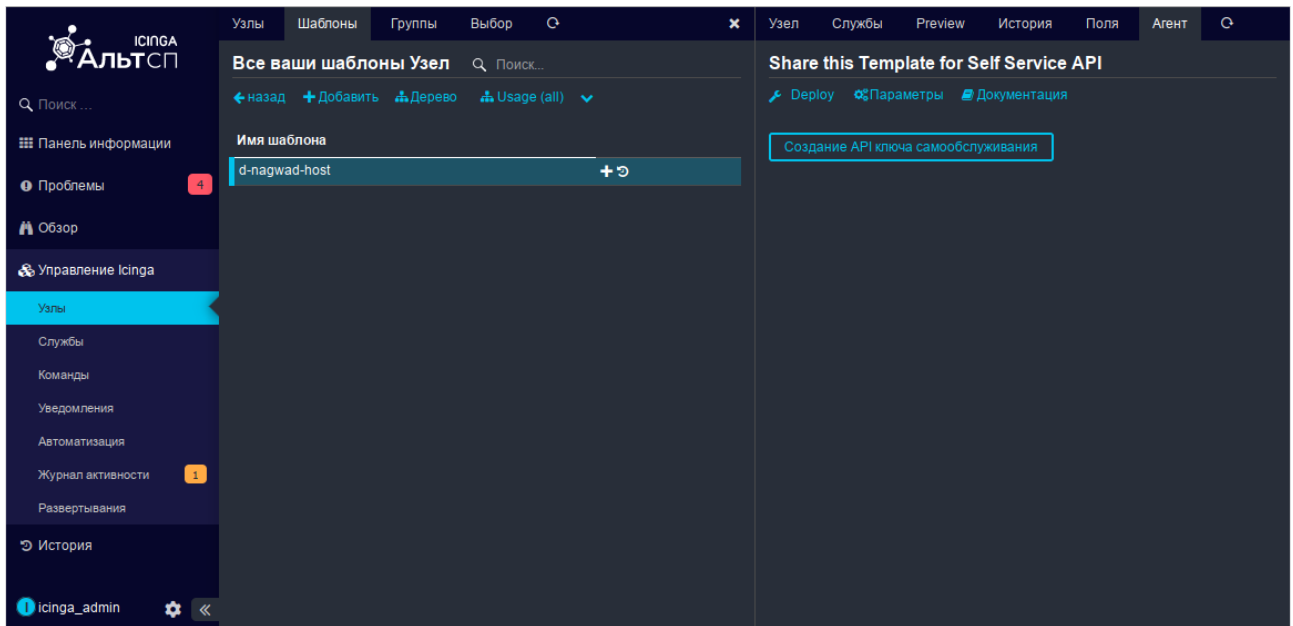


Рис. 141 – Создание API ключа самообслуживания

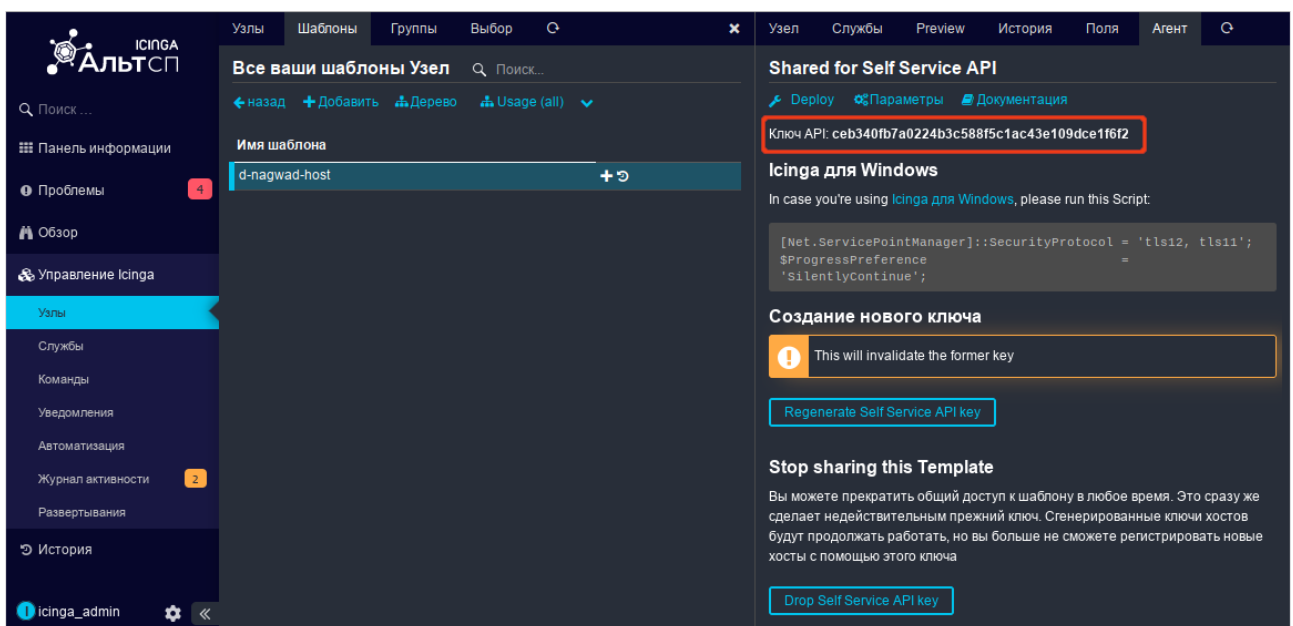


Рис. 142 – API ключ самообслуживания

7.7.3.2.7.2. Регистрация агента

Для регистрации агента может использоваться команда `icinga2-register-host`.

Для авторегистрации наблюдаемого узла следует запустить скрипт регистрации, на агенте, выполнив команду:

```
# icinga2-register-host --name agent3.test.alt \
http://192.168.0.170:81/icingaweb2 60ac7b9a9fc13a32196909ae4e93e438558a93f9
```

где `60ac7b9a9fc13a32196909ae4e93e438558a93f9` – API ключ самообслуживания.

В результате выполнения данного скрипта агент будет зарегистрирован через API самообслуживания Icinga Director.

7.7.3.2.8. Настройка службы синхронизации пользователей API

Для того, чтобы сценарий `10-push-icinga` (см. п. 7.7.3.2.9) мог нормально передавать данные с наблюдаемых узлов, необходимо обеспечить доступ с соответствующими правами к Icinga2 REST API. В целях обеспечения безопасности имеет смысл предоставлять такие права отдельно для каждого наблюдаемого узла, ограничивая сферу возможных действий данными, относящимися к этому узлу. Для этой цели можно использовать службу `icinga2-usersyncd`.

`icinga2-usersyncd` – служба синхронизации наблюдаемых узлов (объектов типа Host) с доступом по REST API (объектов типа ApiUser).

Настройка службы автоматической синхронизации (все команды выполняются на мастере):

- установить пакет:

```
# apt-get install icinga2-usersyncd
```

- сгенерировать клиентский сертификат для пользователя API `icinga2-usersyncd`:

```
# icinga2-usersyncd --setup
information/base: Writing private key to
'/var/lib/icinga2/certs/icinga2-usersyncd.key'.
information/base: Writing certificate signing request to
'/var/lib/icinga2/certs/icinga2-usersyncd.req'.
information/pki: Writing certificate to file
'/var/lib/icinga2/certs/icinga2-usersyncd.crt'
```

- перезапустить сервис icinga2:

```
# systemctl restart icinga2
```

- запустить и добавить в автозагрузку службу icinga2-usersyncd:

```
# systemctl enable --now icinga2-usersyncd
```

Примечание. Конфигурационный файл службы icinga2-usersyncd /etc/sysconfig/icinga2-usersyncd. По умолчанию предполагается доступ к мастер-ноде через `https://localhost:5665/`.

Синтаксис команды icinga2-usersyncd:

```
icinga2-usersyncd [-v] [-q] [-c CONFIG] [--no-config] [-L URL] [-u USERNAME] [-p PASSWORD] [-C CERT] [-K KEY] [-A CA_CERT] [-Q QUEUE] [-P PREFIX] [-T TEMPLATES] [-f FILTER] [-t DELAY]
```

```
icinga2-usersyncd --setup
```

Возможные опции:

- -v, --verbose – подробный вывод сообщений;
- -q, --quiet – подавлять вывод сообщений;
- -c CONFIG, --config CONFIG – указать файл конфигурации (по умолчанию /etc/sysconfig/icinga2-usersyncd);
- --no-config – не использовать конфигурационный файл;
- -L URL, --url URL – Icinga2 API URL;
- -u USERNAME, --username USERNAME – пользователь для аутентификации в Icinga2 API;
- -p PASSWORD, --password PASSWORD – пароль пользователя для аутентификации в Icinga2 API;
- -C CERT, --cert CERT – сертификат для аутентификации в API Icinga2;
- -K KEY, --key KEY – ключ для аутентификации в API Icinga2;
- -A CA_CERT, --ca CA_CERT – сертификат API Icinga2 (CA);
- -Q QUEUE, --queue QUEUE – имя используемой очереди событий (по умолчанию либо из конфигурации, либо icinga2-usersyncd, если опущено);
- -P PREFIX, --prefix PREFIX – префикс для имен ApiUser (по умолчанию – либо из конфигурации, либо «host-», если он опущен);

- -T TEMPLATES, --templates TEMPLATES – набор шаблонов, которые должен импортировать каждый созданный ApiUser (по умолчанию – либо из конфигурации, либо [usersync], если опущено);
- -f FILTER, --filter FILTER – фильтр узла;
- -t DELAY, --delay DELAY – количество секунд ожидания между попытками подключения (по умолчанию – либо из конфигурации, либо 1, если опущено);
- --setup – сгенерировать сертификат для CN icinga2-usersyncd (сертификат будет создан в каталоге /var/lib/icinga2/certs/).

7.7.3.2.9. Настройка работы «пассивных» проверок

Скрипт пост-обработки событий 10-push-icinga (пакет nagwad-icinga-push) предназначен для отправки зарегистрированных событий на сервер Icinga2 через REST API не дожидаясь опроса со стороны мастер-узла. Одним из преимуществ использования этого скрипта является то, что он может снимать флаг подтверждения для события каждый раз, когда регистрируется новое событие того же типа.

Для возможности работы «пассивных» проверок на агенте необходимо установить пакет:

```
# apt-get install nagwad-icinga-push
```

Скрипт 10-push-icinga считывает свою конфигурацию из файла /etc/nagwad/process-event.d/push-icinga.conf и не требует настроек при условии, что узел правильно настроен как агент/спутник Icinga2 (если для регистрации агента использовалась команда icinga2-register-host). Скрипт использует SSL-сертификаты из каталога /var/lib/icinga2/certs).

Однако для использования Icinga2 REST API на сервере должен быть настроен ApiUser с соответствующим набором прав. Для этой цели удобно использовать демон icinga2-usersyncd (см. п. 7.7.3.2.8).

7.7.4. Работа с Icinga

7.7.4.1. Проверка сигнальных файлов

Проверка сигнальных файлов Nagwad производится средствами Icinga и Nagios с помощью сценария `check_nagwad`, которому в качестве аргумента требуется передать имя фильтра:

```
/usr/lib/nagios/plugins/check_nagwad <имя_фильтра>
```

Если сигнальный файл отсутствует, сценарий завершается с кодом 0 и выводит строку `OK: Nothing detected for <имя_фильтра>` (рис. 143). Если же сигнальный файл присутствует, выводится содержащаяся в нем информация (за исключением имени фильтра) (рис. 144), а код завершения сценария соответствует уровню критичности события.

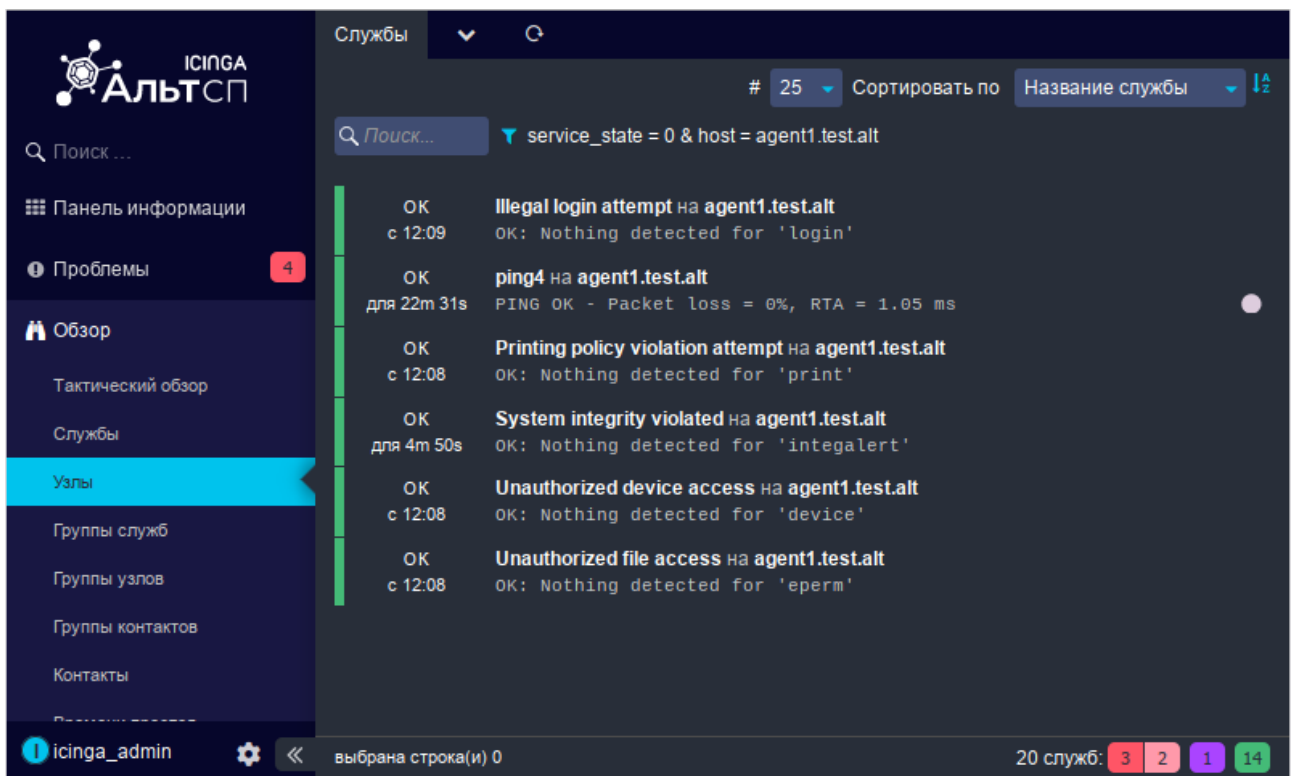


Рис. 143 – Сценарии, завершившиеся с кодом 0



Рис. 144 – Информация из сигнального файла

При наличии нескольких сигнальных файлов, связанных с событием одного и того же типа, сперва обрабатываются сигнальные файлы уровня CRITICAL.

7.7.4.2. Пометка проблем (событий) как разрешенных

После того как событие зафиксировано и обработано, администратор безопасности может пометить сигнальный файл на управляемой машине как решенный. Для этого можно переименовать файл (в каталоге `/var/log/nagwad/<boot_id>/<имя_фильтра>`), изменив суффикс файла на `FIXED` или использовать команду `nagwad fix`.

Пример использования команды `nagwad fix` для пометки проблемы, как разрешенной:

- просмотреть список зарегистрированных событий:

```
# nagwad
2024-07-01+16:35:10.5837078000 integralert.e30128170ee5b3871821adaf5ad75.CRITICAL
2024-07-01+16:35:10.5837078000 integralert.62476f6497eaf88fe1f46d1f5382e.CRITICAL
```

- просмотреть конкретное событие:

```
# nagwad show integralert.e30128170ee5b3871821adaf5ad75.CRITICAL
CRITICAL:          integralert:CRITICAL:2024-07-01T16:35:10+0200          agent3.test.alt
integralert[2371]: System integrity check (chg=3,add=55,del=0)
```

- пометить событие как исправленное:

```
# nagwad fix integralert.e30128170ee5b3871821adaf5ad75.CRITICAL
```

7.8. ГОСТ в OpenSSL

7.8.1. Поддержка шифрования по ГОСТ в OpenSSL

Для включения поддержки шифрования ГОСТ в OpenSSL нужно выполнить следующие действия:

1) установить пакет:

```
# apt-get install openssl-gost-engine
```

2) изменить конфигурационный файл OpenSSL, выполнив команду:

```
# control openssl-gost enabled
```

3) проверить, доступны ли шифры ГОСТ для OpenSSL:

```
$ openssl ciphers|tr ':' '\n'|grep GOST
GOST2012-GOST8912-GOST8912
GOST2001-GOST89-GOST89
```

7.8.2. Создание ключей

Пример генерации закрытого ключа с алгоритмом ГОСТ-2012:

```
$ openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:TCA \
-out ca.key
```

Пример создания сертификата на 365 дней (ca.cer):

```
$ openssl req -new -x509 -md_gost12_256 -days 365 -key ca.key -out ca.cer \
-subj "/C=RU/ST=Russia/L=Moscow/O=SuperPlat/OU=SuperPlat CA/CN=SuperPlat CA Root"
```

Проверка сертификата (ca.cer):

```
$ openssl x509 -in ca.cer -text --noout
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

0c:dc:50:10:4b:de:a8:0f:ed:3f:0c:81:5c:7d:d3:15:55:87:52:69

Signature Algorithm: GOST R 34.10-2012 with GOST R 34.11-2012 (256 bit)

Issuer: C = RU, ST = Russia, L = Moscow, O = SuperPlat, OU = SuperPlat

CA, CN = SuperPlat CA Root

Validity

Not Before: Nov 22 10:24:23 2024 GMT

Not After : Nov 22 10:24:23 2025 GMT

Subject: C = RU, ST = Russia, L = Moscow, O = SuperPlat, OU = SuperPlat

CA, CN = SuperPlat CA Root

Subject Public Key Info:

Public Key Algorithm: GOST R 34.10-2012 with 256 bit modulus

Public key:

```
X:AC949E79BCDC65E4808635A069DB5078F555EBD5E8C25B72426B701FDF6E68D5
```

```
Y:AF06E27ABC4D92CAD091F857CEB54A85738A5193ABE50E25025F9D129272683A
```

Parameter set: GOST R 34.10-2012 (256 bit) ParamSet A

X509v3 extensions:

X509v3 Subject Key Identifier:

ЛКНВ.11100-01 90 03

61:EC:DB:51:A6:A0:5F:79:C3:4C:A1:0B:E9:7B:7B:47:D5:AD:E6:DF
X509v3 Authority Key Identifier:

keyid:61:EC:DB:51:A6:A0:5F:79:C3:4C:A1:0B:E9:7B:7B:47:D5:AD:E6:DF

X509v3 Basic Constraints:

CA:TRUE

Signature Algorithm: GOST R 34.10-2012 with GOST R 34.11-2012 (256 bit)

1c:12:59:e5:c0:2d:db:ec:c2:db:6a:4b:38:d9:e7:4c:09:9e:

d0:9b:78:33:6b:1f:ba:39:db:55:4a:0b:9e:1a:11:9c:cd:00:

b2:59:50:88:bc:61:a0:27:94:c7:e9:35:24:de:42:dc:08:d3:

fd:32:27:35:d3:7c:1a:4b:3c:19

7.9. Утилита уничтожения информации при удалении – dm-secdel

Операции удаления обычно ограничиваются пометкой блоков данных как «неиспользуемых» в файловой системе. Утилита `dm-secdel`, так же помечает блоки как не используемые, но заменяет очищение, записью случайных данных в освобождаемые блоки. Таким образом, данные удаляются надежно.

В силу своего абстрактного характера `dm-secdel` поддерживает множество файловых систем, которые поддерживают опцию `discard` (например, `ext3`, `ext4`, `xf`s, `btrfs`).

⚠ Следует создать сопоставленное устройство с помощью инструмента `secdelsetup`. Убедиться, что файловая система (ФС) смонтирована на это, а не основное устройство. Убедиться, что ФС установлена с опцией `-o discard`.

Проверить, смонтирована ли ФС в данный момент с этой опцией, можно посмотрев вывод команды `mount`:

```
/dev/sdd1 on / type ext4 (rw,discard,errors=remount-ro)
```

Не следует включать ведение журнала данных. Обратите внимание, что при удалении файлов командой `rm` удаление будет выполняться асинхронно, поэтому чтобы убедиться, что данные уже удалены следует использовать команду `sync` или опцию монтирования файловой системы `-o sync` до использования команды `rm`.

Если нужно, чтобы имена файлов также были уничтожены, во-первых, следует убедиться, что файловая система создана полностью без ведения журнала (например, `mkfs.ext4 -O ^has_journal`), а во-вторых, удалите сам каталог, тогда его блоки освободятся и будут стерты.

При использовании команды `fstrim` все свободные блоки файловой системы будут отброшены (`discarded`) и, следовательно, также стерты (файловая система должна быть примонтирована с опцией `-o discard`).

Применение:

```
secdelsetup <источник-устройство> [маппинг]
```

Опции:

- 1) `-d|--detach <устройство>` – отсоединить устройство;
- 2) `-D|--detach-all|--stop` – отключить все устройства;
- 3) `-l|--list` – список активных карт устройства;
- 4) `-a|--all` – список в другом формате;
- 5) `--lsblk` – вывод в формате `lsblk`;
- 6) `--start` – запускать устройства из `secdeltab`;
- 7) `--save` – сохранение активных устройств в `secdeltab`.

Пример: пусть `/home` находится на устройстве `/dev/sda5`, закомментировать строку с разделом `/home` в файле `/etc/fstab` и выполнить перезагрузку системы.

Проверить наличие журналирования на устройстве, выполнить команду:

```
dumpe2fs /dev/sda5 | grep has_journal
```

Если параметры журналирования найдены, отключить их с помощью команды:

```
tune2fs -O ^has_journal /dev/sda5
```

Создадим для `/dev/sda5` сопоставленное устройство (карта) (по умолчанию задается один проход со случайными битами):

```
# secdelsetup /dev/sda5
```

Пример ожидаемого вывода команды:

```
/dev/mapper/secdel0 is attached to /dev/sda5
```

где `/dev/mapper/secdel0` имя созданного сопоставленного устройства.

В файл `/etc/fstab` добавить новую строку, указывающую на точку монтирования `/home`:

```
/dev/mapper/secdel0 /home ext4 noexec,nosuid,relatime,discard 1 2
```

Затем `/dev/mapper/secdel0` должно быть смонтировано с параметром `-o discard`, выполнить команду:

```
# mount /dev/mapper/secdel0 /mnt/test/ -o discard
```

Команда просмотра текущих (существующих) карт:

```
# secdelsetup -all  
/dev/mapper/secdel0 /dev/sda5
```

Для хранения конфигурации карт используется файл `/etc/secdeltab`, который будет автоматически активирован после перезагрузки (системной службой `secdeltab.service`). Для сохранения текущих карт в файл выполнить команду:

```
# secdelsetup --save
```

Для изменения перезаписи, например, с тремя проходами (первый проход – 1, второй проход случайные биты – R, третий проход – 0) выполнить команду:

```
# secdelsetup /dev/sda5 /dev/mapper/secdel0 1R0
```

Команда отсоединения всех активных карт:

```
# secdelsetup --detach-all
```

Пример ожидаемого вывода команды:

```
detach /dev/mapper/secdel0
```

8. СРЕДСТВА УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ, ОРГАНИЗАЦИЯ СЕТЕВОЙ ИНФРАСТРУКТУРЫ С ПОМОЩЬЮ СЕРВЕРА

Дальнейшие разделы описывают некоторые возможности использования ОС, настраиваемые в ЦУС.

⚠ Последующие пункты рекомендуются к прочтению опытным пользователям и системным администраторам.

8.1. Вход в систему

Для начала работы по настройке системы сразу после ее установки нужно использовать веб-ориентированный интерфейс ЦУС (см. п. 7.1.2), позволяющий управлять выбранным компьютером с любого другого в сети.

8.2. Настройка подключения к Интернету

Помимо множества различных служб, которые ОС Альт СП может предоставлять компьютерам сети, важно определить, будет ли сервер предоставлять общий доступ в Интернет для компьютеров домена или нет. В зависимости от этого сервер можно рассматривать как:

- сервер без подключения к сети Интернет – это сервер с одним сетевым интерфейсом (одной сетевой картой), который и связывает его с компьютерами локальной сети. Такой сервер называется также сервер рабочей группы;
- шлюз – в этом случае сервер обычно имеет два сетевых интерфейса (например, две сетевые карты), одна из которых служит для подключения к локальной сети, а другая – для подключения к сети Интернет.

Как для обеспечения доступа в сеть Интернет самого сервера, так и для настройки общего выхода в Интернет для компьютеров сети нужно настроить подключение к Интернету на самом сервере.

Для настройки подключения к сети Интернет можно воспользоваться одним из разделов ЦУС «Сеть»:

- Ethernet-интерфейсы (см. п. 8.2.1);

- PPTP-соединения;
- PPPoE-соединения;
- OpenVPN-соединения (см. п. 8.4).

8.2.1. Конфигурирование сетевых интерфейсов

Конфигурирование сетевых интерфейсов осуществляется в модуле ЦУС «Ethernet-интерфейсы» (пакет alterator-net-eth) из раздела «Сеть» (рис. 145).

Имя компьютера: server

Интерфейсы

enp0s3

Сетевая карта: Intel Corporation 82540EM Gigabit Ethernet Controller
провод подсоединён
MAC: 08:00:27:f1:99:3a

Версия протокола IP: IPv4 Включить

Конфигурация: Вручную

IP-адреса: 192.168.0.191/24

Добавить ↑ IP: /24 (255.255.255.0)

Шлюз по умолчанию: 192.168.0.1

DNS-серверы: 192.168.0.2

Домены поиска:
(несколько значений записываются через пробел)

Рис. 145 – Настройка модуля «Ethernet-интерфейсы»

В модуле «Ethernet-интерфейсы» можно заполнить следующие поля:

- «Имя компьютера» – указать сетевое имя ПЭВМ в поле для ввода имени компьютера (это общий сетевой параметр, не привязанный к какому-либо конкретному интерфейсу);
- «Интерфейсы» – выбрать доступный сетевой интерфейс, для которого будут выполняться настройки;

- «Версия протокола IP» – указать в выпадающем списке версию используемого протокола IP (IPv4, IPv6) и убедиться, что пункт «Включить», обеспечивающий поддержку работы протокола, отмечен;
- «Конфигурация» – выбрать способ назначения IP-адресов (службы DHCP, Zeroconf, вручную);
- «IP-адреса» – пул назначенных IP-адресов из поля «Добавить ↑ IP», выбранные адреса можно удалить нажатием кнопки «Удалить»;
- «Добавить ↑ IP» – ввести IP-адрес вручную и выбрать в выпадающем поле предпочтительную маску сети. Для переноса адреса в пул поля «IP-адреса» необходимо нажать кнопку «Добавить»;
- «Шлюз по умолчанию» – в поле для ввода нужно ввести адрес шлюза, который будет использоваться сетью по умолчанию;
- «DNS-серверы» – в поле для ввода нужно ввести список предпочтительных DNS-серверов, которые будут получать информацию о доменах, выполнять маршрутизацию почты и управлять обслуживающими узлами для протоколов в домене;
- «Домены поиска» – в поле для ввода нужно ввести список предпочтительных доменов, по которым будет выполняться поиск. Если в поле «Домены поиска» перечислить наиболее часто используемые домены (например, domain), то можно пользоваться неполными именами машин (computer вместо computer.domain).

«IP-адрес» и «Маска сети» – обязательные параметры каждого узла IP-сети. Первый параметр – уникальный идентификатор машины, от второго напрямую зависит, к каким машинам локальной сети данная машина будет иметь доступ. Если требуется выход во внешнюю сеть, то нужно указать параметр «Шлюз по умолчанию».

В случае наличия DHCP-сервера можно все вышперечисленные параметры получить автоматически – выбрав в списке «Конфигурация» пункт «Использовать DHCP».

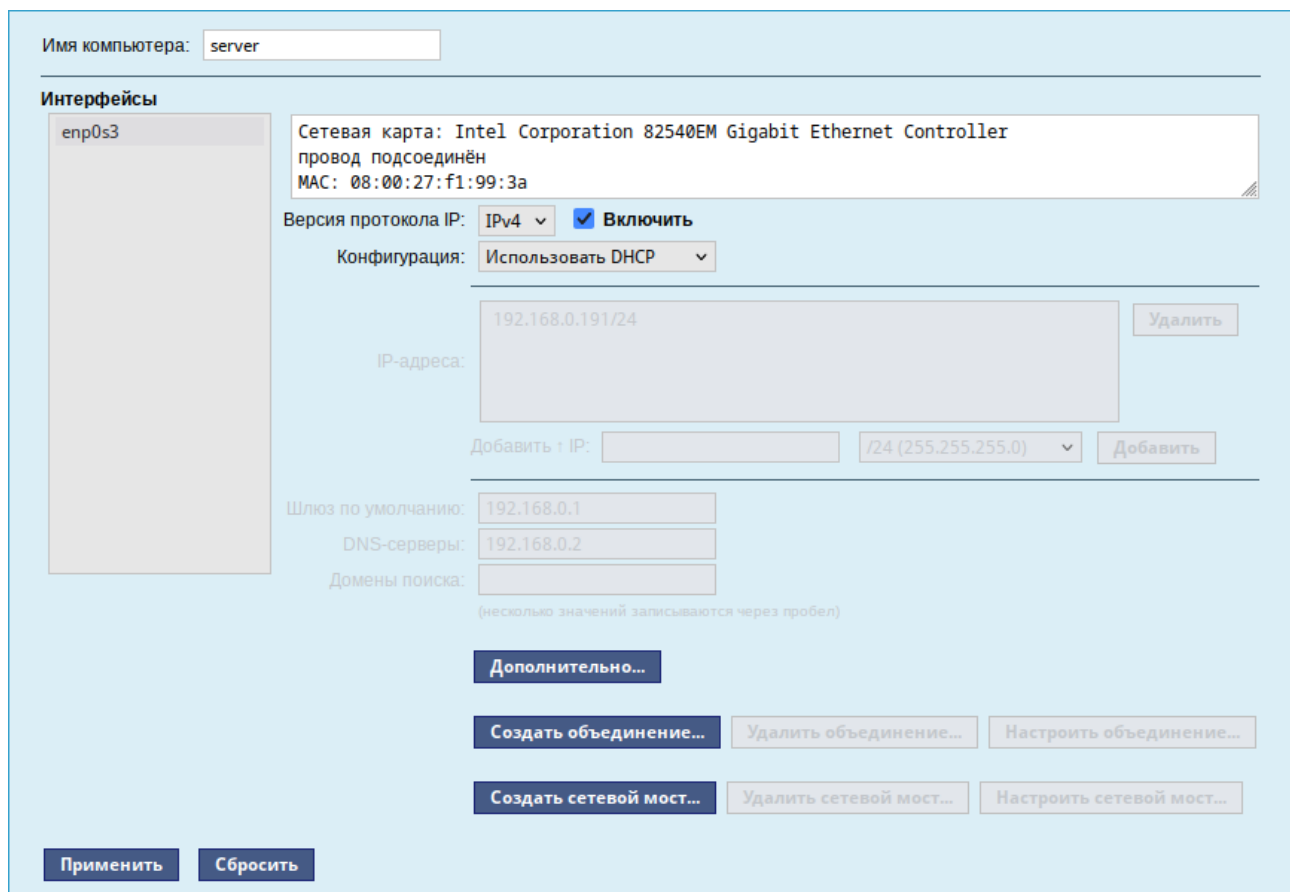


Рис. 146 – Автоматическое получение настроек от DHCP-сервера

Дополнительно для каждого интерфейса можно настроить сетевую подсистему (NetworkManager, Etcnet), а также должен ли запускаться данный интерфейс при загрузке системы (рис. 147).

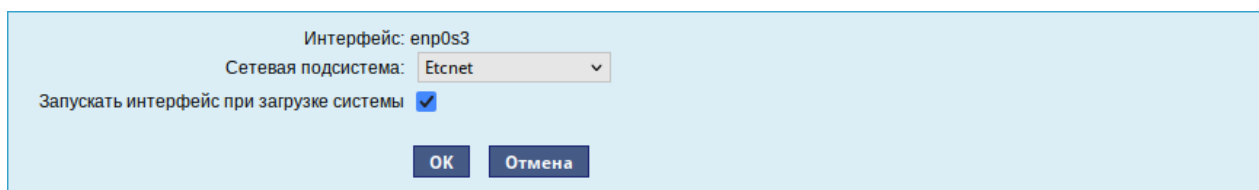


Рис. 147 – Выбор сетевой подсистемы

В списке «Сетевая подсистема» можно выбрать следующие режимы:

- «Etcnet» – в этом режиме настройки берутся исключительно из файлов, находящихся в каталоге настраиваемого интерфейса `/etc/net/ifaces/<интерфейс>`. Настройки сети могут изменяться либо в ЦУС в данном модуле, либо напрямую через редактирование файлов `/etc/net/ifaces/<интерфейс>`;

- «NetworkManager (etcnet)» – в этом режиме NetworkManager сам иницирует сеть, используя в качестве параметров – настройки из файлов Etcnet. Настройки сети могут изменяться либо в ЦУС в данном модуле, либо напрямую через редактирование файлов `/etc/net/ifaces/<интерфейс>`. В этом режиме можно посмотреть настройки сети, например полученный по DHCP IP-адрес, через графический интерфейс NetworkManager;
- «NetworkManager (native)» – в данном режиме управление настройками интерфейса передается NetworkManager и не зависит от файлов Etcnet. Управлять настройками можно через графический интерфейс NetworkManager. Файлы с настройками находятся в директории `/etc/NetworkManager/system-connections`. Этот режим особенно актуален для задач настройки сети на клиенте, когда IP-адрес нужно получать динамически с помощью DHCP, а DNS-сервер указать явно. Через ЦУС так настроить невозможно, так как при включении DHCP отключаются настройки, которые можно задавать вручную;
- «Не контролируется» – в этом режиме интерфейс находится в состоянии DOWN (выключен).

8.2.2. Объединение сетевых интерфейсов

Модуль «Объединение интерфейсов» (пакет `alterator-net-bond`) позволяет объединить несколько физических сетевых интерфейсов в один логический. Это позволяет достичь отказоустойчивости, увеличения скорости и балансировки нагрузки.

Для создания объединения интерфейсов необходимо выполнить следующие действия:

- 1) нажать на кнопку «Создать объединение...» (рис. 148);

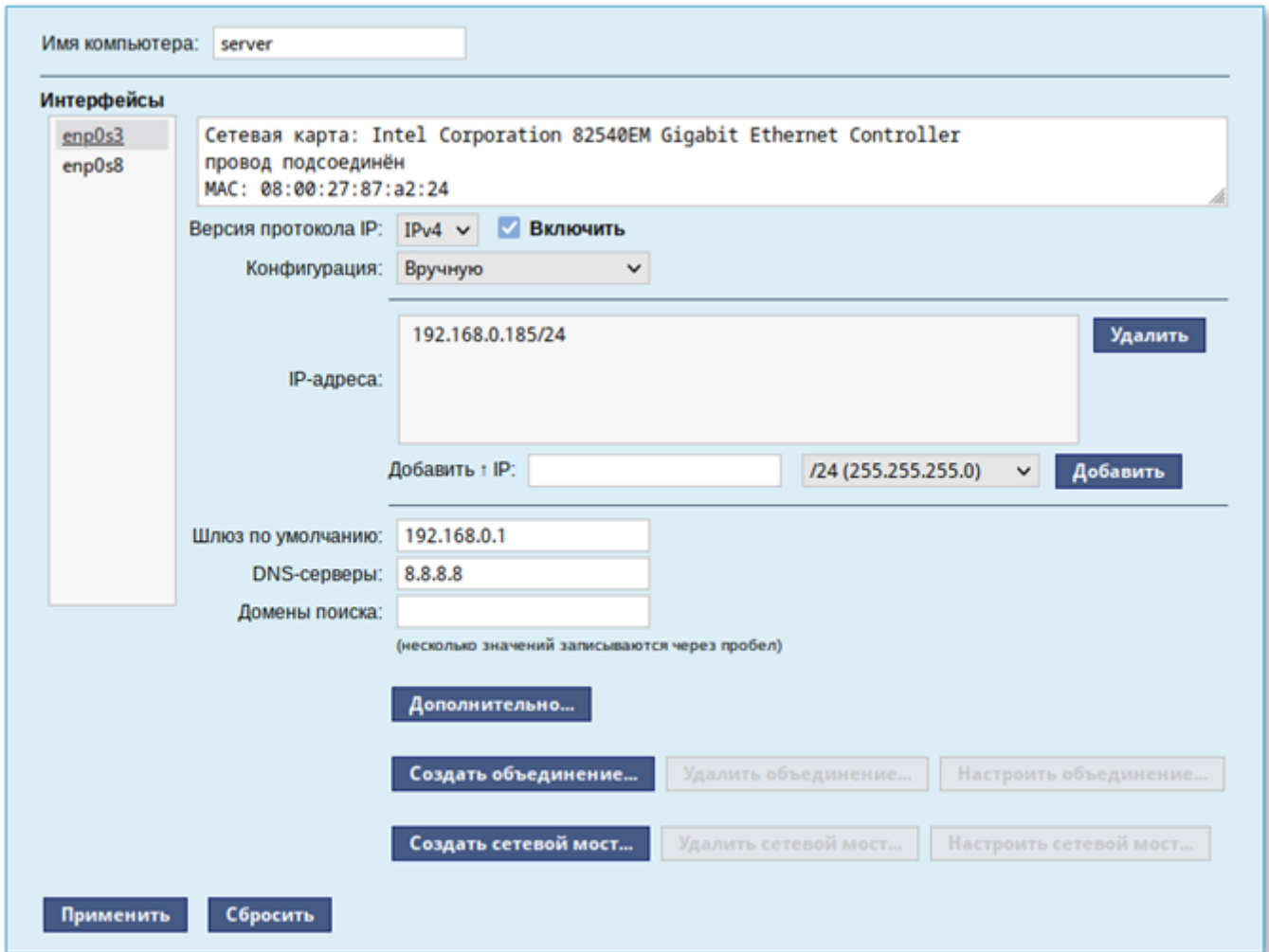


Рис. 148

- 2) переместить сетевые интерфейсы, которые будут входить в объединение, из списка «Доступные интерфейсы» в список «Используемые интерфейсы» (рис. 149);
- 3) выбрать режим объединения:
 - «Round-robin» – режим циклического выбора активного интерфейса для исходящего трафика;
 - «Активный-резервный» – активен только один интерфейс, остальные находятся в режиме горячей замены;
 - «XOR» – один и тот же интерфейс работает с определенным получателем, передача пакетов распределяется между интерфейсами на основе формулы $((\text{MAC-адрес источника}) \text{ XOR } (\text{MAC-адрес получателя})) \% \text{ число интерфейсов}$;

- «Широковещательная» – трафик идет через все интерфейсы одновременно;
 - «Агрегирование каналов по стандарту IEEE 802.3ad» – в группу объединяются одинаковые по скорости и режиму интерфейсы, все физические интерфейсы используются одновременно в соответствии со спецификацией IEEE 802.3ad. Для реализации этого режима необходима поддержка на уровне драйверов сетевых карт и коммутатор, поддерживающий стандарт IEEE 802.3ad (коммутатор требует отдельной настройки);
 - «Адаптивная балансировка нагрузки передачи» – исходящий трафик распределяется в соответствии с текущей нагрузкой (с учетом скорости) на интерфейсах (для данного режима необходима его поддержка в драйверах сетевых карт). Входящие пакеты принимаются только активным сетевым интерфейсом;
 - «Адаптивная балансировка нагрузки» – включает в себя балансировку исходящего трафика и балансировку на прием (rlb) для IPv4 трафика и не требует применения специальных коммутаторов. Балансировка на прием достигается на уровне протокола ARP путем перехвата ARP ответов локальной системы и перезаписи физического адреса на адрес одного из сетевых интерфейсов (в зависимости от загрузки);
- 4) указать, если это необходимо, параметры объединения в поле «Параметры объединения»;
 - 5) нажать на кнопку «Назад»;
 - 6) в результате будет создан агрегированный интерфейс bond0. Для данного интерфейса можно задать IP-адрес и, если необходимо, дополнительные параметры (рис. 150);
 - 7) нажать на кнопку «Применить».

Объединенный интерфейс bond0

Используемые интерфейсы: enp0s3, enp0s8

Доступные интерфейсы:

Политика

- Round-robin
- Активный-резервный
- XOR
- Широковещательная
- Агрегирование каналов по стандарту IEEE 802.3ad
- Адаптивная балансировка нагрузки передачи
- Адаптивная балансировка нагрузки

Параметры объединения: miimon=100 lacp_rate=1 xmit_hash_policy=2

[Назад](#)

Рис. 149 – Выбор сетевых интерфейсов для объединения

Имя компьютера: server

Интерфейсы

bond0

Объединение: enp0s3 enp0s8
Интерфейс ВЫКЛЮЧЕН

Версия протокола IP: IPv4 Включить

Конфигурация: Вручную

IP-адреса: 192.168.0.185/24 [Удалить](#)

Добавить IP: /24 (255.255.255.0) [Добавить](#)

Шлюз по умолчанию: 192.168.0.1

DNS-серверы: 8.8.8.8

Домены поиска:
(несколько значений записываются через пробел)

[Дополнительно...](#)

[Создать объединение...](#) [Удалить объединение...](#) [Настроить объединение...](#)

[Создать сетевой мост...](#) [Удалить сетевой мост...](#) [Настроить сетевой мост...](#)

[Применить](#) [Сбросить](#)

Рис. 150 – Настройки интерфейса bond0

Информацию о получившемся агрегированном интерфейсе можно посмотреть в `/proc/net/bonding/bond0`.

Для удаления агрегированного интерфейса необходимо выбрать его в списке «Интерфейсы» и нажать на кнопку «Удалить объединение...».

8.2.3. Сетевые мосты

Модуль «Сетевые мосты» (пакет `alterator-net-bridge`) позволяет организовать виртуальный сетевой мост.

⚠ Если интерфейсы, входящие в состав моста, являются единственными физически подключенными и настройка моста происходит с удаленного узла через эти интерфейсы, то требуется соблюдать осторожность, так как эти интерфейсы перестанут быть доступны.

Для создания Ethernet-моста необходимо выполнить следующие действия:

- 1) у интерфейсов, которые будут входить в мост, удалить IP-адреса и шлюз по умолчанию (если они были установлены);
- 2) нажать на кнопку «Создать сетевой мост...»(рис. 151);

Имя компьютера:

Интерфейсы

enp0s3
enp0s8

Сетевая карта: Intel Corporation 82540EM Gigabit Ethernet Controller
провод подсоединён
MAC: 08:00:27:33:68:99

Версия протокола IP: IPv4 Включить

Конфигурация: Вручную

IP-адреса:

Добавить + IP: /24 (255.255.255.0)

Шлюз по умолчанию:

DNS-серверы:

Домены поиска:
(несколько значений записываются через пробел)

Рис. 151 – Настройка сети в веб-интерфейсе

- 3) в окне «Сетевые мосты» в поле «Интерфейс-мост» ввести имя моста;
- 4) в выпадающем списке «Тип моста» выбрать тип моста: «Linux Bridge» (по умолчанию) или «Open vSwitch»;
- 5) переместить сетевые интерфейсы, которые будут входить в мост, из списка «Доступные интерфейсы» в список «Члены»;
- 6) нажать на кнопку «Ок» (рис. 152);

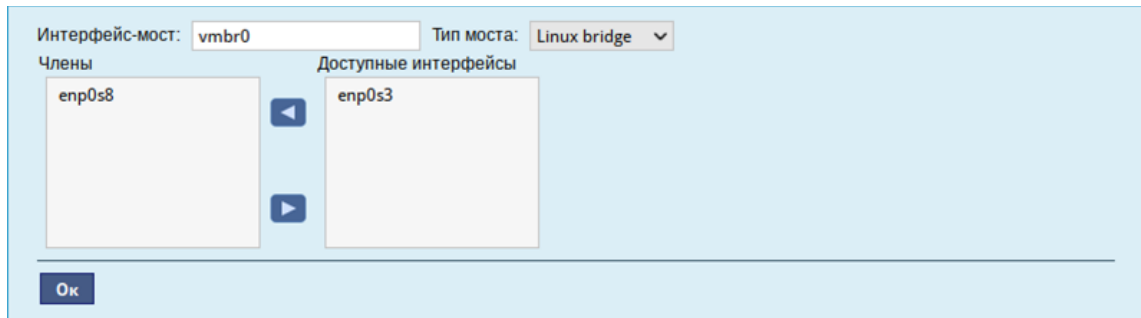


Рис. 152 – Выбор сетевых интерфейсов для моста

- 7) в результате будет создан сетевой интерфейс моста (в примере vmbr0). Для данного интерфейса можно задать IP-адрес и, если необходимо, дополнительные параметры (рис. 153);

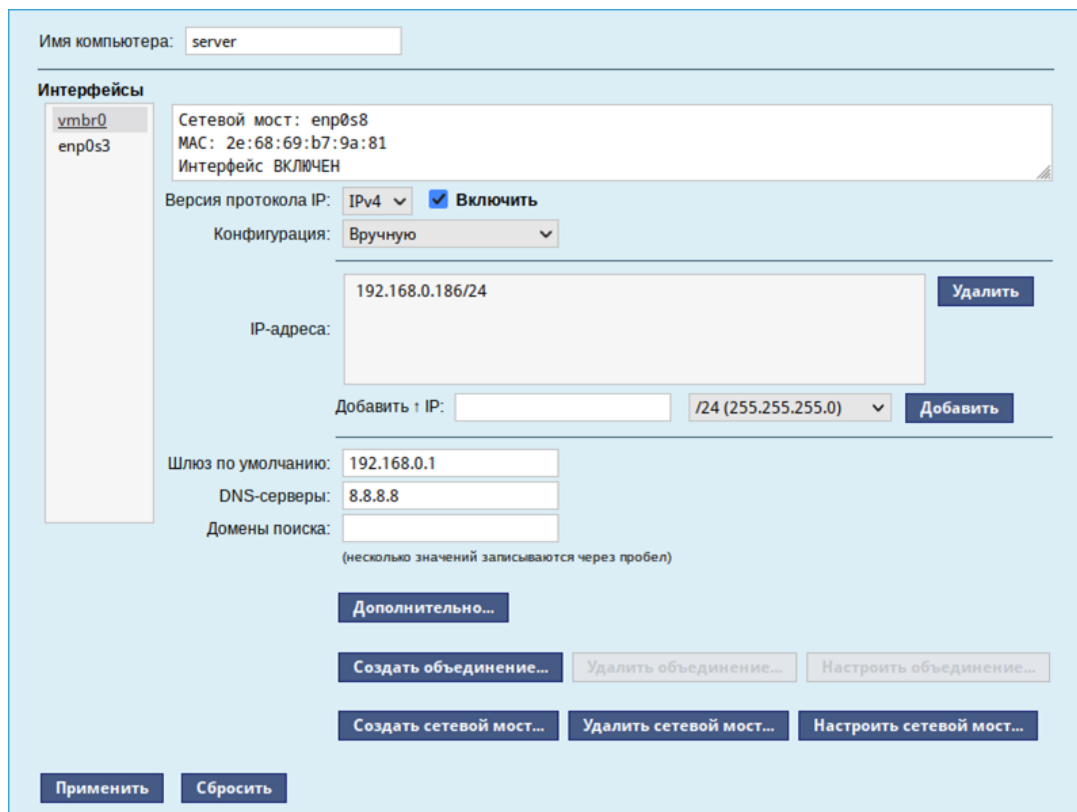


Рис. 153 – Настройка параметров сетевого интерфейса vmbr0

8) нажать на кнопку «Применить».

Для удаления интерфейса моста необходимо выбрать его в списке «Интерфейсы» и нажать кнопку «Удалить сетевой мост...».

8.2.4. Настройка общего подключения к сети Интернет

Пользователи корпоративных сетей обычно подключаются к сети Интернет через один общий канал. Для организации совместного доступа к сети Интернет стандартными средствами поддерживаются две технологии, которые могут использоваться как по отдельности, так и совместно:

- использование прокси-сервера;
- использование NAT.

Оба способа предполагают, что соединение с сетью Интернет компьютера, через который предполагается настроить общий выход, предварительно сконфигурировано. Сделать это можно в разделе ЦУС «Сеть» (см. п. 8.2.1).

8.2.4.1. Прокси-сервер

Отличительной особенностью использования прокси-сервера является то, что, помимо предоставления доступа к веб-сайтам, прокси-сервер кэширует загруженные страницы, а при повторном обращении к ним – отдает их из своего кэша. Это может существенно снизить потребление трафика.

У прокси-сервера есть два основных режима работы:

- прозрачный;
- обычный.

Для работы с прокси-сервером в прозрачном режиме не потребуется специальная настройка рабочих станций. Они лишь должны использовать сервер в качестве шлюза по умолчанию. Этого можно добиться, сделав соответствующие настройки на DHCP-сервере.

Для использования прокси-сервера в обычном режиме потребуется на каждом клиенте в настройках браузера указать данные прокси-сервера (IP-адрес и порт).

Преимуществом обычного режима работы, требующего перенастройки программ локальной сети, является возможность производить аутентификацию пользователей и контролировать их доступ во внешнюю сеть.

В различных браузерах местоположение формы настройки на прокси-сервер различное. Например, в браузере Firefox она доступна через меню «Правка» → «Настройки» → «Основные» → «Настройки сети» кнопка «Настроить...». Здесь следует выбрать «Ручная настройка прокси» и указать IP-адрес и порт прокси-сервера.

По умолчанию прокси-сервер не предоставляет доступ в Интернет никому кроме себя самого. Список сетей, обслуживаемых прокси-сервером можно изменить, нажав на кнопку «Разрешенные сети...» в модуле ЦУС «Прокси-сервер» (пакет alterator-squid) из раздела «Серверы» (рис. 154).

Основные параметры

Основные параметры управления прокси-сервером

Включить сервис прокси-сервера

Выберите режим проксирования: **Прозрачный** ▾

Выберите способ аутентификации: **Без аутентификации** ▾

Порт прокси-сервера: **3128**

(номер порта)

Разрешённые сети... **Разрешённые протоколы...**

Применить

Доступ к доменам

Для каждой из выбранной группы может быть задана политика разрешения или запрета на доступ к указанным в поле внизу доменам.

Все пользователи
Авторизованные пользователи

Группа: **All users**

Политика доступа группы: **Разрешить доступ** ▾

Список суффиксов доменов:

(Список доменных суффиксов разделённых пробелами; каждый суффикс начинается с точки)

Сохранить

Рис. 154 – Модуль «Прокси-сервер»

Для того чтобы включить аутентификацию пользователей и контролировать их доступ во внешнюю сеть, необходимо выбрать обычный режим проксирования и способ аутентификации, отличный от «Без аутентификации» (рис. 155).

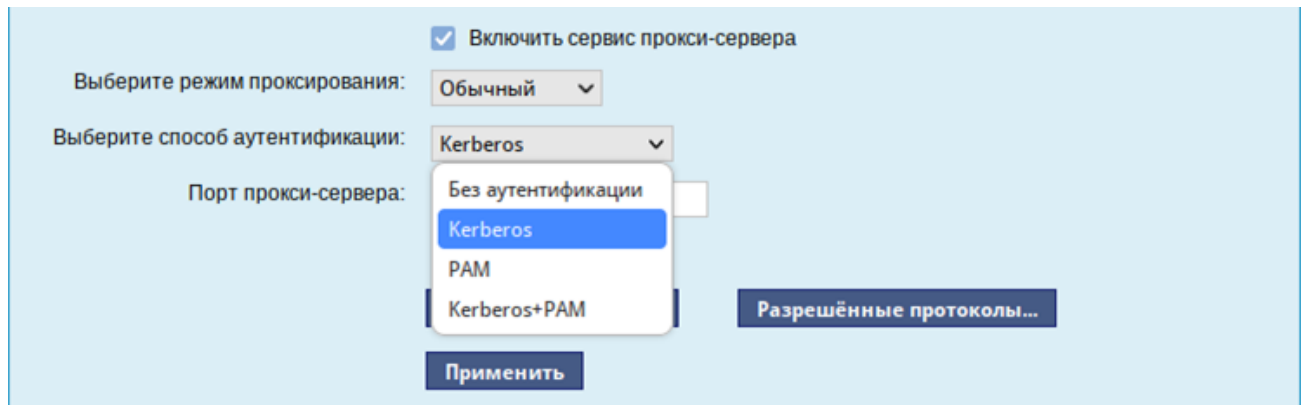


Рис. 155 – Модуль Настройка аутентификации пользователей

Прокси-сервер принимает запросы из локальной сети и, по мере необходимости, передает их во внешнюю сеть. Поступление запроса ожидается на определенном порту, который по умолчанию имеет стандартный номер 3128. Если по каким-то причинам нежелательно использовать данный порт, то можно поменять его значение на любое другое.

Перед тем как выполнить перенаправление запроса, прокси-сервер проверяет принадлежность сетевого адрес узла, с которого запрос был отправлен к группе внутренних сетевых адресов. Для того чтобы запросы, отправленные из локальной сети, обрабатывались прокси-сервером, необходимо добавить соответствующую группу адресов (адрес подсети и адресную маску) в список внутренних сетей в разделе «Разрешенные сети» (рис. 156).

Вторым условием передачи запроса является принадлежность целевого порта к разрешенному диапазону. Посмотреть и отредактировать список разрешенных целевых портов можно в разделе «Разрешенные протоколы» (рис. 157).

Разрешённые сети

Запросы из указанных сетей будут обработаны. Запросы из других сетей будут проигнорированы.

192.168.0.0/24 (Network1)

Сеть IP: 192.168.0.0/24
(IP-адрес/биты подсети)

Комментарий: Network1

Применить Сбросить

Удалить

Создать

Назад

Рис. 156 – Настройка списка внутренних сетей

Разрешённые протоколы

Запросы из указанных сетей будут обработаны. Запросы из других сетей будут проигнорированы.

HTTPS (C)
GSS-HTTP
GOPHER
WAIS
RSYNC
FTP
SWAT
HTTP
CUPS
SNEWS (C)
Multilingual HTTP
Filemaker

С порта: 443 По порт: 443
(номер порта) (номер порта)

Способ соединения: Сквозной
 Включить прозрачное перенаправление

Комментарий: HTTPS (C)

Применить Сбросить

Удалить

Создать

Назад

Рис. 157 – Настройка списка разрешенных целевых портов

Прокси-сервер позволяет вести статистику посещения страниц в Интернете. Она доступна в модуле ЦУС «Прокси-сервер» (пакет alterator-squidmill) в разделе «Статистика» (см. п. 8.6.2). Основное предназначение статистики – просмотр отчета об объеме полученных из Интернета данных в привязке к пользователям (если включена аутентификация) или к IP-адресам клиентов.

Примечание. Статистика не собирается по умолчанию. Включить ее сбор следует в модуле ЦУС «Прокси-сервер» (раздел Статистика) (см. п. 8.6.2). Для этого отметьте «Включить сбор данных прокси-сервера» и нажмите кнопку «Применить».

Примечание. Для учета пользователей в статистике нужно добавить хотя бы одно правило. Самое очевидное – запрет неуаутентифицированных пользователей. Только после этого в статистике начнут показываться пользователи.

8.2.4.2. NAT

NAT (Network Address Translation, преобразование сетевых адресов) – это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Таким образом, компьютеры локальной сети, имеющие IP-адреса, зарезервированные для использования исключительно в локальных сетях, могут использовать общий канал доступа к сети Интернет (общий внешний IP-адрес). При этом на компьютере-шлюзе, непосредственно подключенном к сети Интернет, выполняется преобразование адресов.

Настройка NAT осуществляется в модуле ЦУС «Внешние сети» (пакет alterator-net-iptables, режим эксперт) из раздела «Брандмауэр». Для минимальной настройки достаточно выбрать режим работы «Шлюз (NAT)», отметить правильный внешний сетевой интерфейс (рис. 158) и нажать на кнопку «Применить».

Версия IP: Включить брандмауэр

Выберите режим работы:

Выберите внешние интерфейсы: enp0s3 (Intel Corporation 82540EM Gigabit Ethernet Controller) 192.168.0.185/24

Разрешить входящие соединения на внешних интерфейсах:

Службы:

- Центр управления системой (www)
- Система печати CUPS
- DHCP
- DNS
- Передача файлов (FTP)
- Почтовый сервер (IMAP)
- LDAP
- OpenVPN
- Почтовый сервер (POP3)
- Прокси-сервер
- Файловый сервер (Samba)
- Почтовый сервер (SMTP)

Рис. 158 – Настройка NAT

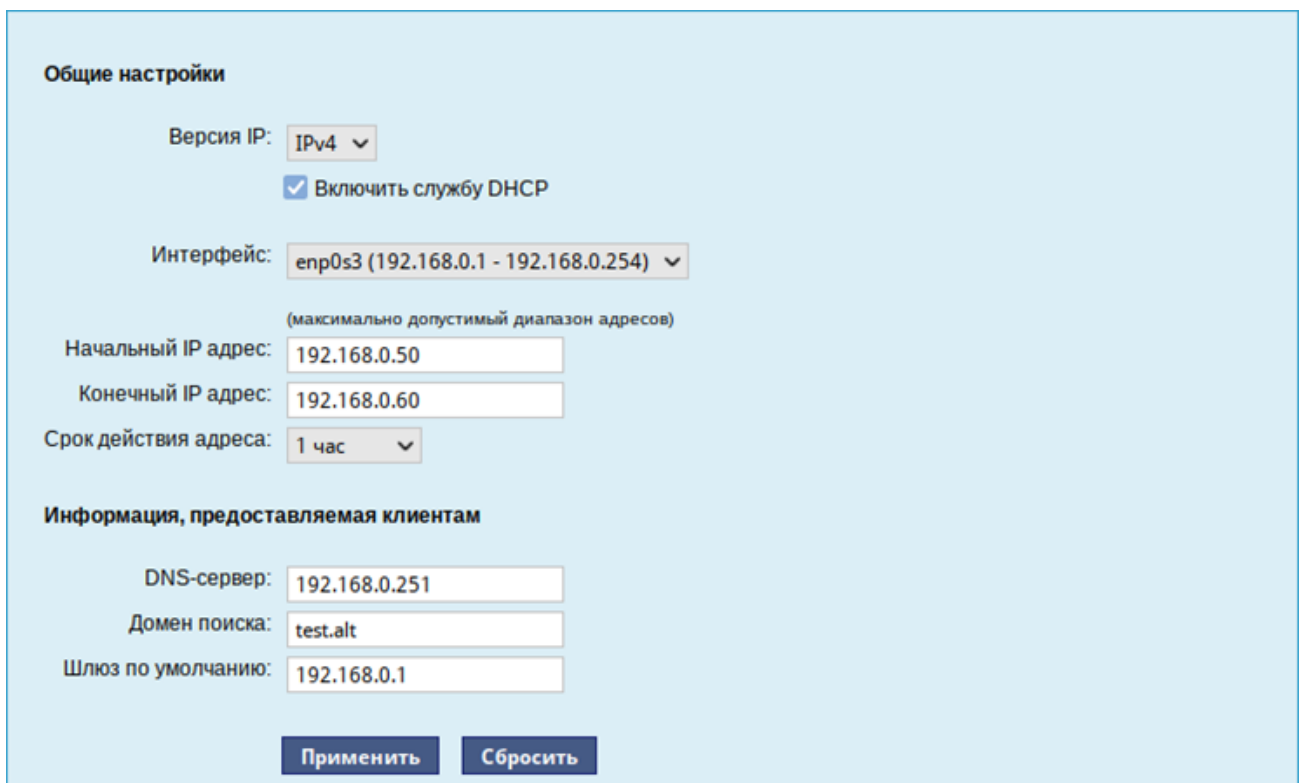
8.2.5. Автоматическое присвоение IP-адресов (DHCP-сервер)

DHCP (Dynamic Host Configuration Protocol) – протокол, позволяющий клиенту самостоятельно получить IP-адрес из зарезервированного диапазона адресов, а также дополнительную информацию о локальной сети (DNS-сервер сети, домен поиска, шлюз по умолчанию). Это облегчает администрирование клиентских машин, избавляя администратора домена от необходимости вручную настраивать сетевые интерфейсы на компьютерах локальной сети.

Чтобы настраивать DHCP-сервер, на машине должен быть хотя бы один статически сконфигурированный Ethernet-интерфейс.

Настройка DHCP-сервера осуществляется в модуле ЦУС «DHCP-сервер» (пакет alterator-dhcp) из раздела «Серверы».

Для включения DHCP-сервера необходимо установить флаг «Включить службу DHCP» (рис. 159), указать начальный и конечный IP-адрес, а также шлюз по умолчанию (обычно это IP-адрес сервера на сетевом интерфейсе, обслуживающем локальную сеть).



Общие настройки

Версия IP: IPv4

Включить службу DHCP

Интерфейс: enp0s3 (192.168.0.1 - 192.168.0.254)

(максимально допустимый диапазон адресов)

Начальный IP адрес: 192.168.0.50

Конечный IP адрес: 192.168.0.60

Срок действия адреса: 1 час

Информация, предоставляемая клиентам

DNS-сервер: 192.168.0.251

Домен поиска: test.alt

Шлюз по умолчанию: 192.168.0.1

Применить Сбросить

Рис. 159 – Настройка DHCP-сервера

Теперь при включении любой клиентской машины с настройкой «получение IP и DNS автоматически» будет присваиваться шлюз 192.168.0.1, DNS 192.168.0.251 и адреса начиная с 192.168.0.50 по порядку включения до 192.168.0.60.

Иногда бывает полезно выдавать клиенту один и тот же IP-адрес независимо от момента обращения. В этом случае он определяется по аппаратному адресу (MAC-адресу) сетевой карты клиента. Для добавления своих значений в таблицу соответствия статических адресов следует ввести IP-адрес и соответствующий ему MAC-адрес и нажать кнопку «Добавить» (рис. 160).

Статические адреса

<input type="checkbox"/>	IP-адрес	MAC-адрес	Имя компьютера
<input type="checkbox"/>	192.168.0.55	08:00:27:4c:d4:84	teacher

Удалить выделенные

Новый статический адрес:

IP-адрес: 192.168.0.59

MAC-адрес: 3c:21:9c:ae:28:b0

Имя компьютера: test

Добавить

Рис. 160 – Привязка IP-адреса к MAC-адресу

Выданные IP-адреса можно увидеть в списке «Текущие динамически выданные адреса». Здесь также имеется возможность зафиксировать выданные адреса за данными компьютерами. Для этого необходимо отметить хост, за которым нужно закрепить IP-адрес, и нажать кнопку «Зафиксировать адрес для выбранных компьютеров» (рис. 161).

Текущие динамически выделенные адреса

<input type="checkbox"/>	Имя компьютера	MAC-адрес	IP-адрес	Годен до
<input type="checkbox"/>	teacher	9c:2d:cd:60:4e:03	192.168.0.51	Чт 14 сен 2023 21:08:20 EET

Зафиксировать адрес для выбранных компьютеров

Рис. 161 – Список динамически выданных адресов

8.3. Сетевая установка ОС на рабочие места

Одной из удобных возможностей ОС Альт СП при разворачивании инфраструктуры является сетевая установка. При помощи нее можно производить установку ОС Альт СП не с компакт-диска дистрибутива, а загрузив инсталлятор по сети.

8.3.1. Подготовка сервера

Перед началом установки рабочих станций следует произвести предварительную настройку сервера: задать имя сервера (модуль «Ethernet-интерфейсы» в ЦУС), включить DHCP-сервер (модуль «DHCP-сервер»), задать имя домена.

Примечание. При сетевой установке с сервера будут переняты настройки домена, и будет включена централизованная аутентификация. Если устанавливается ОС Альт СП с компакт-диска, то настройку домена и аутентификации надо будет производить отдельно на каждом компьютере.

Примечание. Каталог `/var/lib/tftpboot` должен быть доступен клиенту через TFTP, каталог `/srv/public/netinst` должен быть доступен клиенту через NFS.

Примечание. В настоящий момент модуль «Сервер сетевых установок» не позволяет настроить установку в EFI-режиме для PXE-установки.

Перед активацией сетевой установки потребуется импортировать установочный компакт-диска дистрибутива ОС Альт СП, предварительно вставив его в DVD-привод сервера, либо используя образ диска, расположенный на файловой системе на сервере.

Примечание. Локальный файл должен быть доступен для nobody и должен находиться на сервере, где запущен alterator-netinst.

В разделе «Сервер сетевых установок» (пакет alterator-netinst) необходимо указать, откуда импортировать новый образ, и нажать кнопку «Добавить» (рис. 162).

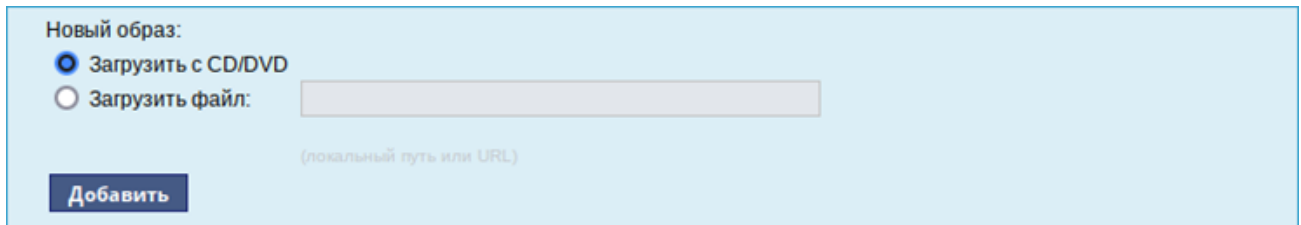


Рис. 162 – Загрузка CD/DVD

Процесс добавления образа (рис. 163) занимает какое-то время. Необходимо дождаться окончания этого процесса.

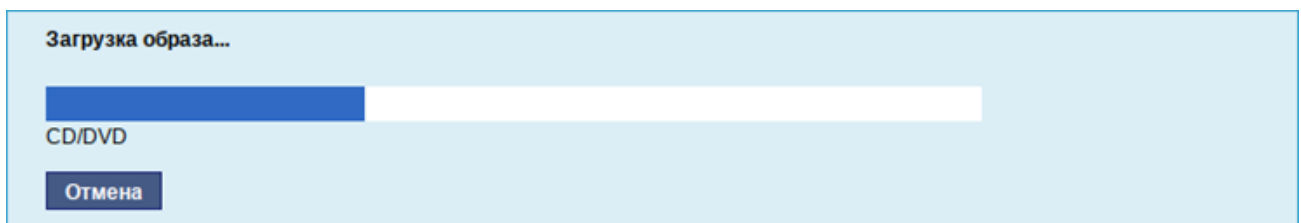


Рис. 163 – Процесс загрузки образа

После добавления образа он появится в списке «Доступные образы дисков». Необходимо выбрать из списка один из образов (рис. 164) и нажать кнопку «Выбрать».

На этом подготовка сервера к сетевой установке рабочих станций завершена.

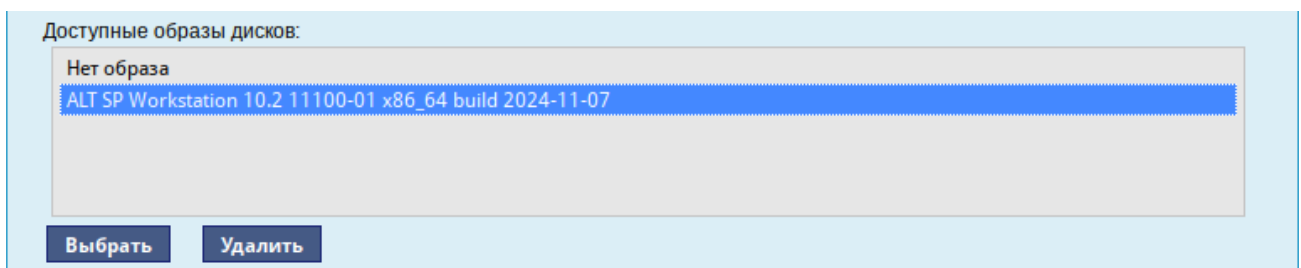


Рис. 164 – Выбор доступного образа диска

Дополнительно данный модуль позволяет выбрать вариант загрузки (рис. 165), например, непосредственно загружать ОС некоторых Live-версий дистрибутивов.

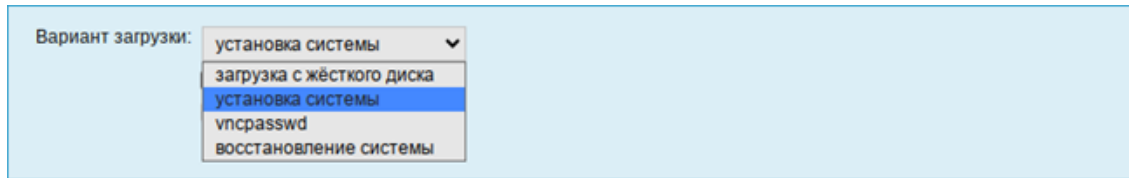


Рис. 165 – Выбор варианта загрузки

Для включения режима автоматической установки необходимо выбрать образ, выбрать вариант загрузки «Установка системы», установить отметку в поле «Автоматическая установка», в поле «Метаданные» указать каталог с установочными файлами (рис. 166) и сохранить настройки, нажав кнопку «Применить».

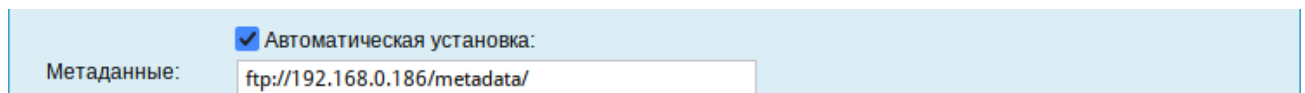


Рис. 166 – Включение режима автоматической установки

Если отмечен пункт «Включить установку по VNC», то далее необходимо выбрать направление соединения (рис. 167). Удаленный доступ к компьютеру бывает двух видов:

- со стороны клиента – во время установки администратор может с помощью VNC-клиента подключиться к компьютеру, на который производится установка, зная его IP-адрес и заданный пароль;
- со стороны сервера – во время установки с каждого компьютера инициируется подключение к запущенному на заданном компьютере VNC-клиенту. Компьютер-приемник соединений задается IP-адресом или именем.

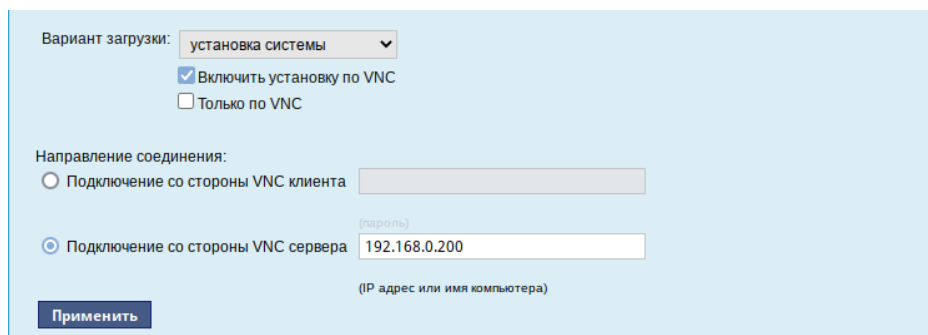


Рис. 167 – Виды удаленного доступа к компьютеру

В случае, когда работа с аппаратной подсистемой ввода-вывода невозможна (например, если клавиатура, мышь или монитор отсутствуют), можно использовать вариант «Только по VNC».

Если необходимо управлять установкой удаленно, необходимо отметить пункт «Включить установку по VNC» и пункт «Подключение со стороны VNC сервера» раздела «Направление соединения» и указать в поле IP-адрес или имя компьютера, с которого будет происходить управление. Для приема подключения можно запустить, например, `vncviewer -listen`.

⚠ По окончании процесса установки ОС на рабочих станциях необходимо отключить сетевую установку. Это можно сделать, выбрав в списке «Доступные образы дисков» пункт «Нет образа» и подтвердив действие нажатием кнопки «Выбрать».

8.3.2. Подготовка рабочих станций

Для сетевой установки следует обеспечить возможность загрузки по сети рабочих станций, на которых будет производиться установка ОС.

Большинство современных материнских плат имеют возможность загрузки по сети, однако она по умолчанию может быть отключена в BIOS (БСВВ). Различные производители материнских плат дают разные названия данной возможности, например: «Boot Option ROM» или «Boot From Onboard LAN».

Примечание. Некоторые материнские платы позволяют выбрать источник загрузки во время включения компьютера. Эта возможность может называться, например, «Select boot device» или «Boot menu».

Последовательность установки при установке с компакт-диска и при сетевой установке не отличаются друг от друга. Подробный о процессе см. в разделе 5 «Установка ОС Альт СП».

8.4. Соединение удаленных офисов (OpenVPN-сервер)

ОС Альт СП предоставляет возможность безопасного соединения удаленных офисов, используя технологию VPN (англ. Virtual Private Network – виртуальная частная сеть), которая позволяет организовать безопасные зашифрованные соединения через публичные сети (например, Интернет) между удаленными офисами или локальной сетью и удаленными пользователями. Таким образом,

можно связать различные офисы организации, что делает работу с документами, расположенными в сети удаленного офиса, более удобной.

Помимо соединения целых офисов, также существует возможность организовать доступ в офисную сеть для работы в ней извне. Это означает, например, что сотрудник может работать в своем привычном окружении, даже находясь в командировке или просто из дома.

8.4.1. Настройка OpenVPN-сервера

OpenVPN-сервер может быть развернут, например, на базе ОС Альт 8 СП Сервер 64 бит (x86_64). Для организации VPN соединения на стороне сервера предусмотрен модуль ЦУС «OpenVPN-сервер» (пакет alterator-openvpn-server) из раздела «Серверы».

Используя модуль «OpenVPN-сервер», можно:

- включить/отключить OpenVPN-сервер;
- настроить параметры сервера: тип, сети сервера, использование сжатия и т. д.;
- управлять сертификатами сервера;
- настроить сети клиентов.

Особое внимание при планировании и настройке подключений следует обратить на используемые сети. Они не должны пересекаться.

Для создания соединения нужно установить флаг «Включить службу OpenVPN» (рис. 168), выбрать тип подключения: маршрутизируемое (используется TUN) или через мост (используется TAP), и проверить открываемую по соединению сеть (обычно это локальная сеть в виде IP-адреса и маски подсети).

Включить службу OpenVPN

Тип: Маршрутизируемое (TUN)

Сети сервера: 192.168.0.0/255.255.255.0 **Удалить**

Новая сеть:

Маска сети: /24 (255.255.255.0) **Добавить**

VPN сеть: 10.8.0.0

Маска сети: /24 (255.255.255.0)

Алгоритм шифрования: default

Алгоритм шифрования TLS: default

Алгоритм хэширования: default

Отключить согласование алгоритмов шифрования (NCP)

Порт: 1194

Сжатие LZO

Использовать соединение TCP

Сертификат и ключ SSL...

Положить сертификат УЦ: **Положить**

Сети клиентов...

Применить **Сбросить**

Рис. 168 – Модуль «OpenVPN-сервер»

Для настройки сертификата и ключа SSL нужно нажать на кнопку «Сертификат и ключ SSL...». Откроется окно модуля «Управление ключами SSL» (пакет alterator-sslkey) (рис. 169).

Здесь нужно заполнить поле «Общее имя (CN)» и поле «Страна (C)» (прописными буквами), отметить пункт «(Пере)создать ключ и запрос на подпись» и нажать на кнопку «Подтвердить». После чего станет активной кнопка «Забрать запрос на подпись».

Если нажать на кнопку «Забрать запрос на подпись» (рис. 170), запрос на подпись (файл openvpn-server.csr) будет загружен в каталог загрузок.

Настройки SSL

Общее имя (CN):

(имя компьютера для сервера или что-либо другое для клиента)

Страна (C):

(двухбуквенный код страны)

Местоположение (L):

(название города или области, написанное латинскими буквами)

Организация (O):

(название организации, написанное латинскими буквами)

Подразделение (OU):

(название подразделения, написанное латинскими буквами)

E-mail адрес:

(ваш адрес электронной почты)

(Пере)создать ключ и запрос на подпись

Рис. 169 – Модуль «Управление ключами SSL»

Подпись

Положить сертификат, подписанный УЦ:

Рис. 170 – Кнопка «Забрать запрос на подпись»

В модуле «Управление ключами SSL» появится новый ключ «openvpn-server (Нет сертификата)» (рис. 171).

Подписать сертификат на сервере можно в модуле «Удостоверяющий Центр» (пакет alterator-ca) → «Управление сертификатами» (рис. 172):

- заполнить поля «Страна» и «Организация»;
- нажать на кнопку «Обзор...»;
- указать путь до полученного файла `openvpn-server.csr`;
- нажать на кнопку «Загрузить запрос».

Примечание. Для доступа к модулям «Управление ключами SSL» и «Удостоверяющий Центр» необходимо переключиться в режим эксперта.

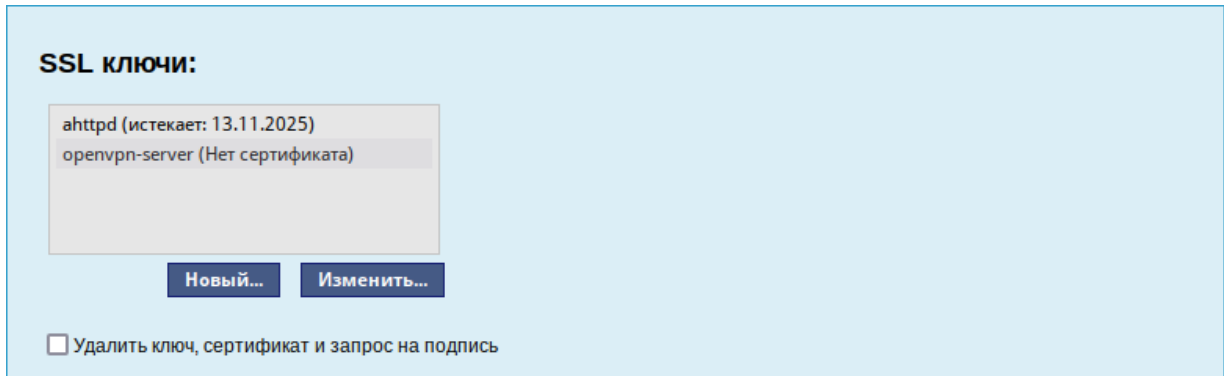


Рис. 171 – SSL ключи

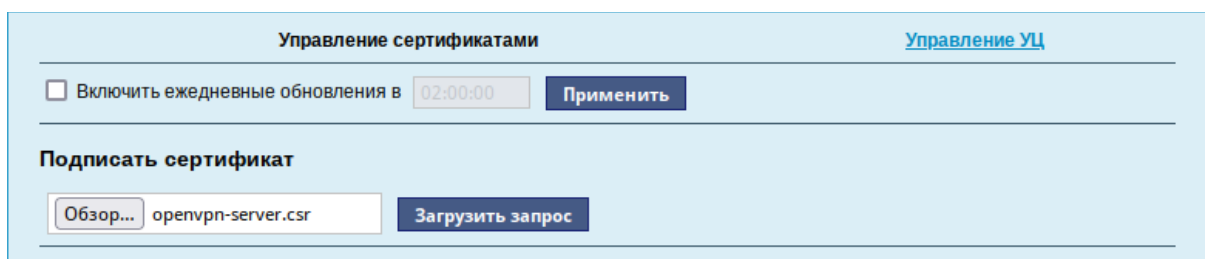


Рис. 172 – Кнопка «Подписать сертификат»

В результате на экране появится две группы цифр и кнопка «Подписать». Нужно нажать на кнопку «Подписать» (рис. 173), подписанный сертификат (файл `output.pem`) будет загружен в каталог загрузок.

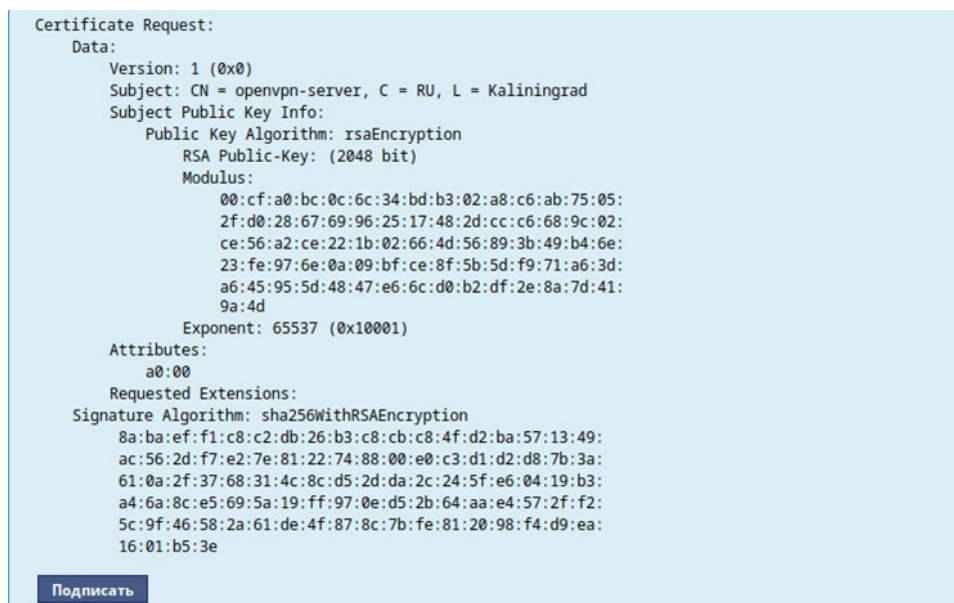


Рис. 173 – Подписание сертификата

Можно также подписать сертификат в консоли, с помощью openssl. Для этого необходимо выполнить следующие действия:

- 1) изменить значение параметра policy в файле `/var/lib/ssl/openssl.cnf` для возможности подписывать любые сертификаты:

```
policy = policy_anything
```

- 2) создать каталоги:

```
# mkdir -p /root/CA/demoCA
# cd /root/CA
# mkdir -p ./demoCA/newcerts
```

Создать файл базы с действующими и отозванными сертификатами:

```
# touch ./demoCA/index.txt
```

Создать файл индекса для базы ключей и сертификатов:

```
# echo '01' > ./demoCA/serial
```

Создать файл индекса для базы отозванных сертификатов:

```
# echo '01' > ./demoCA/crlnumber
```

- 3) создать «самоподписанный» сертификат `ca-root.pem` и закрытый ключ `ca-root.key`, которыми будут заверяться/подписываться ключи и сертификаты клиентов:

```
# openssl req -new -x509 -keyout ca-root.key -out ca-root.pem
```

Ввести пароль для закрытого ключа и ответить на запросы о владельце ключа.

Пароль должен быть не короче 4 символов.

- 4) подписать запрос на сертификат своим «самоподписанным» `ca-root.pem` сертификатом и ключом `ca-root.key` с помощью следующей команды:

```
# openssl ca -cert ca-root.crt -keyfile ca-root.pem -days 3650
-in /home/user/openvpn-server.csr -out /home/user/output.pem
```

где:

- `/home/user/openvpn-server.csr` – запрос на сертификат, файл, полученный в модуле «Управление ключами SSL» (пакет `alterator-sslkey`) (см. рис. 170);

- `/home/user/output.pem` – файл, в который будет записан подписанный сертификат.

Подписанный сертификат (файл `output.pem`) следует положить к его ключу. Для этого в разделе «Управление ключами SSL» нужно выделить ключ «openvpn-server (Нет сертификата)» и нажать кнопку «Изменить». В появившемся окне, в пункте «Положить сертификат, подписанный УЦ» нужно нажать на кнопку «Обзор», указать путь до файла `output.pem` и нажать на кнопку «Положить» (рис. 174).

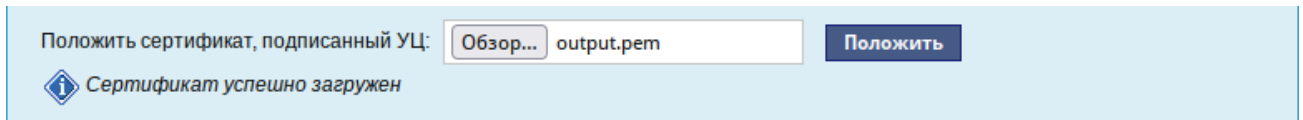


Рис. 174 – Сертификат, подписанный УЦ

В модуле «Управление ключами SSL» видно, что ключ «openvpn-server (истекает_и_дата)» изменился. Ключ создан и подписан.

В модуле «OpenVPN-сервер» необходимо положить сертификат УЦ. Для этого в графе «Положить сертификат УЦ» следует нажать на кнопку «Обзор...», указать путь к файлу сертификата УЦ (`ca-root.pem`) и нажать на кнопку «Положить».

Появится сообщение: «Сертификат УЦ успешно загружен» (рис. 175).

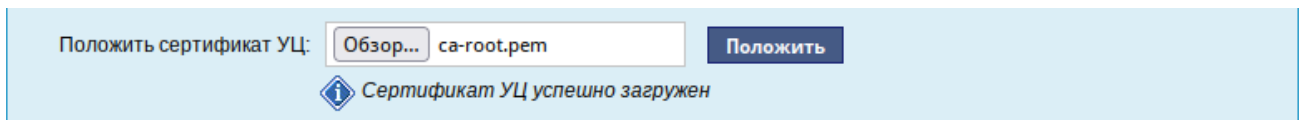


Рис. 175 – Выбор сертификата УЦ в модуле «OpenVPN-сервер»

Примечание. Если использовался модуль «Удостоверяющий Центр», для получения сертификата УЦ необходимо перейти в модуле «Удостоверяющий Центр» на вкладку «Управление УЦ» и забрать сертификат, нажав на ссылку «Сертификат: `ca-root.pem`» (рис. 176).

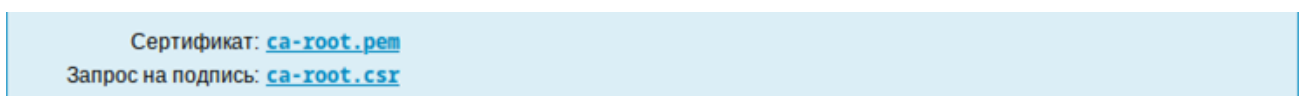


Рис. 176 – Сертификат УЦ

Для включения OpenVPN нужно отметить пункт «Включить службу OpenVPN» и нажать на кнопку «Применить».

8.4.2. Настройка клиентов

Со стороны клиента соединение настраивается в графическом интерфейсе (GUI) ЦУС модуле «OpenVPN-соединения» (пакет alterator-net-openvpn) из раздела «Сеть». Доступ к настроенной приватной сети могут получить пользователи, подписавшие свои ключи и получившие сертификат в удостоверяющем центре на том же сервере.

Для создания нового соединения нужно отметить пункт «Сетевой туннель (TUN)» или «Виртуальное Ethernet устройство (TAP)» и нажать на кнопку «Создать соединение» (рис. 177).

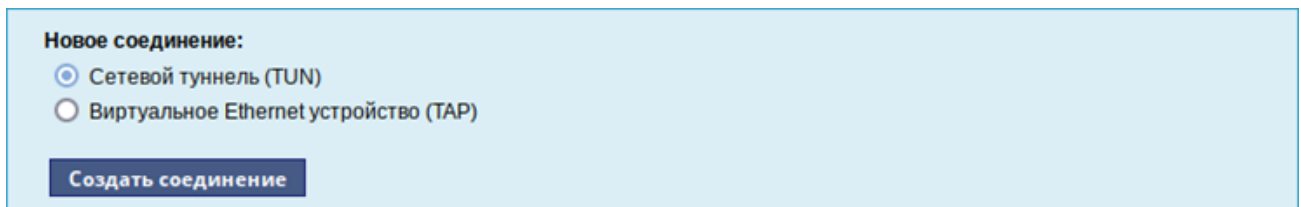


Рис. 177 – Создание нового OpenVPN- соединения

Необходимо обратить внимание, что на стороне клиента должен быть выбран тот же тип виртуального устройства, что и на стороне сервера. Для большинства случаев подходит маршрутизируемое подключение.

В результате станут доступны настройки соединения. На клиенте в модуле «OpenVPN-соединение» нужно указать:

- состояние – «запустить»;
- сервер – IP-адрес сервера или домен;
- порт – 1194;
- ключ – выбрать подписанный на сервере ключ. Ключ (например, openvpn) можно создать в модуле «Управление ключами SSL» и подписать его в модуле «Удостоверяющий Центр» (пакет alterator-ca) на сервере.

Для применения настроек нажать на кнопку «Применить» (рис. 178). Состояние с «Выключено» должно поменяться на «Включено».

Выполнить команду для проверки появилось ли соединение с сервером:

```
ip addr
```

должно появиться новое соединение tun0. При обычных настройках это может выглядеть так:

```
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 100
    link/none
    inet 10.8.0.6 peer 10.8.0.5/32 scope global tun0
        valid_lft forever preferred_lft forever
```

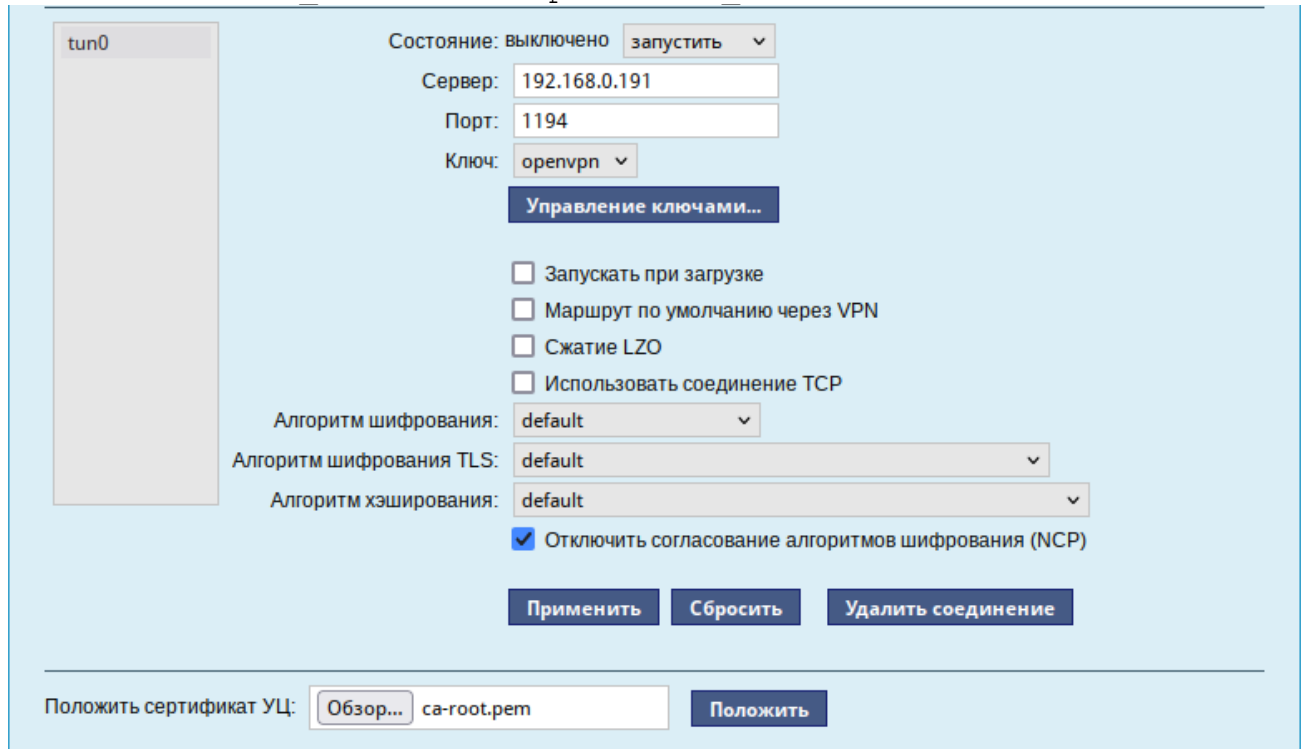


Рис. 178 – Модуль «OpenVPN- соединения»

8.5. Доступ к службам из сети Интернет

8.5.1. Внешние сети

ОС предоставляет возможность организовать доступ к своим службам извне. Например, можно предоставить доступ к корпоративному веб-сайту из сети Интернет. Для обеспечения такой возможности нужно разрешить входящие соединения на внешних интерфейсах. По умолчанию такие соединения блокируются.

Для разрешения внешних и внутренних входящих соединений предусмотрен раздел ЦУС «Брандмауэр».

В списке «Разрешить входящие соединения на внешних интерфейсах» модуля «Внешние сети» (пакет alterator-net-iptables, режим эксперт) перечислены наиболее

часто используемые службы, отметив которые, можно сделать их доступными для соединений на внешних сетевых интерфейсах (рис. 179). Если нужно предоставить доступ к службе, отсутствующей в списке, то нужно задать используемые этой службой порты в соответствующих полях.

Версия IP: IPv4 Включить брандмауэр

Выберите режим работы: Шлюз (NAT)

Выберите внешние интерфейсы: enp0s3 (Intel Corporation 82540EM Gigabit Ethernet Controller) 192.168.0.91/24

Разрешить входящие соединения на внешних интерфейсах:

Службы:

- Центр управления системой (www)
- Система печати CUPS
- DHCP
- DNS
- Передача файлов (FTP)
- Почтовый сервер (IMAP)
- LDAP
- OpenVPN
- Почтовый сервер (POP3)
- Прокси-сервер
- Файловый сервер (Samba)

Рис. 179 – Модуль «Внешние сети»

Можно выбрать один из двух режимов работы:

- роутер – перенаправление пакетов между сетевыми интерфейсами происходит без трансляции сетевых адресов;
- шлюз (NAT) – в этом режиме будет настроена трансляция сетевых адресов (NAT) при перенаправлении пакетов на внешние интерфейсы. Использование этого режима имеет смысл, если на компьютере настроен, по крайней мере, один внешний и один внутренний интерфейс.

Примечания:

1. В любом режиме включено только перенаправление пакетов с внутренних интерфейсов. Перенаправление пакетов с внешних интерфейсов всегда выключено.
2. Все внутренние интерфейсы открыты для любых входящих соединений.

8.5.2. Список блокируемых хостов

Модуль ЦУС «Список блокируемых хостов» (пакет alterator-net-iptables, режим эксперт) предназначен для блокирования любого трафика с указанными узлами. Данный модуль позволяет блокировать любой сетевой трафик с указанными в списке узлов (входящий, исходящий и пересылаемый).

Блокирование трафика с указанных в списке узлов начинается после установки флага «Использовать черный список» (рис. 180).

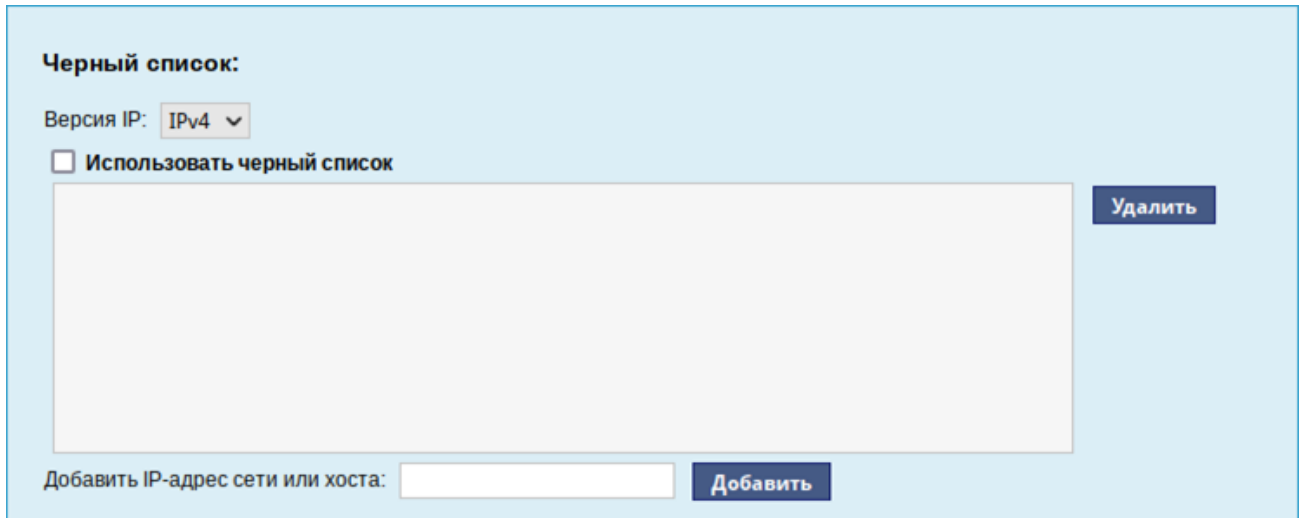


Рис. 180 – Модуль «Список блокируемых хостов»

Для добавления блокируемого узла нужно ввести IP-адрес в поле «Добавить IP-адрес сети или хоста» и нажать на кнопку «Добавить».

Для удаления узла нужно выбрать его из списка и нажать на кнопку «Удалить».

8.6. Статистика

8.6.1. Сетевой трафик

Все входящие и исходящие с сервера сетевые пакеты могут подсчитываться, и выводятся по запросу для анализа.

Модуль ЦУС «Сетевой трафик» (пакет alterator-ulogd) из раздела «Статистика» предназначен для просмотра статистики входящих и исходящих с сервера сетевых пакетов. Данный модуль позволяет оценить итоговый объем

полученных и переданных данных за все время работы сервера, за определенный период времени и по каждой службе отдельно.

Для включения сбора данных нужно установить флаг «Включить сбор данных», и нажать на кнопку «Применить» (рис. 181).

Служба	Входящий трафик(Кб)	Исходящий трафик(Кб)
Центр управления системой (www)	0.0	0.0
Система печати CUPS	0.0	0.0
DHCP	0.0	0.0
DNS	0.0	0.0
Передача файлов (FTP)	0.0	0.0
Почтовый сервер (IMAP)	0.0	0.0
LDAP	0.0	0.0
OpenVPN	0.0	0.0
Почтовый сервер (POP3)	0.0	0.0
Прокси-сервер	0.0	0.0
Файловый сервер (Samba)	0.0	0.0
Почтовый сервер (SMTP)	0.0	0.0
Управление сетью (SNMP)	0.0	0.0
Удалённый доступ (SSH)	0.0	0.0

Рис. 181 – Просмотр статистики входящих и исходящих пакетов

Для просмотра статистики указывается период (в виде начальной и конечной дат). Дата указывается в формате YYYY-MM-DD (год-месяц-день) или выбирается из календаря справа от поля ввода даты. Из списка доступных сетевых интерфейсов нужно выбрать интересующий и нажать на кнопку «Показать» (рис. 181).

Трафик на указанном интерфейсе за заданный период показывается в виде:

- служба (название протокола);
- входящий трафик в Кбайтах;
- исходящий трафик в Кбайтах.

8.6.2. Прокси-сервер

Пересылка каждого запроса во внешнюю сеть фиксируется прокси-сервером в специальном журнале. На основании этих данных автоматически формируются отчеты о статистике использования ресурсов сети, в том числе потраченного времени и количества переданных данных (трафика).

Статистика не собирается по умолчанию. Включить ее сбор следует в модуле ЦУС «Прокси-сервер» (пакет alterator-squidmill) из раздела «Статистика». Для включения сбора статистики прокси-сервера нужно установить флаг «Включить сбор данных прокси-сервера» (рис. 182).

В том случае, если на прокси-сервере производилась аутентификация пользователей, отчеты будут содержать данные об обращениях каждого пользователя. Иначе отчеты будут формироваться только на основании адресов локальной сети.

Включить сбор данных прокси-сервера: Применить

Общий объем трафика принятый за

составляет **0.00 Б**

Список сайтов, набравших

UID/IP-адрес	Количество	Сайт/домен	Время последнего запроса
--------------	------------	------------	--------------------------

Рис. 182 – Настройка сбора статистики прокси-сервера

Для показа отчета нужно задать условия фильтра и нажать на кнопку «Обновить».

Данные в таблице отсортированы по объему трафика в порядке убывания.

Для учета пользователей в статистике нужно добавить хотя бы одно правило. Самое очевидное правило – запрет неаутентифицированных пользователей. Только после этого в статистике начнут показываться пользователи.

8.7. Обслуживание системы

Для безотказной работы системы очень важно следить за корректной работой. Регулярный мониторинг состояния системы, своевременное резервное копирование, обновление установленного ПО, являются важной частью комплекса работ по обслуживанию.

8.7.1. Мониторинг состояния системы

Для обеспечения бесперебойной работы ОС крайне важно производить постоянный мониторинг ее состояния. Все события, происходящие с ОС, записываются в журналы, анализ которых помогает избежать сбоев в работе системы и предоставляет возможность разобраться в причинах некорректной работы.

Для просмотра журналов предназначен модуль ЦУС «Системные журналы» (пакет alterator-logs) из раздела «Система». Интерфейс позволяет просмотреть различные типы журналов с возможностью перехода к более старым или более новым записям.

Различные журналы могут быть выбраны из списка «Журналы» (рис. 183).

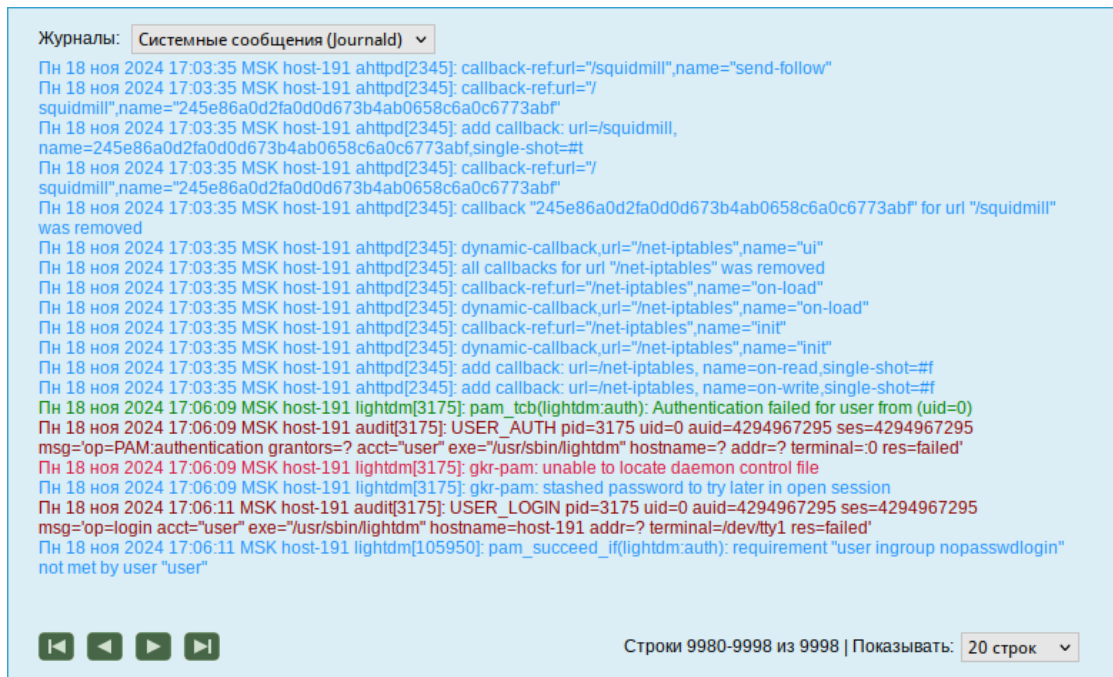


Рис. 183 – Модуль «Системные журналы»

Доступны следующие виды журналов:

- брандмауэр – отображаются события безопасности, связанные с работой межсетевого экрана ОС;
- системные сообщения (Journald) – отображаются события процессов ядра и пользовательской области. У каждого сообщения в этом журнале есть приоритет, который используется для пометки важности сообщений. Сообщения в зависимости от уровня приоритета подсвечиваются цветом.

Каждый журнал может содержать довольно большое количество сообщений.

Уменьшить, либо увеличить количество выводимых строк можно, выбрав нужное значение в списке «Показывать».

8.7.2. Системные службы

Для изменения состояния служб можно использовать модуль ЦУС «Системные службы» (пакет alterator-services) из раздела «Система». Интерфейс позволяет изменять текущее состояние службы и, если нужно, применить опцию запуска службы при загрузке системы (рис. 184).

После выбора названия службы из списка отображается описание данной службы, а также текущее состояние: Работает/Остановлена/Неизвестно.

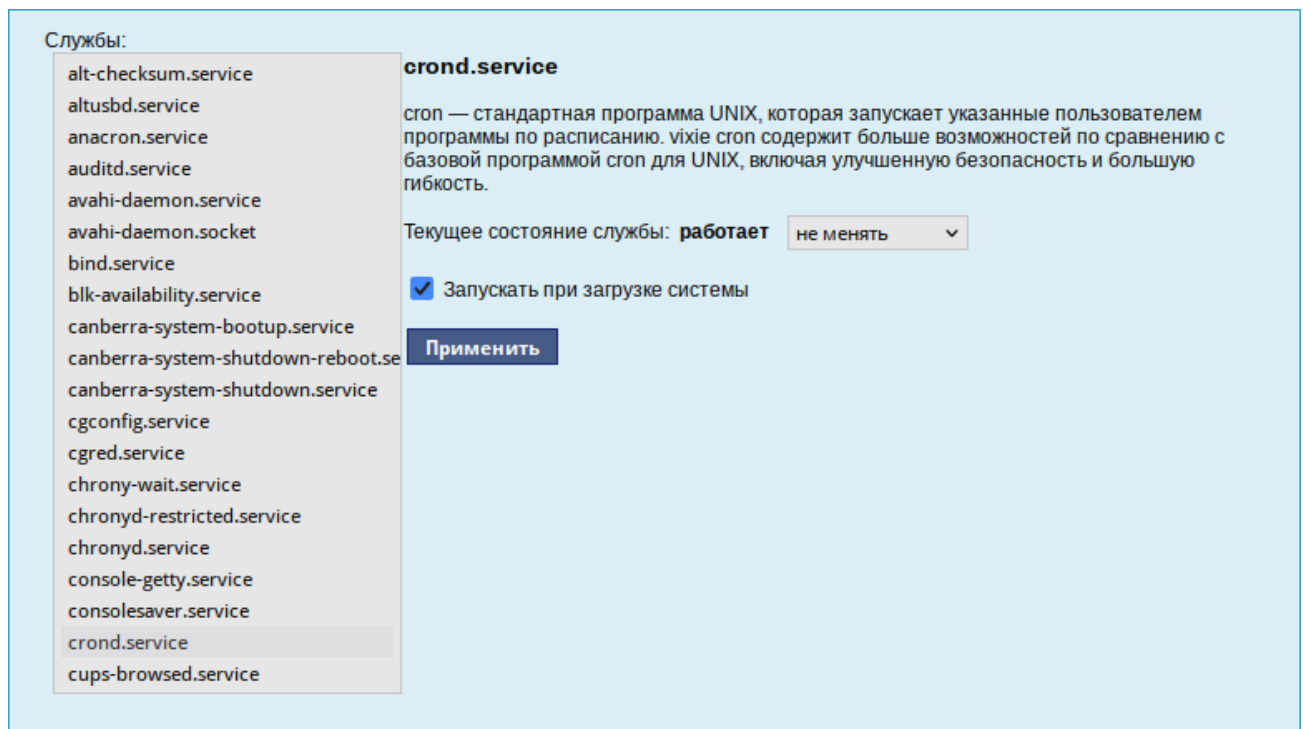


Рис. 184 – Модуль «Системные службы»

8.7.3. Обновление системы

После установки системы крайне важно следить за обновлениями ПО. Обновления для ОС Альт СП могут содержать как исправления, связанные с безопасностью, так и новый функционал или просто улучшение и ускорение алгоритмов. В любом случае настоятельно рекомендуется регулярно обновлять систему для повышения надежности работы системы.

Для автоматизации процесса установки обновлений предусмотрен модуль ЦУС «Обновление системы» (пакет alterator-updates) из раздела «Система». Здесь можно включить автоматическое обновление через Интернет с одного из предлагаемых серверов или задать собственные настройки (рис. 185).

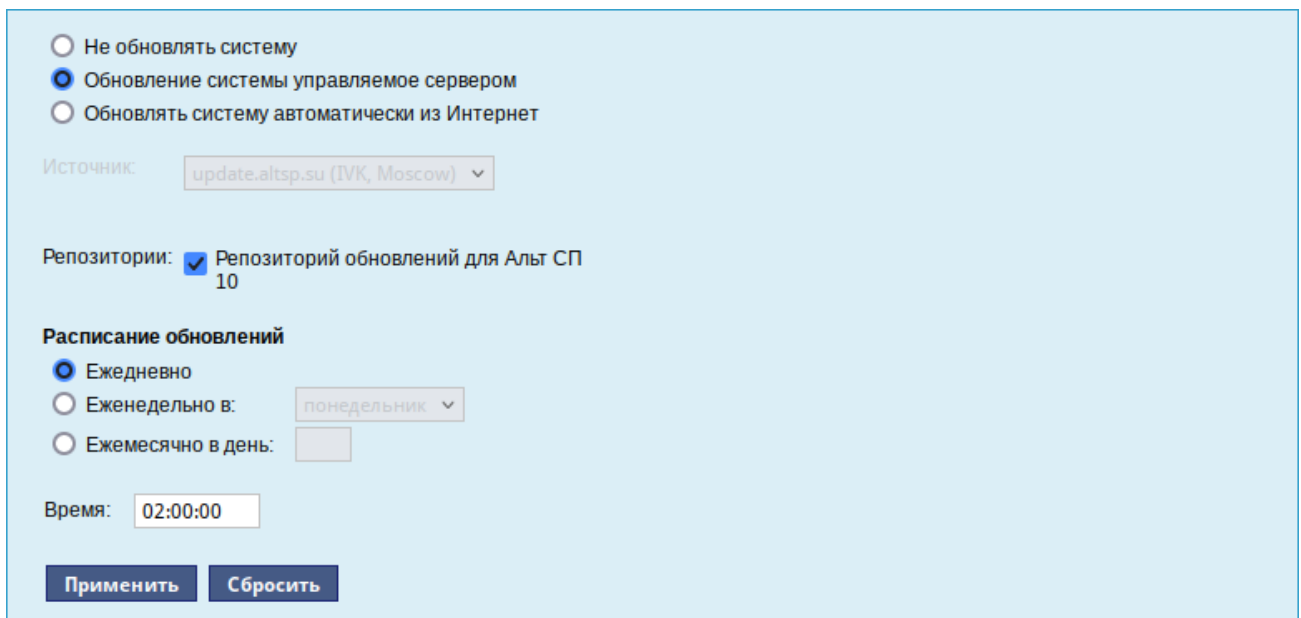


Рис. 185 – Модуль «Обновление системы»

Источник обновлений указывается явно (при выбранном режиме «Обновлять систему автоматически из Интернет») или вычисляется автоматически (при выбранном режиме «Обновление системы, управляемое сервером» и наличии в локальной сети настроенного сервера обновлений (см. в п. 18.14)).

Примечание. Рабочие станции «видят» локальный сервер обновлений, при выборе режима «Обновление системы управляемое сервером» (рис. 185), если они находятся в домене (при этом сервер обновлений должен быть настроен на «Опубликовать как репозиторий для автоматических обновлений»).

Процесс обновления системы будет запускаться автоматически согласно заданному расписанию.

Примечание. Чтобы указать в качестве сервера обновлений локально настроенный источник, необходимо выбрать режим «Обновлять систему автоматически из Интернет», выбрать в списке «Другой адрес» и указать адрес локального сервера обновлений (рис. 186), например, `http://<ip-сервера>/mirror`.

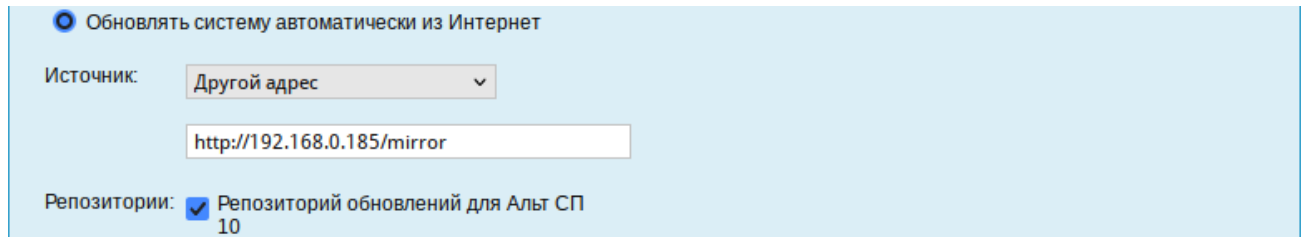


Рис. 186 – Указание источника обновлений

8.7.4. Обновление систем, не имеющих выхода в Интернет

Для систем, не имеющих прямого выхода в Интернет, рекомендуется установка отдельного сервера обновлений (например, на базе ОС Альт 8 СП Сервер 64 бит (x86_64)), находящегося вне защищенного контура и организация ограниченного доступа к этому серверу.

Модуль ЦУС «Сервер обновлений» (пакет `alterator-mirror`) из раздела «Серверы» предназначен для зеркалирования репозиторий и публикации их для обновлений рабочих станций и серверов.

Сервер обновлений – технология, позволяющая настроить автоматическое обновление ПО, установленного на клиентских машинах (рабочих местах), работающих под управлением ОС Альт СП Рабочая станция.

На странице настройки сервера обновлений ЦУС (рис. 187) можно выбрать, как часто выполнять загрузку пакетов, и указать время начала зеркалирования (рис. 188).

Репозиторий	Источник	Архитектуры	Локальное зеркало	Опубликовано
Репозиторий обновлений для Альт СП 10	update.altsp.su	x86_64 x86_64-i586	<input checked="" type="checkbox"/> (31 Гб)	<input type="checkbox"/>

Свободное место: 114 Гб

Предупреждение: зеркалирование потребует наличия большого количества места на диске.

Отключить зеркалирование
 Зеркалировать ежедневно
 Зеркалировать еженедельно в:
 Зеркалировать ежемесячно в день:

Время:

Рис. 187 – Меню «Сервер обновлений»

Свободное место: 114 Гб

Предупреждение: зеркалирование потребует наличия большого количества места на диске.

Отключить зеркалирование
 Зеркалировать ежедневно
 Зеркалировать еженедельно в:
 Зеркалировать ежемесячно в день:

Время:

Рис. 188 – Настройка расписания

Здесь также можно выбрать репозитории, локальные срезы которых необходимы. При нажатии на название репозитория, появляются настройки этого репозитория (рис. 189). Необходимо выбрать источник (сайт, откуда будет скачиваться репозиторий), архитектуру процессора (если их несколько, то стоит выбрать соответствующие).

Примечание. При выборе любой архитектуры также будет добавлен источник с poarch.

Репозиторий: Репозиторий обновлений для Альт СП 10

Источник:

Архитектуры: aarch64
 i586
 x86_64
 x86_64-i586

Локальное зеркало репозитория
 Опубликовать как репозиторий для автоматических обновлений

Исключить каталоги и файлы (каждый шаблон в отдельной строке)

SRPMS
 RPMS.debuginfo
 -debuginfo-

Рис. 189 – Настройки репозитория

Примечание. Источник `update.altsp.su` не отдает пакеты по `rsync`, если требуется использовать протокол `rsync`, нужно указать другой источник.

Сервер обновлений предоставляет возможность автоматически настроить обновление клиентских машин в нужном режиме:

- локальное зеркало репозитория – в этом режиме на сервере создается копия удаленного репозитория. Загрузка ПО клиентскими машинами может производиться с локального сервера по протоколам HTTP, HTTPS, FTP, `rsync` (для каждого протокола нужно настроить соответствующие службы, ниже приведен пример настройки HTTP- и FTP-сервера). Наличие на локальной машине зеркала репозитория при большом количестве машин в сети позволяет существенно сэкономить трафик.

⚠ Зеркалирование потребует наличия большого количества места на диске.

Уменьшить размер скачиваемых файлов и занимаемое репозиторием место на диске можно, указав имена каталогов и файлов, которые будут исключены из синхронизации. Например, не скачивать пакеты с исходным кодом и пакеты с отладочной информацией:

```
SRPMS
*-debuginfo-*
```

Шаблоны указываются по одному в отдельной строке. Символ «*» используется для подстановки любого количества символов.

- публикация репозитория – в этом случае публикуется или URL внешнего сервера, содержащего репозиторий или, если включено локальное зеркало репозитория, адрес этого сервера обновлений. Такая публикация позволяет клиентским машинам автоматически настроить свои менеджеры пакетов на использование внешнего или локального репозитория. Со стороны клиентских машин, в этом случае, необходимо настроить модуль «Обновление системы», отметив в нем «Обновление системы управляемое сервером».

Настройка локального репозитория заканчивается нажатием на кнопку «Применить».

Примечание. По умолчанию локальное зеркало репозитория находится в `/srv/public/mirror`. Для того чтобы зеркалирование происходило в другую папку, необходимо эту папку примонтировать в папку `/srv/public/mirror`. Для этого в файл `/etc/fstab` следует вписать строку:

```
/media/disk/localrepo /srv/public/mirror none rw,bind,auto 0 0
```

где `/media/disk/localrepo` – папка-хранилище локального репозитория.

Примечание. Если в каталогах `/srv/public/mirror/<репозиторий>/branch/<архитектура>/base/` нет файлов `pkglist.*` значит зеркалирование не закончено (т. е. не все файлы загружены на сервер обновлений).

8.7.4.1. Настройка веб-сервера

Установить веб-сервер `nginx`:

```
# apt-get install nginx
```

Создать файл конфигурации веб-сервера в `/etc/nginx/sites-available.d/repo.conf`:

```
server {
    listen 80;
    server_name localhost .local <ваш ip>;

    access_log /var/log/nginx/repo-access.log;
    error_log /var/log/nginx/repo-error.log;
```

```

location /mirror {
    root /srv/public;
    autoindex on;
}

```

Сделать ссылку в /etc/nginx/sites-enabled.d/:

```
# ln -s /etc/nginx/sites-available.d/repo.conf /etc/nginx/sites-enabled.d/repo.conf
```

Запустить nginx и добавить его в автозагрузку:

```
# systemctl enable --now nginx
```

На клиентских машинах необходимо настроить репозитории. Сделать это можно в программе управления пакетами Synaptic («Параметры» → «Репозитории») или в командной строке:

```
# apt-repo rm all
# apt-repo add http://<ip-сервера>/mirror/c10f2/branch
```

Проверить правильность настройки репозитория, например:

```
# apt-repo
rpm http://192.168.0.185/mirror c10f2/branch/x86_64 classic
rpm http://192.168.0.185/mirror c10f2/branch/noarch classic
```

8.7.4.2. Настройка FTP-сервера

Установить, настроить и запустить сервер FTP:

- установить пакеты vsftpd и lftp:

```
# apt-get install vsftpd lftp
```

Настроить параметры использования vsftpd в файле /etc/xinetd.d/vsftpd:

```
# default: off
# description: The vsftpd FTP server.
service ftp
{
    disable = no # включает службу
    socket_type = stream
    protocol = tcp
    wait = no
    user = root
    nice = 10
    rlimit_as = 200M

```

```
server = /usr/sbin/vsftpd
only_from = 0.0.0.0 # предоставить доступ для всех IP
}
```

Перезапустить xinetd:

```
# systemctl restart xinetd
```

Изменить настройку прав доступа в файле /etc/vsftpd/conf:

```
local_enable=YES
```

Создать каталог /var/ftp/mirror:

```
# mkdir -p /var/ftp/mirror
```

Примонтировать каталог /srv/public/mirror в /var/ftp/mirror с опцией --bind:

```
# mount --bind /srv/public/mirror /var/ftp/mirror
```

Примечание. Для автоматического монтирования каталога /srv/public/mirror при загрузке системы необходимо добавить следующую строку в файл /etc/fstab:

```
/srv/public/mirror /var/ftp/mirror none defaults,bind 0 0
```

На клиентских машинах необходимо настроить репозитории:

```
# apt-repo rm all
# apt-repo add ftp://<ip-сервера>/mirror/c10f2/branch
# apt-repo
rpm ftp://192.168.0.185/mirror c10f2/branch/x86_64 classic
rpm ftp://192.168.0.185/mirror c10f2/branch/noarch classic
```

8.7.5. Локальные учетные записи

Модуль «Локальные учетные записи» (пакет alterator-users) из раздела «Пользователи» предназначен для администрирования системных пользователей.

Для создания новой учетной записи нужно ввести имя новой учетной записи и нажать на кнопку «Создать», после чего имя отобразится в списке слева (рис. 190).

Для дополнительных настроек нужно выделить добавленное имя, либо, если нужно изменить существующую учетную запись, выбрать ее из списка.

⚠ При создании пользователя через ЦУС нужно снимать отметку с пунктов «Входит в группу администраторов» (рис. 190) и «Автоматический вход в систему».

Рис. 190 – Управление локальными пользователями в веб-интерфейсе ЦУС

8.7.6. Администратор системы

В модуле «Администратор системы» (пакет alterator-root) из раздела «Пользователи» можно изменить пароль суперпользователя (root), заданный при начальной настройке системы (рис. 191).

В данном модуле (только в веб-интерфейсе) можно добавить публичную часть ключа RSA или DSA для доступа к серверу по протоколу SSH.

Рис. 191 – Модуль «Администратор системы»

8.7.7. Дата и время

В модуле «Дата и время» (пакет alterator-datetime) из раздела «Система» можно изменить дату и время на сервере, сменить часовой пояс, а также настроить автоматическую синхронизацию часов на самом сервере по протоколу NTP и предоставление точного времени по этому протоколу для рабочих станций локальной сети (рис. 192).

Системное время зависит от следующих факторов:

- часы в BIOS – часы, встроенные в компьютер; они работают, даже если он выключен;
- системное время – часы в ядре ОС. Во время работы системы все процессы пользуются именно этими часами;
- часовые пояса – регионы Земли, в каждом из которых принято единое местное время.

При запуске системы происходит активация системных часов и их синхронизация с аппаратными, кроме того, в определенных случаях учитывается значение часового пояса. При завершении работы системы происходит обратный процесс.

Получать точное время с NTP-сервера: pool.ntp.org
 Работать как NTP-сервер

Текущая дата: **Ноябрь 2024**

Пн	Вт	Ср	Чт	Пт	Сб	Вс
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Текущее время:

2024-11-18 17:58:37

Хранить время в BIOS по Гринвичу
Часовой пояс: Европа/Москва **Изменить...**

Выбрать источник сигналов времени: tsc

Применить **Сбросить**

Рис. 192 – Модуль «Дата и время»

Если настроена синхронизация времени с NTP-сервером, то сервер сможет сам работать как сервер точного времени. Для этого достаточно отметить соответствующий пункт «Работать как NTP-сервер» и нажать на кнопку «Применить» (см. рис. 192).

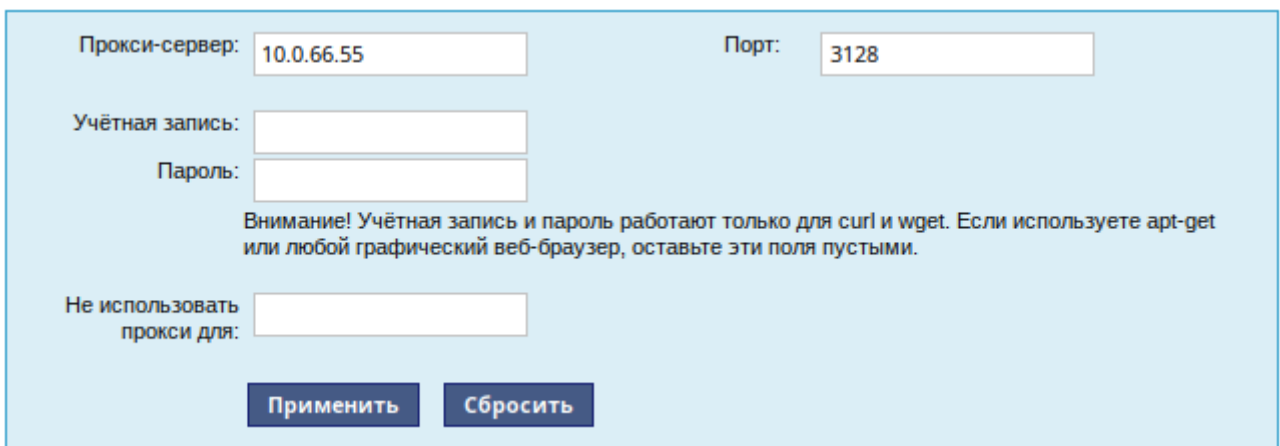
Примечание. Выбор источника сигналов времени (источника тактовой частоты) доступен в режиме эксперта.

8.7.8. Настройка прокси-сервера

Модуль «Прокси-сервер» (пакет `alterator-sysconfig`) в разделе «Сеть» позволяет настроить параметры прокси-сервера, используемого для выхода в Интернет (рис. 193).

Данный модуль позволяет настроить:

- IP-адрес и порт используемого прокси-сервера;
- логин и пароль для доступа, если прокси-сервер требует аутентификацию.



Прокси-сервер: Порт:

Учётная запись:

Пароль:

Внимание! Учётная запись и пароль работают только для curl и wget. Если используете apt-get или любой графический веб-браузер, оставьте эти поля пустыми.

Не использовать прокси для:

Рис. 193 – Веб-интерфейс модуля Прокси-сервер

После нажатия кнопки «Применить» все параметры запишутся в файл `/etc/sysconfig/network` в следующем виде:

```
HTTP_PROXY=http://username:password@address:port
HTTPS_PROXY=http://username:password@address:port
FTP_PROXY=http://username:password@address:port
NO_PROXY=""
```

Указанный прокси-сервер будет использоваться ПО для доступа в сеть Интернет.

Примечание. Для применения настроек прокси-сервера необходимо перезагрузить систему.

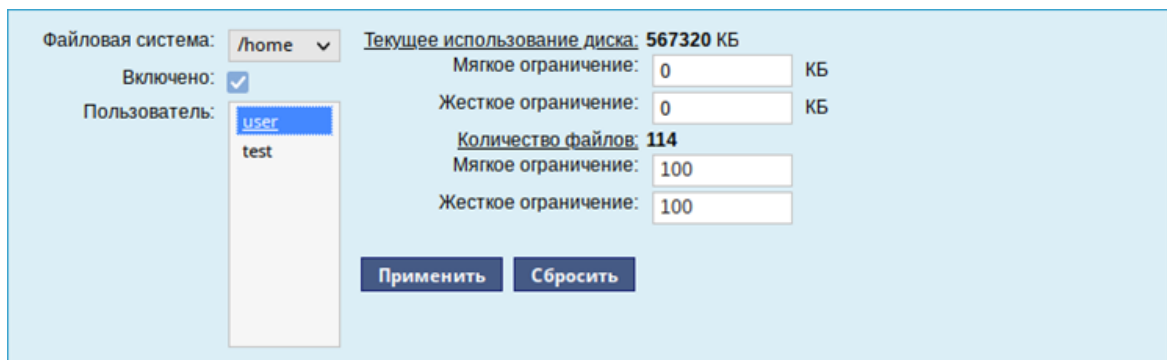
8.7.9. Ограничение использования диска

Модуль «Использование диска» (пакет `alterator-quota`) в разделе «Пользователи» позволяет ограничить использование дискового пространства пользователями, заведенными в системе в модуле «Пользователи».

Модуль позволяет задать ограничения (квоты) для пользователя при использовании определенного раздела диска. Ограничить можно как суммарное количество Кбайт, занятых файлами пользователя, так и количество этих файлов (рис. 194).

Для управления квотами файловая система должна быть подключена с параметрами `usrquota`, `grpquota`. Для этого следует выбрать нужный раздел в списке «Файловая система» и установить отметку в поле «Включено» (рис. 194).

Для того чтобы задать ограничения для пользователя, необходимо выбрать пользователя в списке «Пользователь», установить ограничения и нажать на кнопку «Применить».



Файловая система: /home Включено: Пользователь: user, test

Текущее использование диска: 567320 КБ

Мягкое ограничение: 0 КБ

Жесткое ограничение: 0 КБ

Количество файлов: 114

Мягкое ограничение: 100

Жесткое ограничение: 100

Применить Сбросить

Рис. 194 – Модуль «Использование диска»

При задании ограничений различают жесткие и мягкие ограничения:

- мягкое ограничение: нижняя граница ограничения, которая может быть временно превышена. Временное ограничение – одна неделя;
- жесткое ограничение: использование диска, которое не может быть превышено ни при каких условиях.

Значение 0 при задании ограничений означает отсутствие ограничений.

8.7.10. Выключение и перезагрузка компьютера

Иногда, в целях обслуживания или по организационным причинам необходимо корректно выключить или перезагрузить компьютер. Для этого можно воспользоваться модулем ЦУС «Выключение компьютера» в разделе «Система».

Модуль «Выключение компьютера» позволяет:

- выключить компьютер;
- перезагрузить компьютер;
- приостановить работу компьютера;
- погрузить компьютер в сон.

Возможна настройка ежедневного применения данных действий в заданное время.

Так как выключение и перезагрузка – критичные для функционирования компьютера операции, то по умолчанию настройка выставлена в значение «Продолжить работу». Для выключения, перезагрузки или перехода в энергосберегающие режимы нужно отметить соответствующий пункт и нажать «Применить».

Для ежедневного автоматического выключения компьютера, перезагрузки, а также перехода в энергосберегающие режимы необходимо отметить соответствующий пункт и задать желаемое время (рис. 195). Например, для выключения компьютера следует отметить пункт «Выключать компьютер каждый день в», задать время выключения в поле ввода справа от этого флага и нажать кнопку «Применить».

Продолжить работу
 Выключить компьютер сейчас
 Перезагрузить компьютер сейчас
 Приостановить компьютер сейчас
 Погрузить компьютер в сон сейчас

Выключать компьютер каждый день в: 23:00:00
 Перезагружать компьютер каждый день в: 11:00:00
 Приостанавливать компьютер каждый день в: 23:00:00
 Погружать компьютер в сон каждый день в: 23:00:00

При изменении состояния системы отправлять электронное письмо по адресу:

Рис. 195 – Модуль «Выключение компьютера»

Примечание. Для возможности настройки оповещений на e-mail, должен быть установлен пакет `state-change-notify-postfix`:

```
# apt-get install state-change-notify-postfix
```

Для настройки оповещений необходимо отметить пункт «При изменении состояния системы отправлять электронное письмо по адресу», ввести e-mail адрес и нажать кнопку «Применить».

По указанному адресу, при изменении состояния системы будут приходить электронные письма. Например, при включении компьютера, содержание письма будет следующее:

```
Thu Sep 14 11:46:59 EET 2023: The host-15.test.alt is about to start.
```

При выключении:

```
Thu Sep 14 12:27:02 EET 2023: The host-15.test.alt is about to shutdown.
```

Кнопка «Сбросить» возвращает сделанный выбор к безопасному значению по умолчанию: «Продолжить работу», перечитывает расписания и выставляет отметки для ежедневного автоматического действия в соответствии с прочитанным.

8.7.11. FTP-сервер

Модуль «FTP-сервер» (пакет `alterator-vsftpd`) из раздела «Серверы» (рис. 196) предназначен для настройки FTP-сервера (`vsftpd`).

Чаще всего протокол FTP (File Transfer Protocol) используется для организации файлового сервера с анонимным доступом. Возможность анонимного доступа управляется параметром «Разрешить вход анонимному пользователю». Менее распространенный вариант – сервер с возможностью загружать на него файлы, в том числе и анонимным пользователям. Возможность загрузки включается параметром «Разрешить запись». Еще один вариант – сервер, позволяющий локальным пользователям скачивать и загружать файлы из своих домашних каталогов. Этот вариант используется редко, что связано с небезопасностью протокола FTP. Возможность работы с локальными пользователями управляется

параметром «Разрешить вход локальным пользователям». Чтобы пользователи могли загружать файлы, требуется включить параметр «Разрешить запись».

Разрешение на загрузку файлов можно настраивать индивидуально, для этого нужно отметить параметр «Разрешить настройку локальных пользователей».

The screenshot shows a configuration window for an FTP server. It is divided into three main sections:

- Общие параметры (General parameters):** Contains five checkboxes: 'Включить службу FTP' (checked), 'Разрешить запись' (unchecked), 'Разрешить вход анонимному пользователю' (checked), 'Разрешить вход локальным пользователям' (unchecked), and 'Разрешить настройки для локальных пользователей' (unchecked).
- Параметры записи для анонимного пользователя (Write parameters for anonymous user):** Contains four checkboxes: 'Разрешить создание каталогов' (unchecked), 'Разрешить загрузку файлов' (unchecked), 'Стандартный каталог для приёма файлов (/var/ftp/incoming)' (unchecked), and 'Разрешить переименование/удаление файлов' (unchecked).
- Параметры локальных пользователей (Local user parameters):** Features a table with columns for 'Пользователь' (User) and 'Доступ на запись' (Write access). Below the table are two rows of controls: 'Для выделенных:' (For selected) with a dropdown set to 'разрешить запись' and an 'OK' button; and 'Добавить пользователя:' (Add user) with a dropdown set to 'user' and an 'OK' button.

Buttons 'Применить' (Apply) and 'Сбросить' (Reset) are located between the second and third sections.

Рис. 196 – Настройка модуля «FTP-сервер»

Если нужно создать анонимный FTP-сервер, можно использовать vsftpd в сочетании с пакетом anonftp. В целях безопасности сервер по умолчанию сконфигурирован именно для предоставления анонимного доступа. Запрещены любые команды записи, а также доступ локально зарегистрированных пользователей.

При установке пакета anonftp автоматически создается каталог, который будет корневым при анонимном подключении, – /var/ftp с правами доступа. Владелец этого каталога является пользователь root, а не псевдопользователь, от имени которого работает vsftpd. Это сделано для обеспечения безопасности FTP-сервера и системы в целом. Группой-владельцем каталога является специальная группа ftpadmin, предназначенная для администраторов FTP-сервера.

Многие параметры использования FTP-сервера, в том числе относящиеся к безопасности, могут быть заданы при помощи xinetd (демона Интернет-служб).

В частности, этот сервер позволяет:

- ограничить количество одновременно выполняемых процессов как по системе в целом, так и для каждого отдельного пользователя;
- указать пользователя, от имени которого будет выполняться служба;
- задать приоритет процесса (nice);
- указать адреса, с которых разрешено подключение к данной службе;
- указать время доступа и множество других параметров.

Указать эти настройки можно в модуле «Службы xinetd» (пакет alterator-xinetd) из раздела «Система». Например, установить неограниченный по адресам доступ можно, указав в поле «Только с адресов» значение 0.0.0.0 (рис. 197).

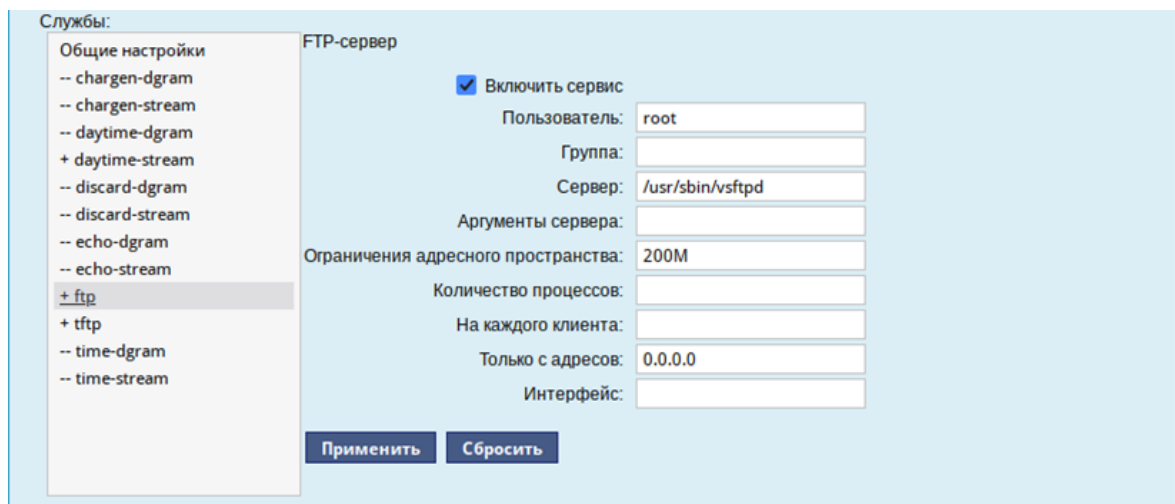


Рис. 197 – Настройка параметров vsftpd в модуле «Службы xinetd»

8.7.12. Удостоверяющий центр

Модуль «Удостоверяющий центр» (пакет alterator-ca) из раздела «Система» позволяет управлять SSL-сертификатами, используемыми для обеспечения безопасных соединений между сетевыми узлами.

Для обеспечения безопасности соединения для клиента (в качестве клиентского ПО может выступать, например, веб-браузер) основным является вопрос о принятии сертификата. При принятии сертификата возможно несколько вариантов.

8.7.12.1. Сертификат сервера подписан одним из известных клиенту удостоверяющих центров (УЦ)

В этом случае сертификат принимается и устанавливается безопасное SSL-соединение. Обычно клиентское ПО (например, веб-браузер) содержит список наиболее известных УЦ и предоставляет возможность управления (добавление/удаление) сертификатами таких УЦ.

8.7.12.2. Сертификат сервера подписан УЦ неизвестным клиенту

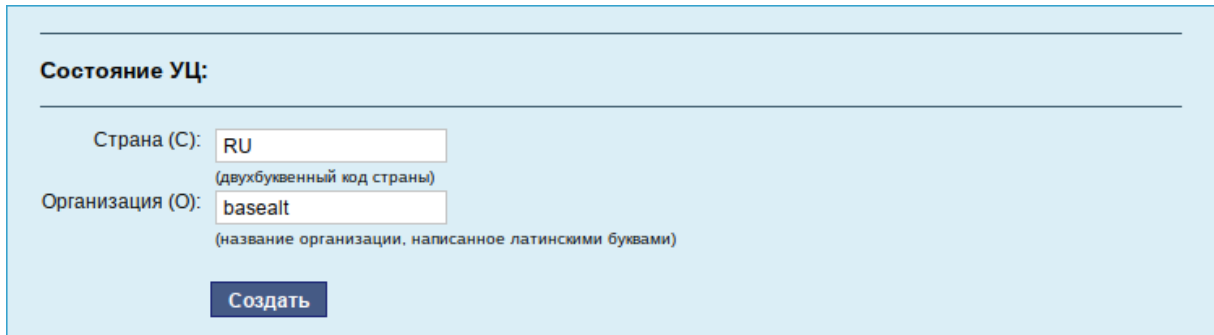
В этом случае следует самостоятельно решить вопрос о принятии такого сертификата:

- можно временно (на время одной сессии) принять сертификат сервера;
- можно принять сертификат сервера на постоянной основе;
- если вы доверяете УЦ, подписавшему сертификат, можно добавить сертификат самого УЦ к списку известных сертификатов, и таким образом, в дальнейшем все сертификаты, подписанные этим УЦ, будут приниматься автоматически.

8.7.12.3. Сертификат сервера является самоподписанным

Это случай, когда сертификат сервера не подтвержден вообще никакой третьей стороной. Такие сертификаты используются в локальных сетях, где вы самостоятельно можете проверить аутентичность сервера. В случае самоподписанных сертификатов вы должны самостоятельно убедиться в том, что сервер является тем, за кого себя выдает. Сделать это можно, сверив отпечатки полученного сертификата и реально находящегося на сервере.

При первом обращении к модулю «Удостоверяющий центр» необходимо создать УЦ, указав страну и организацию (рис. 198).



Состояние УЦ:

Страна (С):
(двухбуквенный код страны)

Организация (О):
(название организации, написанное латинскими буквами)

Рис. 198 – Модуль «Удостоверяющий центр». Создание УЦ

На вкладке «Управление УЦ» (рис. 199) можно:

- просмотреть информацию о сертификате УЦ;
- выгрузить для дальнейшего использования сертификат УЦ (файл `ca-root.pem`). Этот файл можно будет добавить к списку УЦ, используемому клиентским ПО, после чего все сертификаты, подписанные данным УЦ будут приниматься автоматически;
- выгрузить, для дальнейшего использования, запрос на подпись сертификата УЦ (файл `ca-root.csr`). Этот запрос можно подписать сторонним УЦ;
- регенерировать сертификат УЦ с другими параметрами (можно изменить параметры «Страна (С)» и «Организация (О)»).

Управление сертификатами	Управление УЦ
Состояние УЦ: ОК	
Сертификат выдан	
Общее имя (CN): basealt Root Certification Authority	
Подразделение (OU): basealt Certification Authority	
Организация (O): basealt	
Страна (C): RU	
Центр выдачи	
Общее имя (CN): basealt Root Certification Authority	
Подразделение (OU): basealt Certification Authority	
Организация (O): basealt	
Страна (C): RU	
Разное	
Дата выдачи: Nov 18 13:25:22 2024 GMT	
Истекает: Nov 16 13:25:22 2034 GMT	
SHA1-сумма D6:AD:C8:67:E2:66:0A:9F:A4:59:F0:5D:BF:7C:56:02:AA:E5:DE:DE	
MD5-сумма C0:A9:C2:7F:49:75:25:DA:8B:B4:F7:D6:6E:60:92:F5	
Сертификат: ca-root.pem	
Запрос на подпись: ca-root.csr	
<input type="checkbox"/> Регенерировать УЦ	
Страна (C): <input type="text" value="RU"/>	
<small>(двухбуквенный код страны)</small>	
Организация (O): <input type="text" value="basealt"/>	
<small>(название организации, написанное латинскими буквами)</small>	

Рис. 199 – Модуль «Удостоверяющий центр». Вкладка «Управление УЦ»

На вкладке «Управление сертификатами» (рис. 200) можно:

- настроить ежедневное обновление подписей сертификатов, используемых локальными службами и службами подчиненных серверов;
- подписать произвольный сертификат (запрос на подпись) корневым сертификатом УЦ, настроенным на вкладке «Управление УЦ»;
- просмотреть состояния и подпись локальных сертификатов и сертификатов подчиненных серверов (рис. 201).

Управление сертификатами [Управление УЦ](#)

Включить ежедневные обновления в

Подписать сертификат

Управляемые hosts

<input type="checkbox"/>	Хост	▾
<input type="checkbox"/>	Локальные сертификаты	

Для выделенных:

Добавить хост:

Рис. 200 – Модуль «Удостоверяющий центр». Вкладка «Управление сертификатами»

[Вернуться к списку](#)

сертификаты

<input type="checkbox"/>	Имя	Состояние	Дата выдачи	Годен до	Сертификат выдан
<input type="checkbox"/>	ahttpd	self-signed certificate	Nov 13 14:03:06 2024 GMT	Nov 13 14:03:06 2025 GMT	/CN=host-191/O=ahttpd
<input type="checkbox"/>	openvpn-server	OK	Nov 18 13:28:16 2024 GMT	Nov 18 13:28:16 2025 GMT	/C=RU/CN=openvpn-server

Для выделенных:

Рис. 201 – Модуль «Удостоверяющий центр». Локальные сертификаты

Чтобы подписать сертификат, необходимо на вкладке «Управление сертификатами» нажать кнопку «Выберите файл», выбрать файл с запросом на подпись и нажать кнопку «Загрузить запрос». В результате на экране отобразится запрос на подпись. Далее следует нажать кнопку «Подписать». Подписанный сертификат (файл output.pem) будет загружен в каталог загрузок.

8.7.13. Резервное копирование

Резервное копирование является важной частью работ по поддержанию работоспособности сервера и всего домена. Так как сервер является критичной частью сети, производите регулярное резервное копирование. При возникновении

нештатных ситуаций, например, выхода из строя оборудования, восстановить работоспособное состояние сервера можно из резервной копии.

Информацию о резервном копировании при помощи утилиты rsync смотрите в документе «Руководство по комплексу средств защиты. ЛКНВ.11100-01 99 03».

8.8. Сервер электронной почты (SMTP, POP3/IMAP)

8.8.1. Сервер электронной почты

ОС Альт СП Сервер может служить как почтовым сервером, обслуживающим определенный домен, так и посредником (шлюзом) для пересылки почты. Почтовый сервер отвечает как за отправку писем (SMTP-сервер, см. п. 8.9.3) исходящих от почтовых клиентов рабочих станций, так и за предоставление им входящей почты (сервер POP3/IMAP см. п. 8.8.3).

Для настройки параметров работы сервера предусмотрен модуль ЦУС «Почтовый сервер» (пакет alterator-postfix-dovecot) из раздела «Серверы» (рис. 202).

Сервер SMTP

Включить службу SMTP

Программы-клиенты должны использовать STARTTLS

Настройка

Режим работы:

Список доменов:
(Принимать почту для этих доменов)

Псевдоним администратора:
(Почта администратора кладётся в этот ящик)

Максимальный размер сообщения (Мб):
(Максимальный размер сообщения в мегабайтах)

Безопасность

Помечать спам

Фильтровать отправителей
Внутренние сети:

Фильтровать получателей

Проверять антивирусом

Сервер POP3/IMAP

Включить службу POP3/IMAP

Аутентификация SMTP через SASL

Рис. 202 – Настройка параметров работы сервера

8.8.2. Сервер SMTP

Сервер SMTP отвечает за отправку сообщений и может работать в двух режимах:

- 1) посредник – в этом режиме исходящая почта пересылается для дальнейшей отправки на указанный сервер;
- 2) сервер – в этом режиме сервер доставляет почту самостоятельно.

8.8.3. Сервер POP3/IMAP

Сервер POP3/IMAP используется для доступа пользователей к электронной почте на сервере.

Для доступа к службам POP3 и IMAP пользователь должен включить в своем почтовом клиенте аутентификацию и указать свое имя и пароль.

Выбор конкретного используемого протокола для получения почты зависит от предпочтений пользователя:

- 1) POP – при проверке почты клиентом она передается на его машину и сохраняется там. Возможность просмотра принятой/отправленной почты при этом существует, даже если клиент не имеет соединения с сервером;
- 2) IMAP – все сообщения хранятся на сервере. Почтовый клиент может просматривать их только при наличии соединения с сервером.

Помимо включения/отключения служб, модуль ЦУС «Почтовый сервер» позволяет произвести дополнительные настройки: фильтрацию спама, настройку параметров аутентификации и т. д.

8.9. Сервер электронной почты postfix

Postfix представляет собой агент передачи электронной почты и позволяет организовать обмен почтой внутри локальной сети, а также с внешней сетью.

Для расширения возможностей postfix используется ряд дополнений, выделенных в отдельные пакеты, полный список которых можно получить с помощью следующей команды:

```
$ apt-cache search ^postfix-
```

Настройка сервера электронной почты postfix осуществляется с помощью конфигурационных файлов, хранящихся в каталоге `/etc/postfix`. Основные параметры определяются в файле конфигурации `main.cf`. В файле `main.cf` указываются только параметры, выставленные администратором, и некоторые из значений по умолчанию, которые администратору с большой вероятностью нужно будет изменить. Значения по умолчанию для всех остальных параметров перечислены в файле `main.cf.default` (этот файл не следует редактировать, он служит только для справок).

Если конфигурация была изменена при запущенной службе postfix, новые настройки нужно активизировать командой: `# service postfix reload`

Postfix сохраняет все сообщения в журнале `mail.log`, расположенном в каталоге `/var/log/`. Сообщения об ошибках и предупреждения сохраняются отдельно в журналы `mail.err` и `mail.warn` соответственно.

Запуск postfix осуществляется с помощью следующей команды:

```
# postfix start
```

8.9.1. Утилиты командной строки

Postfix поставляется с набором утилит командной строки, которые помогают решать административные задачи. Они выполняют разнообразные функции (обращение к картам, просмотр файлов очередей, постановка сообщений в очередь и извлечение из очереди, изменение конфигурации).

Команда `postfix` останавливает, запускает и перезагружает конфигурацию с помощью параметров `stop`, `start` и `reload`.

Команда `postalias` создает индексированную карту псевдонимов из файла псевдонимов и работает аналогично команде `postmap`, при этом уделяя особое внимание нотации в файле псевдонимов (ключ и значение разделяются двоеточием).

Команда `postcat` выводит содержимое сообщения, находящегося в почтовой очереди. Для того чтобы прочитать сообщение, находящееся в очереди, нужно знать идентификатор очереди. Для получения списка идентификаторов очередей следует выполнить следующую команду: `# mailq`

После получения идентификатора очереди нужно указать его в качестве параметра команды `postcat` для просмотра содержимого файла следующим образом:

```
# postcat -q <идентификатор очереди>
```

Основная задача команды `postmap` заключается в построении индексированных карт на основе обычных текстовых файлов.

Для того чтобы создать карту `/etc/postfix/virtual.db` на основе `/etc/postfix/virtual`, нужно выполнить следующую команду:

```
# postmap hash:/etc/postfix/virtual
```

Также команда `postmap` обеспечивает возможность тестирования карт любого вида, поддерживаемых конфигурацией `postfix`.

Команда `postdrop` считывает почту из стандартного ввода и записывает результат в каталог `maildrop` (программа работает в связке с утилитой `sendmail`).

Команда `postkick` отправляет запрос демону `postfix` по локальному транспортному каналу, делая межпроцессное взаимодействие `postfix` доступным для сценариев оболочки и других программ.

Команда `postlock` предоставляет монопольный доступ к файлам `mbox`, в которые выполняет запись `postfix`, а затем исполняет команду, удерживая блокировку.

Команда `postlog` позволяет внешним программам, таким как сценарии командного интерпретатора, писать сообщения в журнал электронной почты (представляет собой `postfix`-совместимый интерфейс регистрации).

Команда `postqueue` представляет собой пользовательский интерфейс для очередей `postfix`, предоставляющий возможности, обычно доступные в рамках выполнения команды `sendmail`.

Команда `postqueue` с параметром `-f` просит диспетчер очередей доставить всю стоящую в очереди почту вне зависимости от места назначения:

```
# postqueue -f
```

Команда `postqueue` с параметром `-p` выводит содержимое очереди:

```
# postqueue -p
```


Команда `postqueue` с параметром `-s domain` пытается доставить всю стоящую в очереди почту для домена `domain`:

```
# postqueue -s example.com
```

Команда `postsuper` обслуживает задания внутри очередей postfix (в отличие от `postqueue`, эта команда доступна только пользователю с идентификатором `root`, и она может быть выполнена, когда сервер не запущен).

8.9.2. Первичная настройка

В первую очередь после установки postfix нужно настроить параметры, отвечающие за домен и имя сервера. Чтобы установить значение параметра `myhostname`, нужно отредактировать конфигурационный файл `main.cf`. (для параметра `myhostname` нужно ввести полностью определенное доменное имя хоста):

```
myhostname = mail.example.com
```

Postfix может автоматически получить значение `mydomain` после того, как параметр `myhostname` настроен, для этого postfix отбрасывает первую часть значения `myhostname` до первой точки включительно:

```
mydomain = example.com
```

Далее нужно указать домен, с которого отправляется локальная почта. Postfix будет добавлять значение из `mydomain` к любому адресу, если он задан не полностью. Для этого нужно в конфигурационном файле `main.cf` для параметра `myorigin` установить следующее значение:

```
myorigin = $mydomain
```

Примечание. Сообщение от процесса `stop` пользователю `root` получит адрес `root@$mydomain`, которое будет преобразовано в `root@example.com`.

Далее нужно указать домены, для которых данный сервер является конечной точкой доставки электронной почты. Для того чтобы postfix принимал любую почту, адресованную в домен `example.com` нужно в файл конфигурации внести следующие изменения:

```
mydestination = $mydomain
```

Домены, для которых сервер получает почту, отличные от значения `mydomain` и не сконфигурированные как виртуальные домены `postfix`, нужно перечислить с помощью параметра `mydestination` либо в дополнительном файле, на который ссылается этот параметр.

Адресаты указываются через запятую следующим образом:

```
mydestination =  
$mydomain,  
$myhostname
```

Аналогичным образом параметр `mynetworks` описывает блоки IP-адресов, которые считаются внутренними и с которых разрешен прием исходящих сообщений.

После внесения изменений в конфигурацию `postfix` для применения новых настроек нужно перезапустить службу `postfix`:

```
# service postfix reload
```

8.9.3. Работа в режиме SMTP-сервера

После установки служба `postfix` функционирует в режиме `local`, в котором сервер электронной почты `postfix` не принимает соединения из внешней сети, ограничиваясь приемом локальных соединений посредством сокетов семейства UNIX (UNIX-domain socket).

Для настройки возможности приема сообщений по протоколу SMTP или ESMTP, как из внешней сети, так из внутренней, нужно переключить службу `postfix` в режим работы `server` с помощью следующей команды:

```
control postfix server
```

Рабочие станции в локальной сети или машины в сети провайдера, отделенной от внешней сети, должны перенаправлять исходящую почту на почтовый сервер, обслуживающий данную сеть.

Для того чтобы `postfix` отправлял почту из локальной сети на SMTP-сервер провайдера, нужно для параметра `relayhost` установить следующее значение:

```
relayhost = [smtp.provider.net]
```

8.9.4. SMTP-аутентификация

SMTP-аутентификация обеспечивает идентификацию клиентов независимо от их IP-адресов и позволяет серверу пересылать сообщения от почтовых клиентов, чьи IP-адреса не входят в список доверенных. Postfix реализует SMTP-аутентификацию при помощи протокола SASL (Simple Authentication and Security Layer) и использует библиотеки Cyrus-SASL.

Для защиты соединений используется протокол SSL/TLS (для включения поддержки нужно установить пакет postfix-tls).

Для проверки поддержки SMTP-аутентификации postfix нужно от имени администратора (root) выполнить следующую команду:

```
ldd `postconf h daemon_directory`/smtpd
```

Если в выводе команды присутствует строка `libsasl.so.2`, значит, пакет postfix был собран с поддержкой SASL.

8.9.4.1. Настройки SMTP-аутентификации на сервере

Настройка SMTP-аутентификации на сервере осуществляется в несколько этапов:

- 1) включение SMTP-аутентификации на серверной части;
- 2) настройка механизмов SASL, которые будут предоставляться клиентам;
- 3) настройка поддержки SMTP-аутентификации для нестандартных почтовых клиентов;
- 4) настройка области (realm), которую postfix будет передавать библиотеке SASL;
- 5) определение разрешения на пересылку в postfix.

Чтобы включить SMTP-аутентификацию, нужно в конфигурационный файл `main.cf` добавить следующую запись:

```
smtpd_sasl_auth_enable = yes
```

8.9.4.1.1. Настройка механизмов SASL

Управление предоставляемыми механизмами осуществляется с помощью параметра `smtpd_sasl_security_options`, в котором через запятые следует указать список из одного или более значений:

- 1) `noanonymous` – значение параметра, позволяющее включить проверку сервером верительных данных клиента (список значений параметра `smtpd_sasl_security_options` всегда должен включать в себя значение `noanonymous`);
- 2) `noplaintext` – значение параметра, позволяющее исключить использование всех механизмов открытого текста, таких как PLAIN и LOGIN (значение, рекомендуемое для использования, так как отправляемые открытым текстом верительные данные могут быть легко перехвачены в сети);
- 3) `noactive` – значение параметра, исключающее использование механизмов SASL, которые восприимчивы к активным атакам);
- 4) `nodictionary` – значение параметра, исключающее все механизмы, не устойчивые к атакам по словарю (атаки, осуществляемые методом полного перебора паролей);
- 5) `mutual_auth` – значение параметра, позволяющее включить поддержку только механизмов, обеспечивающих взаимную аутентификацию (сервер аутентифицирует себя для клиента).

8.9.4.1.2. Настройка SMTP-аутентификации для нестандартных почтовых клиентов

Для настройки альтернативной нотации для устаревших клиентов, не распознающих SMTP-аутентификацию по стандарту RFC 2222, но распознающих более раннюю нотацию, использованную в черновом варианте этого стандарта (где между командой AUTH и названиями механизмов стоял не пробел, а знак равенства), нужно в конфигурационном файле `main.cf` установить параметр `broken_sasl_auth_clients`:

```
broken_sasl_auth_clients = yes
```

8.9.4.1.3. Настройка области SASL

Для аутентификации клиента сервер postfix отправляет службе паролей Cyrus SASL область аутентификации (realm) вместе с верительными данными клиента. Такая необходимость определяется версией Cyrus SASL и выбором службы. Для указания области аутентификации в файле `main.cf` используется параметр `smtpd_sasl_local_domain`. По умолчанию этот параметр пуст и должен оставаться пустым, если только не используется вспомогательный плагин, которому действительно требуется область аутентификации.

8.9.4.1.4. Настройка разрешений на пересылку

Для разрешения пересылки для клиентов, прошедших аутентификацию SASL, нужно добавить параметр `permit_sasl_authenticated` в список ограничений `smtpd_recipient_restrictions` своей конфигурации следующим образом:

```
smtpd_recipient_restrictions =  
[...]  
permit_sasl_authenticated,  
permit_mynetworks,  
reject_unauth_destination  
[...]
```

Нужно поместить ключевое слово `permit_sasl_authenticated` достаточно близко к началу списка ограничений, чтобы аутентифицированный клиент не был случайно отвергнут из-за несоответствия какому-то другому правилу (например, `reject_unauth_destination`).

8.9.4.2. Настройка SMTP-аутентификации на стороне клиента

Для настройки SMTP-аутентификации для клиента нужно выполнить следующее:

- 1) запросить у удаленного сервера список поддерживаемых механизмов аутентификации;
- 2) включить SMTP-аутентификацию на клиентской части;
- 3) предоставить файл для хранения верительных данных;
- 4) настроить postfix на работу с файлом верительных данных;
- 5) отключить ненадежные механизмы аутентификации.

Клиентская ПЭВМ должна поддерживать механизмы аутентификации, поддерживаемые сервером. Для получения списка механизмов аутентификации нужно подключиться к почтовому серверу и отправить приветствие EHLO с помощью следующих команд:

```
$ telnet mail.remoteexample.com 25
EHLO mail.example.com
```

По умолчанию SMTP-аутентификация на стороне клиента выключена. Для того чтобы включить SMTP-аутентификацию нужно в конфигурационный файл `main.cf` добавить следующую запись:

```
smtp_sasl_auth_enable = yes
```

После включения аутентификации на клиентской ПЭВМ нужно сообщить серверу postfix, где следует искать данные, которые нужны для аутентификации, и какой из механизмов (из предлагаемых удаленным сервером) postfix может использовать.

8.9.4.2.1. Хранение верительных данных

Нужно подготовить данные, которые клиент postfix будет использовать для того, чтобы аутентифицировать себя на сервере, для этого следует создать от имени root файл карты `/etc/postfix/sasl_passwd` (если он еще не существует) с помощью следующей команды:

```
# touch /etc/postfix/sasl_passwd
```

Далее нужно отредактировать этот файл, поместив полностью определенное доменное имя почтового сервера, который требует аутентификации, с левой стороны, а разделенную двоеточием пару «имя пользователя – пароль» – с правой. Для имен пользователей `mail.example.com` и `relay.another.example.com`, а также соответствующих паролей файл `sasl_passwd` будет выглядеть следующим образом:

```
mail.example.com test:testpass
relay.another.example.com username:password
```

После редактирования файла `sasl_passwd` нужно изменить права на него так, чтобы читать его мог только пользователь root (в файле хранится конфиденциальная

информация, которая не должна быть доступна локальным пользователям), для этого нужно использовать команды `chown` и `chmod`:

```
# chown root:root /etc/postfix/sasl_passwd && chmod 600  
/etc/postfix/sasl_passwd
```

Затем нужно преобразовать файл карты в индексированную карту для быстрого доступа postfix (нужно выполнять при каждом изменении файла `sasl_passwd`) с помощью следующей команды:

```
# postmap hash:/etc/postfix/sasl_passwd
```

8.9.4.2.2. Настройка postfix для использования верительных данных

Нужно сообщить клиенту postfix, где хранится созданная карта верительных данных аутентификации, для этого нужно в параметре `smtp_sasl_password_maps` в файле `main.cf` указать полный путь к файлу `sasl_passwd`, указывая при этом (с помощью спецификатора `hash:`), что значения карты хранятся в хеш-файле, например:

```
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
```

8.9.4.2.3. Отключение некоторых механизмов аутентификации

Для отключения использования ненадежных механизмов следует указать в параметре `smtp_sasl_security_options` список (через запятую) типов механизмов, которые клиент не может использовать. По умолчанию параметр `smtp_sasl_security_options` установлен в значение «noanonymous», но по возможности (если сервер поддерживает механизм с шифрованием, такой как DIGEST-MD5 или CRAM-MD5) следует также отключить использование механизмов открытого текста. Для этого нужно добавить в файл `main.cf` следующую строку:

```
smtp_sasl_security_options = noanonymous, noplaintext
```

8.9.5. Триггеры ограничений

Ограничения позволяют почтовому серверу принять или отвергнуть сообщения на основе данных SMTP-соединения между клиентом и сервером. Информация, полученная из этого диалога, позволяет postfix наложить или отменить ограничения на клиента (отправителя и получателя).

Postfix поддерживает следующие триггеры:

- 1) `smtpd_client_restrictions` – триггер применяется к IP-адресу или имени хоста клиента либо к ним обоим (по умолчанию postfix разрешает подключение любому клиенту);
- 2) `smtpd_helo_restrictions` – триггер применяется к аргументу HELO/EHLO клиента и к IP-адресу и (или) имени хоста клиента (по умолчанию допускается любой аргумент HELO/EHLO);
- 3) `smtpd_sender_restrictions` – набор триггеров, который относится к частям конверта (Postfix применяет его к отправителю конверта, аргументу HELO/EHLO и клиенту, по умолчанию любому отправителю конверта разрешено отправлять сообщения);
- 4) `smtpd_recipient_restrictions` – триггер применяется к получателям конверта, отправителю конверта, аргументу HELO/EHLO и к IP-адресу и (или) имени хоста клиента (по умолчанию postfix допускает любых получателей для клиентов, которые определены в параметре конфигурации `mynet_works`, для остальных же разрешены получатели в доменах из `relay_domains` и `mydomains`);
- 5) `smtpd_data_restrictions` – триггер выявляет клиентов, которые отправляют содержимое письма прежде, чем postfix ответит на команду DATA (Postfix выполняет это посредством трассировки DATA, когда клиент отправляет команду на сервер, по умолчанию ограничения нет);
- 6) `smtpd_etrn_restrictions` – специальный триггер может ограничить клиенты, которые могут запрашивать у postfix очистку очереди сообщений (по умолчанию всем клиентам разрешено выдавать команду ETRN).

В postfix существуют несколько видов ограничений, которые можно разбить на четыре группы:

- 1) общие ограничения;
- 2) переключаемые ограничения;
- 3) настраиваемые ограничения;
- 4) дополнительные параметры контроля спама.

Общие ограничения выполняют следующие команды:

- 1) `permit` – разрешает запрос;
- 2) `defer` – откладывает запрос;
- 3) `reject` – отвергает запрос;
- 4) `warn_if_reject` – содействует последующим ограничениям (если ограничение после `warn_if_reject` решает отвергнуть запрос, то `postfix` записывает в журнал сообщение `reject_warning`);
- 5) `reject_unauth_pipelining` – отвергает запрос, когда клиент отправляет команды SMTP раньше времени, еще не зная о том, действительно ли `postfix` поддерживает конвейерную обработку команд ESMTP (таким образом, достигается противодействие программам массовой рассылки, которые некорректно используют конвейерную обработку команд ESMTP для ускорения доставки).

Переключаемые ограничения работают как переключатели, при активации которых они проверяют выполнение некоторого условия. К переключаемым ограничениям относятся следующие:

- 1) `smtpd_helo_required` – ограничение, требующее от клиентов отправки команды HELO (или EHLO) в начале сеанса SMTP (наличия команды HELO/EHLO требуют RFC 821 и RFC 2821);
- 2) `strict_rfc821_envelopes` – ограничение, регулирующее степень терпимости postfix к ошибкам в адресах, указанных в команде MAIL FROM (отправитель конверта) или RCPT TO;
- 3) `disable_vrfy_command` – SMTP-команда VRFY позволяет клиентам проверять существование получателя (ограничение позволяет отменить команды VRFY);
- 4) `allow_percent_hack` – ограничение, регулирующее преобразование из формы «user%domain» в «user@domain»;
- 5) `swap_bangpath` – ограничение, контролирующее преобразование из формы «site!user» в «user@site» (нужно, если ПЭВМ подключена к сети UUCP).

Настраиваемые ограничения представляют собой карты, которые работают как фильтры. В каждой записи карты ключ является фильтром, а значение – тем действием, которое нужно выполнить при совпадении:

- 1) HELO (EHLO) имя хоста – ограничения, относящиеся к именам хостов, которые клиенты могут отправлять с командой HELO или EHLO;
- 2) имя хоста/адрес клиента – ограничения, определяющие клиенты, которые могут устанавливать SMTP-соединения с почтовым сервером;
- 3) адрес отправителя – ограничения, определяющие адреса отправителей (конвертов), которые postfix разрешает для использования в командах MAIL FROM;
- 4) адрес получателя – ограничения, определяющие адреса получателей (конвертов), которые postfix разрешает для использования в командах RCPT TO;
- 5) ETRN-команды – ограничение, накладываемое на клиентов, которые могут выдавать команды ETRN;
- 6) проверка заголовка – ограничение, регулирующее заголовки сообщений;
- 7) проверка тела – ограничения, накладываемые на содержимое, которое может появляться в теле сообщения;
- 8) черные списки DNSBL – черные списки, ограничивающие соединения от IP-адресов (клиентов), которые включены в черные списки DNSBL;
- 9) черные списки RHSBL – черные списки, запрещающие те домены отправителей (конверта), которые присутствуют в черных списках RHSBL.

Дополнительные параметры контроля спама поддерживают другие ограничения или возможности, не входящие в функциональность postfix по умолчанию:

- 1) `default_rbl_reply` – создает шаблон ответа по умолчанию, который будет использоваться при блокировании запроса SMTP-клиента ограничением `reject_rbl_client` или `reject_rhsbl_sender`;
- 2) `permit_mx_backup_networks` – ограничивает использование функции контроля за пересылкой `permit_mx_backup` теми адресатами, у которых основные хосты MX входят в указанный список сетей;

- 3) `rbl_reply_maps` – определяет таблицы поиска и шаблоны ответов DNSBL, индексированные по имени домена DNSBL;
- 4) `relay_domains` – указывает postfix на необходимость приема почты для этих доменов несмотря на то, что данный сервер не является местом их конечного назначения;
- 5) `smtpd_sender_login_maps` – определяет пользователя, которому разрешено использовать определенный адрес MAIL FROM.

В postfix по умолчанию встроен набор ограничений. Для того чтобы посмотреть список ограничений нужно выполнить следующую команду:

```
# postconf -d smtpd_recipient_restrictions
```

Для включения режима фильтрации почты в postfix в зависимости от наличия в них нежелательной информации (спам) нужно выполнить следующую команду:

```
control postfix filter
```

8.9.6. Алиасы и преобразование адресов

В postfix для передачи сообщений электронной почты используются алиасы, которые позволяют создавать псевдонимы для длинных или плохо запоминаемых адресов электронной почты. Настройка алиасов в postfix осуществляется с помощью таблиц `aliases`.

При установке postfix в таблице создается алиас на имя пользователя `root`: вся корреспонденция, предназначенная администратору и поступающая на другие системные адреса, будет отправляться на имя реального пользователя, который осуществляет функции администратора.

Рабочий образ таблицы строится с помощью следующей команды:

```
newaliases
```

а также при актуализации всех изменений посредством следующей команды:

```
service postfix reload
```

При отправке сообщения postfix формирует адрес отправителя автоматически из имени учетной записи пользователя и значения собственного домена (или значения «`myorigin`»). Преобразование адресов отправителей в глобальные адреса задаются в таблице типа `canonical`:

```
sender_canonical_maps = cdb:/etc/postfix/sender_canonical
```

Аналогичная таблица `recipient_canonical` и соответствующий параметр `recipient_canonical_maps` могут быть использованы для преобразования адресов назначения.

8.9.7. Настройка ограничений размера почтового ящика и отправляемого сообщения

По умолчанию размер файла почтового ящика при локальной доставке ограничен 51 200 000 байтами. Это ограничение можно изменить с помощью параметра `mailbox_size_limit`.

Например, снять ограничение можно установив этот параметр в 0:

```
mailbox_size_limit = 0
```

Также можно установить требуемый размер, указав в значении параметра величину:

```
mailbox_size_limit = <размер почтового ящика в байтах>
```

Для настройки размера отправляемого сообщения используется параметр `message_size_limit`:

```
message_size_limit = <размер сообщения в байтах>
```

Для настройки виртуальных аккаунтов используется параметр `virtual_mailbox_limit`:

```
virtual_mailbox_limit= <размер почтового ящика виртуального аккаунта в байтах>
```

8.10. Настройка удаленного подключения

Для получения удаленного доступа к другим ПЭВМ и предоставления такого доступа в ОС Альт СП используется протокол SSH (Secure Shell).

SSH реализует соединение с удаленным компьютером, защищающее от следующих угроз:

- прослушивание данных, передаваемых по этому соединению;
- манипулирование данными на пути от клиента к серверу;
- подмена клиента, либо сервера, путем манипулирования IP-адресами, DNS, либо маршрутизацией.

SSH обладает следующими возможностями:

- сжатие передаваемых данных;
- туннелирование каналов внутри установленного соединения – в том числе соединений с X-сервером;
- широкая распространенность: существуют реализации SSH для самых различных аппаратных платформ и ОС.

OpenSSH – реализация SSH, входящая в состав дистрибутива. Эта реализация включает в себя следующие программы и утилиты:

- клиентские программы `ssh`, `scp` и `sftp` (используются для запуска программ на удаленных серверах и копирования файлов по сети);
- серверные программы `sshd`, `sftp-server` (используются для предоставления доступа по протоколу SSH);
- вспомогательные программы `scp`, `rescp`, `ssh-keygen`, `ssh-add`, `ssh-agent`, `ssh-copy-id`, `ssh-keyscan`.

8.10.1. OpenSSH, сервер протокола SSH (sshd)

OpenSSH Daemon (`sshd`) – программа-сервер, обслуживающая запросы программы-клиента `ssh`. Вместе эти программы заменяют `rlogin` и `rsh` и обеспечивают защищенную и кодированную связь между двумя непроверенными компьютерами через незащищенную сеть.

`sshd` – это служба, принимающая запросы на соединения от клиентов. Для каждого нового соединения создается (с помощью вызова «fork») новый экземпляр службы. Ответвленный экземпляр обрабатывает обмен ключами, кодирование, аутентификацию, выполнение команд и обмен данными.

Параметры определяются при помощи ключей командной строки или файла конфигурации (по умолчанию – `sshd_config`). Ключи командной строки имеют больший приоритет, чем значения, указанные в файле конфигурации. При получении сигнала отбоя `SIGHUP` перечитывает свой файл конфигурации путем запуска собственной копии с тем же самым именем, с которым был запущен, например, `/usr/sbin/sshd`.

Синтаксис команды:

```
sshd [-4Ddeigt] [-b длина ключа_1] [-f файл конфигурации] [-g
время_задержки_регистрации] [-h файл_ключа_хоста] [-k
частота_генерации_ключа] [-o директива] [-p порт] [-u длина]
```

Доступны ключи, приведенные в таблице 10.

Т а б л и ц а 10 – Ключи команды sshd

Ключ	Описание
-4	Использовать только адреса IPv4
-6	Использовать только адреса IPv6
-b длина_ключа_1	Определяет число битов в ключе сервера протокола версии 1 (по умолчанию 1024)
-D	Не переходить в фоновый режим и не становиться службой. Это упрощает слежение за экземпляром sshd
-d	Режим отладки. Сервер посылает расширенную отладочную информацию в файл журнала событий системы и не переходит в фоновый режим работы. Сервер не создает дочерних процессов и обрабатывает только одно соединение. Параметр предназначен только для отладки работы сервера. Несколько параметров -d указанных один за другим, повышают уровень отладки. Максимум – это 3
-e	Направлять вывод в консоль (stderr) вместо механизма журналирования событий системы
-f файл_конфигурации	Определяет имя файла конфигурации (по умолчанию – /etc/openssh/sshd_config). Не работает, если нет файла конфигурации
-g время_задержки_регистрации	Определяет период, в течение которого клиент должен себя идентифицировать (по умолчанию – 120 секунд). Если клиент не смог идентифицировать себя в течение этого времени, экземпляр сервера прекращает свою работу. Значение равное нулю отменяет ограничение на время ожидания
-h файл_ключа_хоста	Определяет файл, из которого будет считан ключ хоста. Этот параметр должен быть указан, если запущен не от имени пользователя с идентификатором root (так как обычно стандартные файлы хоста доступны для чтения только пользователю с идентификатором root). Стандартное расположение файла – /etc/openssh/ssh_host_key для протокола версии 1, и /etc/openssh/ssh_host_dsa_key, /etc/openssh/ssh_host_ecdsa_key и /etc/openssh/ssh_host_rsa_key для протокола версии 2. Можно иметь несколько ключей хоста для разных версий протокола и алгоритмов генерации ключей

Окончание таблицы 10

Ключ	Описание
-i	Позволяет уведомить программу о том, что она запускается службой inetd. Обычно sshd не запускается из inetd, так как требуется генерировать ключ сервера до ответа клиенту, а это может отнять десятки секунд. Клиент будет вынужден ожидать слишком долго, если ключ будет повторно генерироваться каждый раз. Однако, при малых размерах ключа (например, 512), использование из inetd может быть оправдано
-k частота_генерации_ключа	Определяет, как часто будет регенерироваться ключ сервера протокола версии 1 (по умолчанию 3600 секунд – один раз в час). Значение ноль означает, что ключ никогда не будет регенерирован
-o директива	Позволяет указывать директивы в формате файла конфигурации, например, такие, для которых нет соответствующего ключа командной строки. Директивы файла конфигурации описаны в <code>sshd_config</code>
-p порт	Порт, на котором сервер будет ожидать соединения (по умолчанию – 22). Возможно указание нескольких ключей с разными портами. Если данный ключ указан, параметр Port файла конфигурации игнорируется, однако порты, указанные в ListenAddress имеют больший приоритет, чем указанные в командной строке
-q	Не заносить в системный журнал регистрации событий никакой информации. В обычном режиме в нем фиксируется подключение, аутентификация и разрыв каждого соединения.
-t	Режим тестирования. Выполняется только проверка соответствия файла конфигурации и готовность ключей. Полезно для проверки состояния службы после обновления, при котором были изменены файлы конфигурации
-u длина	Размер поля в структуре utmp хранящей имя удаленного хоста. Если разрешенное имя хоста превышает указанное значение, то взамен будет использован десятичное представление IP-адреса через точку. Это позволяет уникально идентифицировать машины со слишком длинными именами. Указание -u0 включает использование в файле utmp IP-адресов во всех случаях. При этом будет производиться DNS-запросы только если это явно требуется конфигурацией (from="pattern-list") или механизмом аутентификации (либо RhostsRSAAuthentication либо HostbasedAuthentication). Использование DNS также обязательно в случае задания параметрам AllowUsers и DenyUsers значения в формате USER@HOST

8.10.1.1. Аутентификация

Служба OpenSSH SSH поддерживает версии протокола SSH 1 и 2. При этом использование протокола версии 1 крайне не рекомендуется. Запретить использование протокола версии 1 можно, указав в файле конфигурации `/etc/openssh/sshd_config` параметр `Protocol`:

```
Protocol 2
```

Протокол 2 поддерживает ключи DSA, ECDSA и RSA; протокол 1 поддерживает только ключи RSA. Независимо от протокола, каждый подключающийся хост имеет собственный, обычно 2048-битный идентифицирующий его ключ.

Для протокола версии 1 подтверждение субъекта сервера обеспечивается 768-битным ключом, который генерируется при запуске сервера. Ключ генерируется заново каждый час, при условии его использования, и не хранится на диске. При получении запроса на подключение со стороны клиента служба посылает в ответ свой открытый ключ и свои ключи. Клиент сравнивает ключ хоста RSA со своими данными, чтобы убедиться в том, что это тот же сервер. Затем клиент генерирует 256-битное произвольное число, шифрует его при помощи обеих ключей (своего и сервера) и отправляет результат серверу. Это число становится ключом сеанса, и с его помощью выполняется кодирование всех последующих данных, по согласованному методу – Blowfish или 3DES (клиент выбирает метод из предложенных сервером). В настоящее время по умолчанию используется 3DES.

Для протокола версии 2 подтверждение субъекта сервера обеспечивается по схеме Диффи-Хеллмана, в результате которой также получается общий ключ сеанса. Дальнейший обмен данными шифруется симметричным кодом, 128-битным AES, Blowfish, 3DES, CAST128, Arcfour, 192-битным AES или 256-битным AES, который выбирает клиент из предложенных сервером. Кроме того, целостность передаваемых данных обеспечивается кодом подтверждения подлинности сообщения (hmac-md5, hmac-sha1, умас-64, hmac-ripemd160, hmac-sha2-256 или hmac-sha2-512).

Далее, сервер и клиент переходят в режим аутентификации. Клиент пытается аутентифицировать себя по своему хосту, открытому ключу, паролю или с помощью беспарольного механизма («вызов-ответ»).

Независимо от типа аутентификации служба проверяет доступность соответствующей учетной записи в системе. Так, она может быть заблокирована посредством добавления ее в параметр `DenyUsers` или ее группы в `DenyGroups`. Для запрета только аутентификации по паролю укажите в файле `passwd` 'NP' или '*NP*'.

После успешной аутентификации себя клиентом связь переходит в режим подготовки сеанса. В этот момент клиент может запросить такие вещи, как выделение псевдо-терминала, перенаправление соединения X11, перенаправление соединения TSP/IP или перенаправление соединения агента аутентификации через защищенный канал.

Наконец, клиент запрашивает оболочку или выполнение команды, после чего стороны входят в режим сеанса. В этом режиме, каждая из сторон в любой момент может пересылать данные и эти данные будут переданы оболочке или команде на стороне сервера и на пользовательский терминал соответственно.

По завершении работы пользовательской программы и закрытии всех перенаправленных X11 и других соединений сервер посылает клиенту команду со статусом выхода и сеанс завершается.

8.10.1.2. Вход в систему

После успешной аутентификации пользователя выполняются следующие действия:

- если регистрация в системе произведена на терминале (tty) и не указана никакая команда, то отображается время последнего входа в систему и содержимое файла `/etc/motd` (если только это не отключено в файле конфигурации или `~/.hushlogin`);
- если регистрация в системе произведена на терминале, записывается время регистрации;

- проверяется `/etc/nologin` если он присутствует, выводится его содержимое и завершается работа (исключение – `root`);
- осуществляется переход к выполнению с правами обычного пользователя;
- устанавливаются значения основных переменных среды;
- интерпретируется файл `~/.ssh/environment`, если таковой имеется, и пользователям разрешено изменять среду;
- происходит переход в домашний каталог пользователя;
- если имеется файл `~/.ssh/rc`, то производится его выполнение, а если нет и имеется `/etc/openssh/sshrс`, то выполняется он, в противном случае выполняется `xauth`. Файлам `rc` на стандартный ввод передается протокол аутентификации X11 и `cookie`;
- запускается оболочка пользователя или выполняется указанная команда.

8.10.1.3. SSHRC

Если файл `~/.ssh/rc` существует, он будет выполняться после файлов определения переменных среды, но перед запуском оболочки пользователя или команды. Если используется подмена X11, то на его стандартный ввод будет передана пара «proto cookie», также ему будет доступна переменная среды `DISPLAY`. Сценарий должен вызывать `xauth` самостоятельно для добавления `cookie X11`.

Основная цель этого файла состоит в выполнении процедур инициализации, прежде, чем станет доступным основной каталог пользователя. AFS – пример такой среды.

Этот файл будет, содержать блок аналогичный следующему:

```
if read proto cookie && [ -n "$DISPLAY" ]; then
if [ `echo $DISPLAY | cut -c1-10` = 'localhost:' ]; then
# X11UseLocalhost=yes
echo add unix:`echo $DISPLAY |
cut -c11-` $proto $cookie
else
# X11UseLocalhost=no
echo add $DISPLAY $proto $cookie
fi | xauth -q -
fi
```

Если этот файл отсутствует, то выполняется `/etc/openssh/sshrс`, а если отсутствует и он, то для добавления cookie используется `хauth`.

8.10.1.4. Формат файла `authorized_keys`

Параметр `AuthorizedKeysFile` файла конфигурации определяет путь к файлу с открытыми ключами. Значение по умолчанию – `~/.ssh/authorized_keys` и `~/.ssh/authorized_keys2`. Каждая строка файла содержит один ключ (пустые строки или строки, начинающиеся с символа «#» считаются комментариями и игнорируются). Открытые ключи протокола 1 (RSA) состоят из следующих полей, разделенных пробелами: параметры, битность, порядок, модуль, комментарий. Открытые ключи протокола версии 2 состоят из полей: параметр, тип ключа, ключ в виде `base64`, комментарий. Поля параметров необязательны; их отсутствие определяется наличием в начале строки цифры (поле параметра никогда не начинается с цифры). Поля битности, порядка, модуля и комментарий определяют ключ RSA; поле комментария не используется (но может быть удобно пользователю для отметки ключа). Для протокола версии 2 типом ключа является `ecdsa-sha2-nistp256`, `ecdsa-sha2-nistp384`, `ecdsa-sha2-nistp521`, `ssh-dss` или `ssh-rsa`.

Строки в этих файлах, обычно имеют длину в несколько сотен байт (из-за размера открытого ключа RSA) и могут достигать длины в 8 килобайт (таким образом, максимальный размер ключа DSA – 8 килобит, а RSA – 16 килобит). Очевидно, не стоит вводить их вручную. Вместо этого следует скопировать файл `identity.pub`, `id_dsa.pub` или `id_rsa.pub` и отредактировать их.

Минимальная длина модуля RSA независимо от протокола составляет 768 бит.

Параметры (если таковые имеются) состоят из разделенных запятой определений. Для указания пробелов следует воспользоваться двойными кавычками. Поддерживаются следующие определения параметров (регистр названий параметров не учитывается):

- `command="команда"` – выполнять команду при каждом использовании данного ключа для аутентификации. Команда, передаваемая пользователем, будет игнорироваться. Команда выполняется на псевдо-терминале, если последний запрашивается клиентом; в противном случае она выполняется

без терминала. Если требуется «чистый» 8-битный канал, запрашивать псевдо-терминал или указывать по-pty нельзя. В команду может быть включена кавычка, предваренная обратной косой чертой. Данный параметр полезен для ограничения использования определенных RSA-ключей. Примером может служить ключ, по которому можно выполнять удаленные операции резервного копирования и ничего более. Учтите, что клиент по-прежнему может запросить перенаправление TCP и (или) X11, если только это не запрещено явно. Команда, запрашиваемая клиентом, заносится в переменную `SSH_ORIGINAL_COMMAND`. Заметьте, что данный параметр относится к выполнению оболочки, команды или подсистемы;

- `environment="ПЕРЕМЕННАЯ=значение"` – добавить переменную в среду (или переопределить ее значение) при регистрации в системе с использованием данного ключа. Допускается указание нескольких таких директив. По умолчанию изменение переменных среды таким образом отключено. За его включение отвечает параметр `PermitUserEnvironment`. Этот параметр отключается автоматически при включении `UseLogin`;
- `From="список-шаблонов"` – если параметр определен, то в дополнение к прохождению аутентификации по открытому ключу каноническое имя удаленного хоста должно соответствовать одному из шаблонов в списке (шаблоны указываются через запятую). Цель этого параметра – увеличение степени защиты: если частный ключ хоста каким-либо образом удастся похитить, то он позволит злоумышленнику войти в систему из любой точки мира. Этот дополнительный параметр делает использование ворованных ключей более затруднительным (кроме перехвата ключа, требуется взлом серверов имен и (или) маршрутизаторов). Смотрите секцию ШАБЛОНЫ в `ssh_config`;
- `no-agent-forwarding` – запретить перенаправление агента аутентификации при аутентификации данным ключом;
- `no-port-forwarding` – запретить перенаправление TCP/IP при аутентификации данным ключом. Любой запрос на перенаправление порта

приведет к получению клиентом сообщения об ошибке. Это может быть использовано, например, вместе с параметром `command`;

- `no-pty` – запретить назначение терминала (запросы на назначение псевдо-терминала не будут удовлетворены);
- `no-X11-forwarding` – запретить перенаправление X11 при аутентификации данным ключом. Любой запрос на перенаправление порта возвратит клиенту сообщение об ошибке;
- `permitopen="хост:порт"` – для функции перенаправления данных с локального клиентского порта на порт удаленной системы (выполняемого при указании `ssh -L`) ограничить набор возможных целей для перенаправления указанной машиной и портом. Для указания адресов IPv6 можно использовать альтернативный синтаксис: `хост/порт`. Допускается указание нескольких целей через запятую. Значение параметра не интерпретируется как шаблон (т. е. является литеральным);
- `tunnel="n"` – принудительно использовать устройство `tun` на сервере. Без этого параметра при запросе клиентом туннеля используется ближайшее доступное для этого устройство.

Пример файла `authorized_keys`:

```
# допустимы комментарии только на всю строку
ssh-rsa AAAAB3Nza...LiPk== user@example.test
from="*.sales.example.test,!pc.sales.example.test" ssh-rsa
AAAAB2...19Q== test@example.test
command="dump /home",no-pty,no-port-forwarding ssh-dss
AAAAC3...51R== example.test
permitopen="192.0.2.1:80",permitopen="192.0.2.2:25" ssh-dss
AAAAB5...21S==
tunnel="0",command="sh /etc/netstart tun0" ssh-rsa AAAA...==
user@example.test
```

8.10.1.5. Формат файла `ssh_known_hosts`

В файлах `/etc/openssh/ssh_known_hosts` и `~/.ssh/known_hosts` хранятся открытые ключи всех машин, с которыми когда-либо устанавливалась связь. Глобальный файл должен быть подготовлен администратором (это необязательно), пользовательский файл поддерживается автоматически: каждый раз, когда поступает запрос на соединение от неизвестной машины, ее ключ автоматически заносится в пользовательский файл.

Каждая строка в этом файле содержит следующие поля: имена хостов, битность, порядок, модуль, комментарий. Поля разделены пробелами.

Имена хостов – это разделенный запятыми список шаблонов (символы подстановки – ('*' и '?')); каждый шаблон сопоставляется с каноническим именем машины (при аутентификации клиента) или с именем, которое указано пользователем (при аутентификации сервера). Этот шаблон может также быть предварен знаком '!' для обозначения отрицания: если имя машины соответствует отрицаемому шаблону, оно будет отвергнуто (этой строкой) даже если оно соответствует другому шаблону в этой же строке. Также можно, заключив имя хоста или IP-адрес в квадратные скобки – '[' и ']', – через ':' указать нестандартный порт.

Вместо имен хостов можно записывать их хеши. Это позволит скрыть их от злоумышленника в случае попадания файла в его руки. Для различия хешей от имен хостов первые предваряются символом '!'. На одной строке может быть не больше одного хеша, операция отрицания в этом случае не доступна.

Разрядность, порядок и модуль копируются из ключа хоста RSA, например, `/etc/openssh/ssh_host_key.pub`. Необязательное поле комментария занимает всю оставшуюся часть строки и игнорируется.

Комментариями также считаются пустые и строки, начинающиеся с «#».

Идентификация машины принимается, если любая совпавшая строка содержит правильный ключ. Таким образом, можно (хотя это не рекомендуется) иметь несколько строк или различных ключей для одного и того же хоста. Это неизбежно случается при помещении в файл кратких форм имен хостов из различных доменов. В файлах может содержаться противоречивая информация. Идентификация принимается, если корректная информация имеется в любом из них.

Заметьте, что строки в этих файлах, обычно имеют длину в несколько сотен символов и, очевидно, не стоит вводить имена хостов вручную. Вместо этого их можно сгенерировать при помощи сценария оболочки или взять из файла `/etc/ssh/ssh_host_key.pub`, добавив вначале имя хоста.

Пример файла `ssh_known_hosts`:

```
# допустимы явные комментарии только на всю строку
closenet,...,192.0.2.53 1024 37 159...93 closenet.example.test
```

```

cvs.example.test,192.0.2.10 ssh-rsa AAAA1234.....=
# хеш имени хоста
|1|JfKTdBh7rNbXkVAQCRp4OQoPfmI=|USECr3SWf1JUPsms5AqfD5QfxkM= ssh-
rsa
AAAA1234.....=

```

8.10.1.6. Файлы

`~/.hushlogin` – позволяет отключить вывод времени последнего входа в систему и содержимого файла `/etc/motd`, если в файле конфигурации включены соответственно `PrintLastLog` и `PrintMotd`. Файл не влияет на вывод содержимого `Banner`.

`~/.rhosts` – используется для аутентификации по хосту. На некоторых машинах, если каталог пользователя находится на разделе NFS, для того чтобы он был доступен пользователю `root`, он должен быть доступен для чтения всем. Файл должен принадлежать пользователю и не должен быть доступен для записи другим. Рекомендуемый набор прав доступа в общем случае – чтение/запись для пользователя и недоступность для других.

`~/.shosts` – аналогичен файлу `.rhosts`, но позволяет проводить аутентификацию на основе хоста, не разрешая вход в систему с помощью `rlogin/rsh`.

`~/.ssh/authorized_keys` – содержит список открытых ключей (DSA/ECDSA/RSA), которые могут быть использованы для регистрации данного пользователя. Формат файла описан выше. Этот файл не очень важен для злоумышленника, но мы рекомендуем сделать его доступным только пользователю (чтение/запись).

Если этот файл, каталог `~/.ssh` или домашний каталог пользователя доступны для записи другим пользователям, этот файл может быть изменен или заменен любым пользователем системы, имеющим сколько угодно мало прав. В этом случае `sshd` не будет использовать этот файл, если только параметр `StrictModes` не имеет значение «по». Установить рекомендуемый набор прав доступа можно командой `chmod go-w ~/ ~/.ssh ~/.ssh/authorized_keys`.

`~/.ssh/environment` – этот файл (при его наличии) считывается в среду при регистрации в системе. Он может содержать только пустые строки, строки комментария (начинающиеся с «#»), и определения значений переменных в виде: переменная=значение. Правом на запись этого файла должен обладать только пользователь; он не должен быть доступен остальным. Задание переменных среды отключено по умолчанию, за что отвечает параметр `PermitUserEnvironment`.

`~/.ssh/known_hosts` – список адресов, к которым когда-либо подключался пользователь, и которые отсутствуют в общесистемном файле, и соответствующих им открытых ключей. Формат файла описан выше. Файл должен быть доступен для записи только владельцу и администратору. Он может также быть доступен для чтения всем остальным, но это не обязательно.

`~/.ssh/rc` – сценарий инициализации, запускаемый перед запуском оболочки пользователя или команды. Этот файл должен быть доступен для записи только пользователю и не должен быть вообще доступен другим.

`/etc/hosts.allow` и `/etc/hosts.deny` – данные о разрешении и запрете соединений с хостами для надстроек TCP.

`/etc/hosts.equiv` – используется для аутентификации на основе хоста. Должен быть доступен для записи только `root`.

`/etc/openssh/moduli` – модули для схемы Диффи-Хеллмана.

`/etc/motd` – содержимое файла отображается программой `login` после того, как осуществлен успешный вход в систему, перед запуском команды интерпретатора.

`/etc/nologin` – если существует, подключение будет разрешено только пользователю с идентификатором `root`. Любому, кто пытается войти в систему, будет показано содержимое этого файла, и запросы на регистрацию в качестве не пользователя с идентификатором `root` будут отвергнуты. Этот файл должен быть доступен для чтения всем.

`/etc/shosts.equiv` – аналогичен `hosts.equiv`, но позволяет проводить аутентификацию на основе хоста, не разрешая вход в систему с помощью `rlogin/rsh`.

`/etc/openssh/ssh_known_hosts` – общесистемный список известных хостов и их ключей. Этот файл должен составляться администратором. В него следует включать открытые ключи всех компьютеров организации. Формат файла описан выше. Файл должен быть доступен всем для чтения и владельцу/администратору для записи.

`/etc/openssh/ssh_host_key`, `/etc/openssh/ssh_host_dsa_key`,
`/etc/openssh/ssh_host_ecdsa_key`, `/etc/openssh/ssh_host_rsa_key` – содержат частные ключи хостов. Файлы должны принадлежать `root`, и быть доступными только для него. Служба OpenSSH не запустится, если эти файлы доступны для чтения кому-либо, кроме пользователя с идентификатором `root`.

`/etc/openssh/ssh_host_key.pub`, `/etc/openssh/ssh_host_dsa_key.pub`,
`/etc/openssh/ssh_host_ecdsa_key.pub`, `/etc/openssh/ssh_host_rsa_key.pub` – содержат открытые ключи хостов. Эти файлы должны быть доступны всем для чтения, но только `root` может изменять их содержимое. Содержимое файлов должно соответствовать содержимому соответствующих файлов с частными ключами. Эти файлы не используются программой и предназначены для копирования пользователем в файлы `known_hosts`. Эти файлы создаются командой `ssh-keygen`.

`/etc/openssh/sshd_config` – конфигурация службы `sshd`.

`/etc/openssh/sshrc` – аналогичен `~/.ssh/rc`, позволяет задавать инициализационный сценарий глобально для всех пользователей. Должен быть доступен всем для чтения и только `root` для записи.

`/var/empty` – каталог `chroot` используемый при отделении полномочий на предаутентификационном этапе. В папке не должно быть никаких файлов, она должна принадлежать только `root` и не должна быть доступна другим для записи.

`/var/run/sshd.pid` – идентификатор процесса, ожидающего запросов на подключение (если одновременно работает несколько экземпляров служб для нескольких портов, в него записывается идентификатор экземпляра, запущенного последним). Содержимое этого файла может не быть защищено и может быть доступно всем.

8.10.1.7. Использование openssh и openssh-gostcrypto

По умолчанию, в ОС используется openssh-gostcrypto – сборка с использованием библиотек криптоалгоритмов, описанных в ГОСТ 34.11–2018 «Информационная технология. Криптографическая защита информации. Функция хэширования». При необходимости использовать openssh вместо openssh-gostcrypto, предварительно следует удалить все пакеты openssh-* в которых встречается gostcrypto, а затем установить аналогичные пакеты openssh-*

Для этого выполнить команду (от пользователя root):

```
apt-get install `rpm -qa |grep openssh |grep gostcrypto |sed 's/-gostcrypto-.*//'\`
```

8.10.2. SSHD_CONFIG

8.10.2.1. Описание файла конфигурации

Служба sshd считывает данные о конфигурации из файла /etc/openssh/sshd_config (или из файла, указанного в командной строке при помощи параметра -f). Файл содержит пары «параметр-значение», по одной на строку. Пустые строки и строки, начинающиеся с «#», интерпретируются как комментарии. В случае, если аргументы содержат пробелы, они должны быть заключены в двойные кавычки (”).

Файл /etc/openssh/sshd_config должен быть доступен для записи только пользователю root, и рекомендуется делать его доступным для чтения всем.

В таблице 11 приведены описания возможных параметров (регистр имен аргументов учитывается, регистр имен параметров – нет).

Т а б л и ц а 11 – Описание параметров

Параметр	Описание
AcceptEnv	Список переменных среды, которые, будучи заданы клиентом, будут копироваться в <code>envirop</code> сеанса. Соответствующая настройка на стороне клиента выполняется параметром <code>SendEnv</code> и описана в <code>ssh_config</code> . Переменные указываются по имени, допускаются символы подстановки «*» и «?» Несколько переменных среды можно указывать через пробелы или в нескольких параметрах <code>AcceptEnv</code> . Данный параметр введен для предотвращения обхода ограничений среды пользователя посредством изменения значений переменных среды. По умолчанию не принимаются никакие переменные среды
AddressFamily	Семейство адресов, которое должна использовать служба <code>sshd</code> . Допустимые значения: «any», «inet» (только IPv4) и «inet6» (только IPv6). Значение по умолчанию – «any»
AllowGroups	Список шаблонов имен групп через пробел. Если параметр определен, регистрация в системе разрешается только тем пользователям, чья главная или вспомогательная группы соответствуют какому-либо из шаблонов. Допустимы только имена групп. По умолчанию разрешена регистрация в системе для членов всех групп. Разрешающие/запрещающие (<code>allow/deny</code>) директивы обрабатываются в следующем порядке: <code>DenyUsers AllowUsers DenyGroups AllowGroups</code>
AllowTcpForwarding	Определяет, будет ли разрешено перенаправление TCP. Значение по умолчанию – «yes». Отключение пересылки TCP не увеличит уровень защищенности системы, пока пользователям не запрещен доступ к командной оболочке, так как они всегда могут установить свои собственные перенаправления
AllowUsers	Список имен пользователей через пробел. Если параметр определен, регистрация в системе будет разрешена только пользователям, чьи имена соответствуют одному из шаблонов. Допустимы только имена пользователей; числовой идентификатор пользователя не распознается. По умолчанию разрешена регистрация в системе для всех пользователей. Если шаблон указывается в форме <code>ПОЛЬЗОВАТЕЛЬ@ХОСТ</code> , его две части проверяются отдельно, таким образом, разрешая доступ только пользователям с указанными именами, подключающимся с указанных хостов. Разрешающие/запрещающие (<code>allow/deny</code>) директивы обрабатываются в следующем порядке: <code>DenyUsers AllowUsers DenyGroups AllowGroups</code>
AuthorizedKeysFile	Файл с открытыми ключами, которые могут быть использованы для аутентификации пользователей. Допустимо указание шаблонов, они преобразуются при настройке соединения: «%» заменяется на символ '%', «h» заменяется на домашний каталог идентифицируемого пользователя, «u» – на имя пользователя. После преобразования <code>AuthorizedKeysFile</code> интерпретируется либо как абсолютный путь, либо как путь относительно домашнего каталога пользователя. Значение по умолчанию: <code>/etc/openssh/authorized_keys/%u</code> <code>/etc/openssh/authorized_keys2/%u .ssh/authorized_keys .ssh/authorized_keys2.</code>

Продолжение таблицы 11

Параметр	Описание
Banner	Содержимое указанного файла будет отправлено удаленному пользователю прежде, чем будет разрешена аутентификация. Этот параметр доступен только с протоколом версии 2. По умолчанию не выводится никакой информации
ChallengeResponseAuthentication	Определяет, разрешается ли беспарольная аутентификация «вызов-ответ». Поддерживаются все схемы аутентификации <code>login.conf</code> . Значение по умолчанию – «no»
Ciphers	Допустимые для протокола версии 2 шифры. Несколько кодов указываются через запятую. Поддерживаются следующие шифры: «3des-cbc», «aes128-cbc», «aes192-cbc», «aes256-cbc», «aes128-ctr», «aes192-ctr», «aes256-ctr», «arcfour128», «arcfour256», «arcfour», «blowfish-cbc» и «cast128-cbc». Значение по умолчанию: <ul style="list-style-type: none"> - aes256-ctr, aes192-ctr, aes128-ctr, arcfour256, arcfour128; - blowfish-cbc, aes256-cbc, aes192-cbc, aes128-cbc, 3des-cbc, cast128-cbc, arcfour
ClientAliveCountMax	Количество запросов, проверяющих доступность клиента, которые могут оставаться без ответа. Если предел достигнут, <code>sshd</code> отключит клиента и завершит сеанс. Запросы <code>client alive</code> отличаются от <code>TCPKeepAlive</code> . Данные запросы отправляются через защищенный канал и поэтому не могут быть подменены. Параметр <code>TCPKeepAlive</code> допускает возможность подмены данных. Механизм <code>client alive</code> полезен, если поведение клиента или сервера зависит от активности соединения. Значение по умолчанию – 3. Если <code>ClientAliveInterval</code> равно 15, а для <code>ClientAliveCountMax</code> оставлено значение по умолчанию, не отвечающие клиенты SSH будут отключаться приблизительно через 45 секунд. Данный параметр относится только к протоколу версии 2
ClientAliveInterval	Время бездействия со стороны клиента в секундах, после которого <code>sshd</code> отправляет через защищенный канал запрос отклика клиенту. Значение по умолчанию – 0, что означает, что клиенту не будут направляться такие запросы. Этот параметр применим только с протоколом версии 2
Compression	Разрешить сжатие сразу, после аутентификации или вообще запретить его. Допустимые значения – «yes», «delayed» и «no». Значение по умолчанию – «delayed»
DenyGroups	Список шаблонов имен групп через пробел. Если параметр определен, регистрация в системе пользователям, чья главная или вспомогательная группа соответствует содержащимся в списке шаблонам, не разрешается. Допустимы только имена групп. По умолчанию регистрация в системе разрешена для всех групп. Разрешающие/запрещающие (<code>allow/deny</code>) директивы обрабатываются в следующем порядке: <code>DenyUsers AllowUsers DenyGroups AllowGroups</code>

Продолжение таблицы 11

Параметр	Описание
DenyUsers	Список имен пользователей через пробел. Если параметр определен, регистрация в системе пользователей, чьи имена соответствуют одному из шаблонов, будет запрещена. Допустимы только имена пользователей; числовой идентификатор пользователя не распознается. По умолчанию разрешена регистрация в системе для всех пользователей. Если шаблон указывается в форме <code>ПОЛЬЗОВАТЕЛЬ@ХОСТ</code> , его две части проверяются отдельно, таким образом, запрещается доступ только пользователям с указанными именами, подключающимся с указанных хостов. Разрешающие/запрещающие (<code>allow/deny</code>) директивы обрабатываются в следующем порядке: <code>DenyUsers AllowUsers DenyGroups AllowGroups</code>
ForceCommand	Выполнять указанную команду после регистрации пользователя в системе, игнорируя команду, запрашиваемую им. Команда запускается оболочкой пользователя с ключом <code>-c</code> . Это относится к выполнению оболочки, команды или подсистемы, обычно применяется внутри блока <code>Match</code> . Команда, запрошенная пользователем, помещается в переменную среды <code>SSH ORIGINAL COMMAND</code>
GatewayPorts	Определяет, разрешено ли удаленным машинам подключение к портам, выделенным для туннелирования трафика клиентов. По умолчанию <code>sshd</code> делает доступными порты, используемые для туннелирования иницируемого сервером, только для кольцевого (<code>loopback</code>) адреса, то есть удаленные машины подключаться к перенаправляемым портам не могут. С помощью данного параметра можно исправить такое положение дел. Значение « <code>no</code> » разрешает туннелирование только в рамках данной системы, « <code>yes</code> » разрешает туннелирование для хостов, соответствующих шаблону, а « <code>clientspecified</code> » позволяет клиенту самостоятельно выбирать адрес для туннелирования. Значение по умолчанию – « <code>no</code> »
GSSAPIAuthentication	Допускать аутентификацию по GSSAPI. Значение по умолчанию – « <code>no</code> » Данный параметр относится только к протоколу версии 2
GSSAPICleanupCredentials	Очищать ли кэш аутентификационных данных клиента при завершении сеанса. Значение по умолчанию – « <code>yes</code> » Данный параметр относится только к протоколу версии 2
HostbasedAuthentication	Допускать аутентификацию по хостам, т. е. аутентификацию по <code>rhosts</code> или <code>/etc/hosts.equiv</code> в сочетании с открытым ключом клиента. Этот параметр схож с <code>RhostsRSAAuthentication</code> и применим только к протоколу версии 2. Значение по умолчанию – « <code>no</code> »
HostbasedUsesNameFromPacketOnly	Отключить выполнение запросов имени хоста при обработке файлов <code>~/.shosts</code> , <code>~/.rhosts</code> и <code>/etc/hosts.equiv</code> в рамках аутентификации по хосту (<code>HostbasedAuthentication</code>). При значении « <code>yes</code> » для сравнения будет использоваться имя, указанное клиентом, а не имя, которое может быть получено стандартными средствами соединения TCP. По умолчанию – « <code>no</code> »

Продолжение таблицы 11

Параметр	Описание
HostKey	Файл с частными ключами хоста. Значение по умолчанию – /etc/ssh/ssh_host_key для протокола 1, и /etc/ssh/ssh_host_dsa_key, /etc/ssh/ssh_host_ecdsa_key и /etc/ssh/ssh_host_rsa_key для протокола 2. sshd не будет принимать файлы частных ключей доступные для чтения всей группе или вообще всем пользователям. Можно указывать несколько файлов с ключами хоста. Ключи «rsa1» используются для протокола версии 1, ключи «dsa», «ecdsa» и «rsa» – для версии 2 протокола SSH
IgnoreRhosts	Не учитывать содержимое файлов .rhosts и .shosts при аутентификации RhostsRSAAuthentication и HostbasedAuthentication. При этом будут учитываться только /etc/hosts.equiv и /etc/openssh/shosts.equiv. Значение по умолчанию – «yes»
IgnoreUserKnownHosts	Не учитывать содержимое файла ~/.ssh/known_hosts при RhostsRSAAuthentication или HostbasedAuthentication. Значение по умолчанию – «no»
KerberosAuthentication	Определяет, дозволена ли аутентификация Kerberos. Проверять ли пароль, указанный пользователем для аутентификации PasswordAuthentication в Kerberos KDC. Это может быть либо в форме тикетов Kerberos или, если PasswordAuthentication установлена в «yes», пароль, предоставленный пользователем, будет утвержден через Kerberos KDC. Для использования этого параметра серверу нужна Kerberos servtab, которая разрешит проверку субъекта KDC. Значение по умолчанию – «no»
KerberosGetAFSToken	Если AFS активна и у пользователя имеется Kerberos 5 TGT, получать талон AFS перед обращением к домашнему каталогу пользователя. Значение по умолчанию – «no».
KerberosOrLocalPasswd	В случае непринятия аутентификации посредством Kerberos, проверять пароль другими механизмами, такими как /etc/passwd. Значение по умолчанию – «yes»
KerberosTicketCleanup	Очищать ли кэш талонов пользователя при завершении сеанса. Значение по умолчанию – «yes»
KeyRegenerationInterval	В протоколе версии 1 эфемерный ключ сервера будет автоматически регенерироваться по истечении этого количества секунд. Цель регенерации состоит в том, чтобы предохранить кодированные установленные сеансы от более поздних вторжений на машину и захвата ключей. Ключ нигде не сохраняется. Если установлено значение 0, то ключ не будет регенерироваться. Значение по умолчанию – 3600 (секунд)
ListenAddress	Локальные адреса, по которым sshd должен ожидать соединения. Может быт использован следующие форматы записей: ListenAddress хост адрес-IPv4 адрес-IPv6 ListenAddress хост адрес-IPv4:порт ListenAddress [хост адрес-IPv6]:порт

Продолжение таблицы 11

Параметр	Описание
	Если порт не указан, sshd будет ожидать соединения на указанном адресе и на всех указанных ранее (но не после) в параметре Port портах. По умолчанию ожидается соединение на всех локальных адресах. Допустимо указание нескольких параметров
LoginGraceTime	Сервер отключается по истечении этого времени, если пользователю не удалась регистрация в системе. Если стоит значение 0, то время ожидания не ограничено. Значение по умолчанию – 120 секунд
LogLevel	Задаёт степень подробности сообщений для протоколов sshd. Допустимыми являются значения: QUIET, FATAL, ERROR, INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2, и DEBUG3. Значение по умолчанию – INFO. Значения DEBUG и DEBUG1 эквивалентны. Использование значения DEBUG* нарушает конфиденциальность пользователей и потому не рекомендуется
MACs	Допустимые алгоритмы MAC (Message Authentication Code – код установления подлинности сообщения). Они используются в протоколе версии 2 для гарантирования целостности данных. Несколько алгоритмов следует указывать через запятую. Значение по умолчанию: hmac-md5, hmac-sha1, umac-64@openssh.com, hmac-ripemd160, hmac-sha1-96, hmac-md5-96, hmac-sha2-256, hmac-sha256-96, hmac-sha2-512, hmac-sha2-512-96
Match	Начинает условный блок. Если все критерии на строке Match удовлетворены, указанные в блоке директивы будут иметь больший приоритет, чем указанные в глобальном разделе файла конфигурации. Концом блока считается либо следующая директива Match, либо конец файла. В качестве аргументов Match принимаются пары критерий-шаблон. Допустимые критерии: User Group Host и Address. В самом блоке Match допустимо указание следующих параметров: AllowAgentForwarding, AllowTcpForwarding, AuthorizedKeysFile, AuthorizedPrincipalsFile, Banner, ChrootDirectory, ForceCommand, GatewayPorts, GSSAPIAuthentication, HostbasedAuthentication, HostbasedUsesNameFromPacketOnly, KbdInteractiveAuthentication, KerberosAuthentication, Match, MaxAuthTries, MaxSessions, PasswordAuthentication, PermitEmptyPasswords, PermitOpen, PermitRoot-Login, PermitTunnel, PubkeyAuthentication, RhostsRSAAuthentication, RSAAuthentication, X11DisplayOffset, X11Forwarding и X11UseLocalHost
MaxAuthTries	Ограничение на число попыток идентифицировать себя в течение одного соединения. При достижении количества неудачных попыток аутентификации записи о последующих неудачах будут вноситься в протокол. Значение по умолчанию:
MaxSessions	Ограничение на число одновременно открытых сессий в каждом сетевом соединении. Значение по умолчанию – 10

Продолжение таблицы 11

Параметр	Описание
MaxStartups	Ограничение на число одновременных соединений, в которых не был пройден этап аутентификации. Все последующие соединения не будут приниматься, пока на уже существующем соединении не будет произведена аутентификация или не истечет время, указанное в параметре LoginGraceTime. Значение по умолчанию – «10:30:100». Как альтернатива может быть задействован ранний случайный отказ в подключении путем указания трех разделенных через двоеточие значений «старт:норма:предел» (например, «10:30:60»). Соединение будет сбрасываться с вероятностью «норма/100» (30%) если имеется «старт» (10) (10) соединений с не пройденным этапом аутентификации. Вероятность возрастает линейно и постоянно, попытки будут отвергаться при достижении числа «предел» (60)
PasswordAuthentication	Допускать аутентификацию по паролю. Значение по умолчанию – «yes»
PermitEmptyPasswords	Допускать использование пустых паролей при аутентификации по паролю. Значение по умолчанию – «no»
PermitOpen	Ограничить возможные конечные точки для туннелирования TCP. Допустимые формы указания точек: PermitOpen хост:порт PermitOpen адрес-IPv4:порт PermitOpen [адрес-IPv6]:порт Возможно указание нескольких конечных точек через пробел. Значение «any» снимает ограничение и является значением по умолчанию
PermitRootLogin	Допускать вход в систему через ssh в качестве пользователя с идентификатором root. Допустимые значения: «yes», «without-password», «forced-commands-only», «no». Значение по умолчанию – «without-password». Если этот параметр установлен в значение «without-password» войти в систему в качестве пользователя с идентификатором root, указав для аутентификации пароль, будет невозможно. Если этот параметр установлен в значение «forced-commands-only» будет разрешена регистрация пользователя с идентификатором root в системе по открытому ключу, но только если определен параметр command команда (может быть полезно для удаленного создания резервных копий, даже если регистрация пользователя с идентификатором root в системе не разрешена). Все другие методы аутентификации для пользователя с идентификатором root будут отключены. При значении «no» вход в систему в качестве root будет полностью запрещен
PermitTunnel	Допускать использование перенаправления для устройств tun. Допустимые значения: «yes» «point-to-point» (уровень 3), «ethernet» (уровень 2), «no». Значение «yes» эквивалентно «point-to-point» и «ethernet» одновременно. Значение по умолчанию – «no»

Продолжение таблицы 11

Параметр	Описание
PermitUserEnvironment	Учитывать ли файл ~/.ssh/environment и параметры environment= в файле ~/.ssh/authorized_keys. Значение по умолчанию – «no». Посредством изменения переменных среды пользователи могут обойти ограничения своих полномочий. Например, с помощью механизма LD_PRELOAD
PidFile	Файл в который следует записывать идентификатор процесса службы SSH. Значение по умолчанию – /var/run/sshd.pid
Port	Порт, на котором следует ожидать запросы на соединение. Значение по умолчанию – 22. Допустимо указание параметра несколько раз. См. также ListenAddress
PrintLastLog	Выводить ли время и дату предыдущего входа в систему при интерактивной регистрации пользователя в ней. Значение по умолчанию – «yes»
PrintMotd	Выводить ли содержимое файла /etc/motd при интерактивной регистрации пользователя в системе (в некоторых системах это выполняется оболочкой, сценарием /etc/profile или аналогичным). Значение по умолчанию – «yes»
Protocol	Версии протокола, которые следует принимать. Допустимые значения – «1» и «2» Несколько значений указываются через запятую. Значение по умолчанию – «2». Порядок указания протоколов не имеет значения, т.к. протокол выбирается клиентом из списка доступных
PubkeyAuthentication	Допускать аутентификацию по открытому ключу. Значение по умолчанию – «yes». Данный параметр относится только к протоколу версии 2
RhostsRSAAuthentication	Допускать аутентификацию по rhosts или /etc/hosts.equiv совместно с аутентификацией по хосту RSA. Значение по умолчанию – «no» Данный параметр относится только к протоколу версии 1
RSAAuthentication	Допускать аутентификацию только по ключу RSA. Значение по умолчанию – «yes». Данный параметр относится только к протоколу версии 1
ServerKeyBits	Длина ключа сервера для эфемерного протокола 1. Минимальное значение – 512 (по умолчанию – 1024)
StrictModes	Проверять наборы прав доступа и принадлежность конфигурационных файлов и домашнего каталога пользователя перед разрешением регистрации в системе. Это рекомендуется выполнять потому, что новички иногда оставляют свои каталоги или файлы доступными для записи всем. Значение по умолчанию – «yes»
Subsystem	Позволяет настроить внешнюю подсистему (например, службу FTP). В качестве параметров должны выступать имя подсистемы и команда, которая будет выполняться при запросе подсистемы. Команда sftp-server реализует подсистему передачи файлов sftp. По умолчанию подсистемы не определены. Данный параметр относится только к протоколу версии 2

Продолжение таблицы 11

Параметр	Описание
SyslogFacility	Код источника сообщений для протокола syslog. Допустимые значения: DAEMON, USER, AUTHPRIV, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7. Значение по умолчанию – AUTHPRIV
TCPKeepAlive	Указывает, будет ли система посылать другой стороне контрольные сообщения для удержания соединения активным. Если они посылаются, то разрыв соединения или аварийный отказ одной из машин будут должным образом замечены. При этом временная потеря маршрута также повлечет за собой разрыв соединения. С другой стороны, если контрольные сообщения не посылаются, сеанс на сервере может зависнуть, оставив после себя «пользователей-привидений» и отнимая ресурсы сервера. Значение по умолчанию – «yes». Это позволяет избежать бесконечно долгих сеансов. Для отключения отправки сообщений TCP keepalive установите значение «no»
UseDNS	Выполнять ли запросы DNS для получения имени удаленного хоста для того чтобы убедиться в том, что обратное преобразование выдает тот же самый IP-адрес. Значение по умолчанию – «no»
UseLogin	Использовать login для интерактивных сеансов регистрации в системе. Значение по умолчанию – «no». login никогда не используется для удаленного выполнения команд. Если этот параметр включен, функция x11Forwarding будет отключена, потому что login не может обрабатывать cookie xauth В случае использования разделения полномочий (UsePrivilegeSeparation) данный параметр будет отключен после прохождения аутентификации
UsePAM	Включить интерфейс модулей аутентификации Pluggable Authentication Module. При значении «yes» аутентификация PAM будет доступна через ChallengeResponseAuthentication и PasswordAuthentication в дополнение к учетной записи PAM и обработке модулей сеансов для всех типов аутентификации. Поскольку беспарольная аутентификация PAM «вызов-ответ» служит заменой аутентификации по паролю, нужно отключить либо PasswordAuthentication, либо ChallengeResponseAuthentication. При включенном UsePAM службу sshd можно будет выполнять только с правами root. Значение по умолчанию – «yes»
UsePrivilegeSeparation	Разделять полномочия посредством создания дочернего процесса с меньшими правами для обработки входящего трафика. После прохождения аутентификации для работы с клиентом будет создан специальный процесс, соответствующий его правам. Если значение параметра равно «sandbox», то на непривилегированный процесс до прохождения аутентификации будут наложены дополнительные ограничения. Значение по умолчанию – «sandbox»

Окончание таблицы 11

Параметр	Описание
X11DisplayOffset	Номер первого дисплея доступного для туннелирования трафика X11 sshd (по умолчанию – 10). Позволяет избежать вмешательства sshd в работу настоящих серверов X11
X11Forwarding	Допускать туннелирование X11. Допустимые значения – «yes» и «no». Значение по умолчанию – «yes». Если дисплей-посредник ожидает соединений от любых адресов (или по шаблону) sshd включение туннелирования X11 подвергает сервер и логические дисплеи клиентов дополнительной опасности. Поэтому такое поведение не является поведением по умолчанию. Проверка и подмена аутентификационных данных при атаке выполняются на стороне клиента При туннелировании X11 графический сервер клиента может подвергаться атаке при запросе клиентом SSH туннелирования. Для большей защиты пользователей администратор может запретить туннелирование, установив значение «no». Туннелирование X11 отключается автоматически при включении UseLogin
X11UseLocalhost	К какому адресу следует привязывать сервер туннелирования X11: к кольцевому (loopback) или адресу, указанному по шаблону. По умолчанию сервер туннелирования привязывается к кольцевому адресу, а в качестве хоста в переменную среды DISPLAY заносится «localhost». Это не позволяет удаленным хостам подключаться к дисплею-посреднику. Однако, в случае старых клиентов X11, такая конфигурация может не сработать. Установите тогда X11UseLocalhost в «no». Допустимые значения – «yes» и «no». Значение по умолчанию – «yes»
XAuthLocation	Путь к команде xauth. Значение по умолчанию – /usr/bin/xauth

8.10.2.2. Указание времени

Ключи командной строки sshd и параметры файлов конфигурации могут требовать указания времени. Оно должно указываться в виде последовательности:

время [единицы]

где время – положительное целое число, e обозначающее количество единиц времени; единицы могут принимать следующие значения:

- ничего – секунды;
- s | S – секунды;
- m | M – минуты;
- h | H – часы;
- d | D – дни;
- w | W – недели.

Итоговое время получается в результате сложения всех выражений.

Примеры:

- 600 – 600 секунд (10 минут);
- 10m – 10 минут;
- 1h30m – 1 час 30 минут (90 минут).

8.10.2.3. Настройка беспарольного доступа по ssh

Генерация SSH-ключа (на первом контроллере домена DC1):

```
# ssh-keygen -t ed25519
```

На вопрос о файле для сохранения ключа нажать клавишу «Enter» (по умолчанию).

На вопрос о пароле к ключу также нажать клавишу «Enter» (не указывать пароль).

Скопировать публичную часть SSH-ключа на второй контроллер домена (DC2) для пользователя user:

```
# ssh-copy-id -i ~/.ssh/id_ed25519.pub user@dc2.test.alt
```

Проверка, что ключ был скопирован на DC2:

```
# ssh user@dc2.test.alt
```

```
[user@dc2 ~]$ su -
```

```
Password:
```

```
[root@dc2 ~]# cat /home/user/.ssh/authorized_keys >>.ssh/authorized_keys
```

```
[root@dc2 ~]# exit
```

```
ВЫХОД
```

```
[user@dc2 ~]$ exit
```

```
ВЫХОД
```

```
Connection to dc2 closed.
```

Теперь есть возможность удаленно выполнять команды на DC2 с привилегиями администратора.

8.10.3. USB/IP

USB/IP выполняет задачу подключения USB-устройства к удаленному компьютеру через локальную сеть (проброс USB-устройств по локальной сети).

В качестве пробрасываемых устройств могут быть:

- USB-накопители (fdisk, mkfs, mount/umount, операции с файлами);
- USB-клавиатуры и USB-мыши;
- USB веб-камеры и динамики;
- USB-принтеры, USB-сканеры, USB-конвертеры последовательных интерфейсов и адаптеры USB-Ethernet.

На сервере USB/IP можно выводить перечень устройств, устанавливать и убирать их привязки. На клиенте USB/IP можно выводить перечень устройств, экспортированных серверами USB/IP, присоединять и отсоединять их.

Примечание. К серверу подключаются USB-устройства, которые экспортируются на хост-клиент. Хост-клиент виртуально импортирует USB-устройства.

8.10.3.1. Настройка сервера

Установить пакеты `usbip`, `usbip-server`:

```
# apt-get install usbip usbip-server
```

Подгрузить модули драйверов USB:

```
# modprobe usbip-core
```

```
# modprobe usbip-host
```

Запустить сервис `usbipd` и добавить его в автозапуск:

```
# systemctl enable --now usbipd
```

8.10.3.2. Настройка клиента

Установить пакет `usbip`:

```
# apt-get install usbip
```

Подгрузить модули драйверов USB:

```
# modprobe usbip-core
```

```
# modprobe vhci-hcd
```

8.10.3.3. Управление устройствами

8.10.3.3.1. Сервер

Вывести информацию о подключенных локальных устройствах:

```
# usbip list -l
- busid 1-1.1 (0402:9665)
  ALi Corp. : Gateway Webcam (0402:9665)

- busid 1-1.4 (13fe:4300)
  Kingston Technology Company Inc. : unknown product (13fe:4300)

- busid 2-1.2 (090c:1000)
  Silicon Motion, Inc. - Taiwan (formerly Feiya Technology
Corp.) : Flash Drive (090c:1000)
```

Сделать устройство, например, с ID 2-1.2 доступным:

```
# usbip bind --busid 2-1.2
usbip: info: bind device on busid 2-1.2: complete
```

Теперь к устройству можно получить доступ с клиента.

Закрывать доступ к устройству:

```
# usbip unbind --busid 2-1.2
usbip: info: unbind device on busid 2-1.2: complete
```

8.10.3.3.2. Клиент

Получить список доступных устройств на указанном IP-адресе можно, выполнив команду:

```
# usbip list --remote <IP-адрес>
```

Например:

```
# usbip list --remote 192.168.0.118
Exportable USB devices
=====
- 192.168.0.118
  2-1.2: Silicon Motion, Inc. - Taiwan (formerly Feiya
Technology Corp.) : Flash Drive (090c:1000)
        : /sys/devices/pci0000:00/0000:00:1d.0/usb2/2-1/2-1.2
        : (Defined at Interface level) (00/00/00)
```

Команда подключения к доступному USB-устройству:

```
# usbip attach --remote <IP-адрес> --busid <ID-устройства>
```

Например:

```
# usbip attach --remote 192.168.0.118 --busid 2-1.2
```

Получить список подключенных устройств:

```
# usbip port
Imported USB devices
=====
Port 00: <Port in Use> at High Speed(480Mbps)
        Silicon Motion, Inc. - Taiwan (formerly Feiya Technology
Corp.) : Flash Drive (090c:1000)
        3-1 -> usbip://192.168.0.118:3240/2-1.2
        -> remote bus/dev 002/003
```

Команда отключения устройства:

```
# usbip detach --port <Port_number>
```

Например:

```
# usbip detach --port 00
usbip: info: Port 0 is now detached!
```

8.10.3.4. Графическая утилита

Для проброса устройств, а также для присоединения/отсоединения USB-устройств с сервера можно воспользоваться графическим интерфейсом (пакет `usbip-gui`).

Установка:

```
# apt-get install usbip-gui
```

Примечание. Должны быть также установлены соответствующие пакеты для сервера и клиента.

Примечание. Для того чтобы использовать все возможности утилиты, ее необходимо запускать с правами суперпользователя:

```
# usbip-gui
```

После запуска программы будут отображены текущие подключенные устройства (рис. 203).

В поле «Remote USB Devices» отображается список устройств, доступных на удаленном сервере, в поле «Local USB Devices» – список локально-подключенных устройств, а в поле «Attached Devices» – список устройств, подключенных с удаленного сервера.

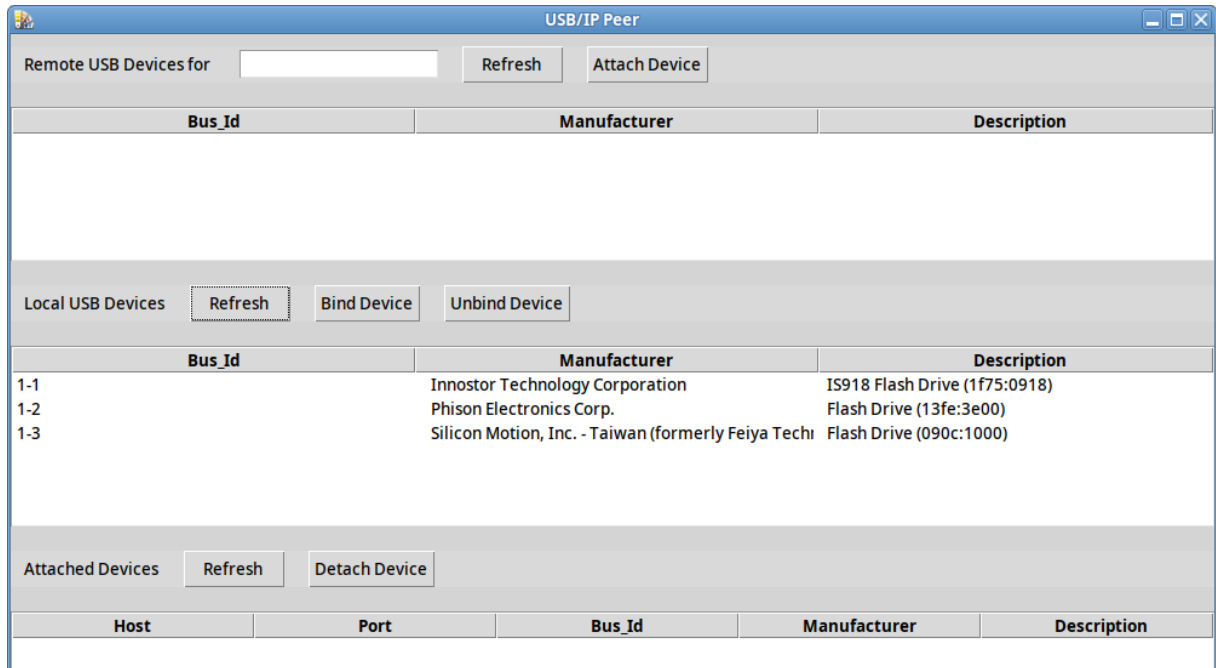


Рис. 203 – Usbip-gui. Подключенные USB-устройства

Кнопки «Refresh», расположенные над каждым полем, позволяют обновить соответствующий список USB-устройств.

Для подключения/отключения USB-устройства с удаленного сервера необходимо:

- 1) ввести IP-сервера в поле «Remote USB Devices for» и нажать на кнопку «Refresh»;
- 2) если на удаленном сервере есть доступные устройства, они появятся в списке «Remote USB Devices»;
- 3) выбрать нужное устройство и нажать на кнопку «Attach Device» (рис. 204);
- 4) устройство появится в списке «Attached Devices» (рис. 205).

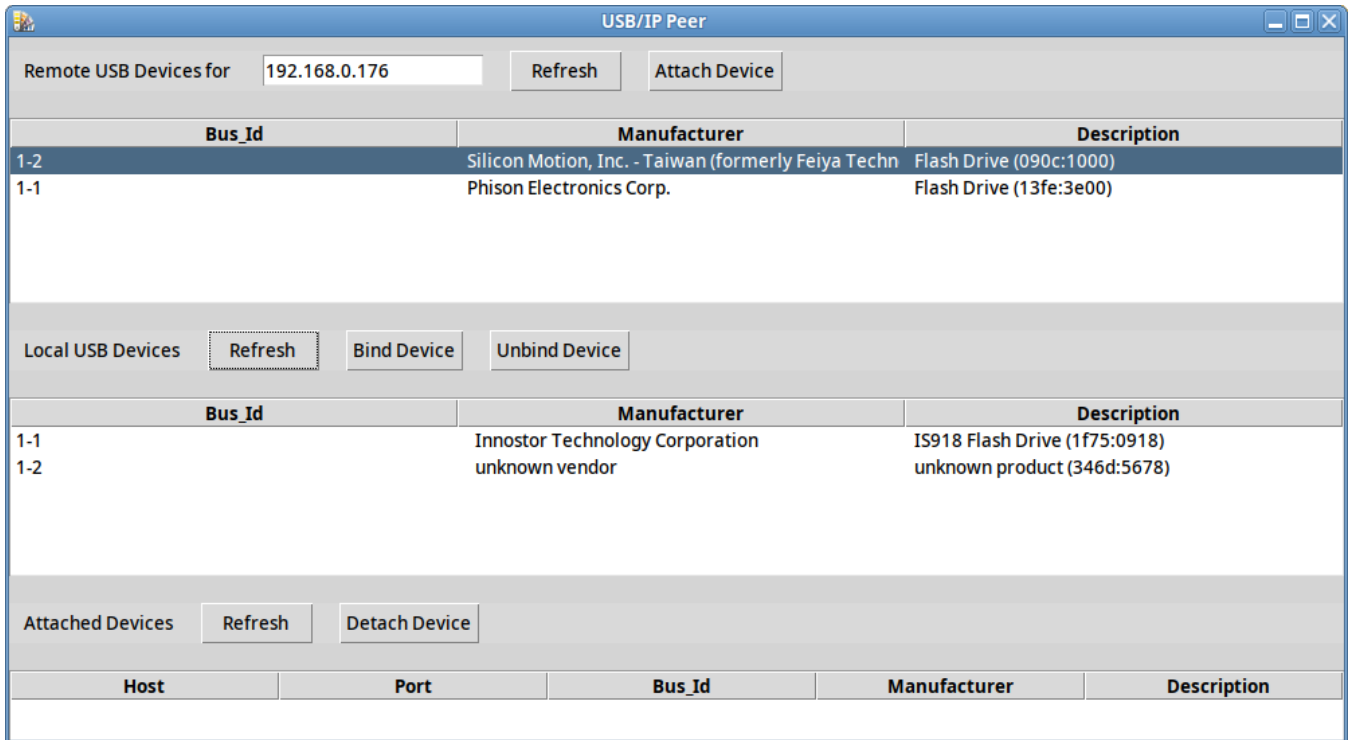


Рис. 204 – Usbip-gui. Подключение к доступному USB-устройству

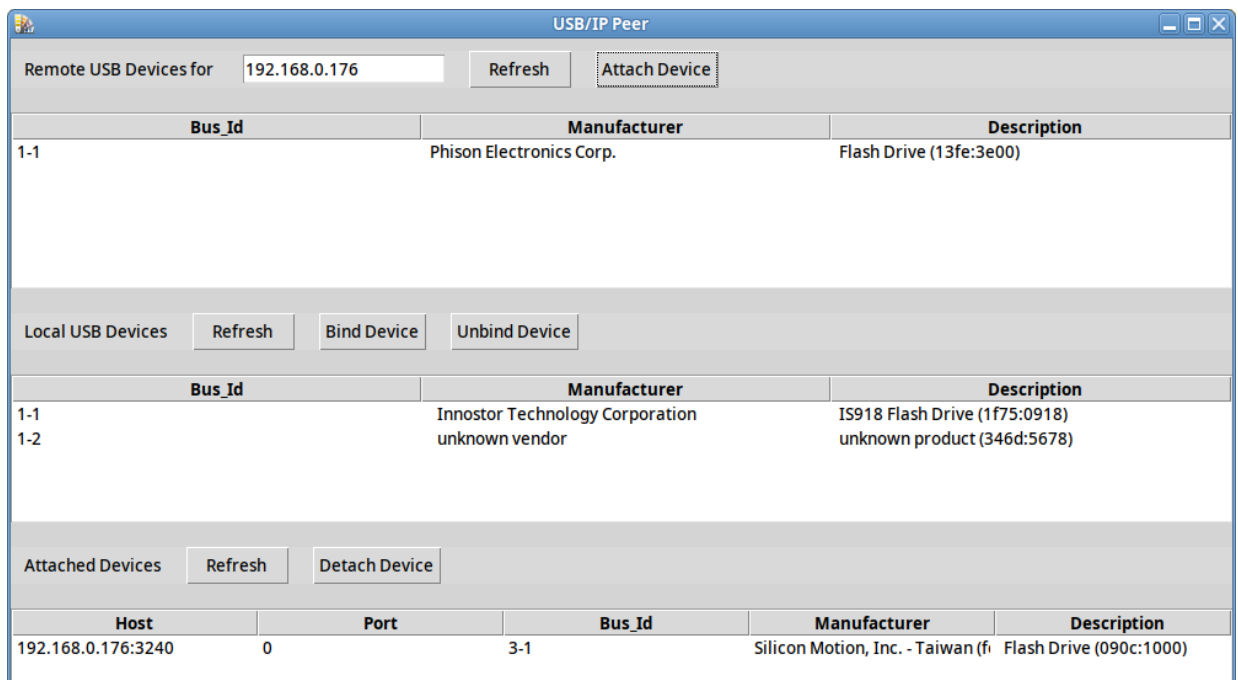


Рис. 205 – Usbip-gui. Список подключенных устройств

Для отключения устройства, достаточно выбрать его в списке «Attached Devices» и нажать на кнопку «Detach Device».

Для того чтобы открыть доступ к локальному USB-устройству, необходимо:

- 1) в поле «Local USB Devices» выбрать нужное устройство (рис. 206);
- 2) нажать кнопку «Bind Device».

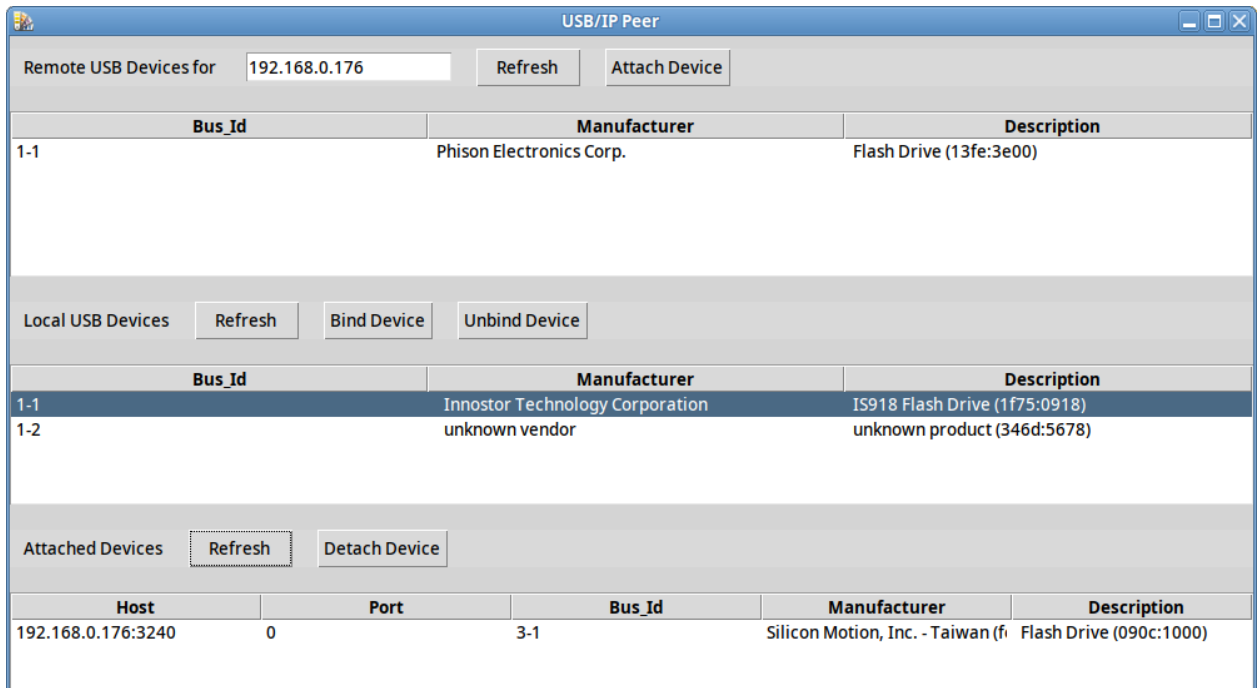


Рис. 206 – Usbip-gui. Локальное USB-устройство

Примечание. Чтобы закрыть доступ к локальному USB-устройству, следует выделить устройство и нажать на кнопку «Unbind Device».

8.11. Прокси-сервер (Squid)

Для обеспечения контролируемого доступа ПЭВМ локальной сети к сети Интернет в составе ОС Альт СП используется кэширующий прокси-сервер Squid.

Примечание. Пакет squid не установлен по умолчанию, для установки выполнить следующую команду:

```
# apt-get install squid
```

Для обеспечения возможности использования ПЭВМ, на которую установлен Squid, в качестве прокси-сервера нужно настроить таблицы управления доступом (Access Control Lists, далее – ACL), которые хранятся в конфигурационном файле squid.conf в директории /etc/squid/.

Для того чтобы сервер Squid принимал соединения из всей внутренней сети, нужно в раздел # TAG: acl включить следующую запись:

```
acl our_networks src <адреса внутренней сети>
http_access allow our_networks
```

При настройке таблиц управления доступом следует учитывать, что при обработке запроса на доступ к серверу Squid все строки http_access файла squid.conf просматриваются последовательно сверху вниз до первой строки, соответствующей параметрам запроса.

8.11.1. Настройка прозрачного доступа через прокси-сервер

Для настройки прозрачного доступа пользователей локальной сети к сети Интернет через прокси-сервер нужно выполнить настройку фильтра адресов, для этого нужно выполнить команду iptables, перенаправляющую HTTP-запросы к внешним серверам на порт Squid:

```
# iptables -t nat -A PREROUTING ! -d <прокси-сервер> \
-i <внутренний_интерфейс> -p tcp -m tcp --dport 80 \
-j REDIRECT --to-ports 3128
```

Также можно выполнить альтернативную команду:

```
# iptables -t nat -A PREROUTING -p tcp -d 0/0 --dport www \
-i <внутренний_сетевой_интерфейс> -j DNAT \
--to <локальный_адрес_на_котором_слушает_прокси>:3128
```

Настройка squid.conf при этом использует обратное проксирование. Далее нужно добавить в конфигурационный файл squid.conf следующую строку:

```
http_port 80 intercept
```

Примечание. Параметр intercept заменяет параметр transparent, который также использовался в предыдущих версиях squid.conf.

8.11.2. Фильтрация доступа

В Squid существует гибкая схема фильтрации внешних ссылок, с помощью которой предоставляется возможность ограничить (запретить) доступ к определенным сетевым ресурсам. Содержимое фильтруется с помощью таблиц управления доступом ACL и настроек http_access deny, примеры которых приведены в конфигурационном файле squid.conf. При задании фильтруемого URL или доменного имени сервера можно использовать регулярные выражения, определяя в одной строке фильтр для целого класса адресов или доменных имен.

Запрет доступа к домену `baddomain.com`, например, можно оформить следующим образом:

```
acl Bad dstdomain baddomain.com
http_access deny Bad
```

8.11.3. Авторизация доступа

Squid позволяет настраивать таблицы доступа ACL индивидуально для пользователей и (или) категорий пользователей. Если для определения того, какой именно пользователь подключается к серверу, недостаточно IP-адреса его компьютера, следует использовать схемы авторизации, принятые в Squid. Авторизация конфигурируется с помощью тега TAG: `auth_param`. Схемы (программы) авторизации, поддерживаемые Squid, хранятся в каталоге `/usr/lib/squid`.

Для настройки аутентификации в LDAP можно использовать следующую конфигурацию:

```
auth_param basic program /usr/lib/squid/squid_ldap_auth -b
ou=People,dc=office,dc=lan -f (uid=%s) -h ldap.office.lan
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
```

8.11.4. Кэширование данных

Squid обеспечивает возможность кэширования данных, полученных по запросам из сети Интернет (при повторных запросах данные извлекаются из сохраненной копии).

Настройка правил кэширования данных осуществляется с помощью таблиц доступа ACL, а также с помощью настройки конфигурационного файла `squid.conf`. Для отключения функции кэширования данных нужно использовать параметр `always_direct`, для включения принудительного кэширования – `never_direct`.

Например, чтобы запретить кэширование данных, получаемых по протоколу FTP, нужно в конфигурационный файл `squid.conf` добавить следующие строки:

```
acl FTP proto FTP
always_direct allow FTP
```

Squid поддерживает возможность обмена данными с кэшем авторизованного сервера (`parent peer` (родительский прокси-сервер) / `sibling peer` (братский прокси-сервер)), например, если запрашиваемый ресурс в локальном кэше Squid не найден.

8.11.5. Настройка режима работы в качестве обратного прокси-сервера

Squid поддерживает режим работы в качестве обратного прокси-сервера. Работа в таком режиме обеспечивает ретрансляцию запросов из внешней сети на один или несколько серверов, логически расположенных во внутренней сети, и позволяет скрыть реальное расположение и структуру серверов, а также уменьшить нагрузку на них.

Для настройки сервера Squid для работы в качестве единственного обратного прокси-сервера, принимающего HTTP-запросы из внешней сети, нужно в конфигурационный файл `squid.conf` добавить следующие строки:

```
http_port 80 accel defaultsite=internal.www.com
cache_peer <имя сервера> parent 80 <порт ICP> no-query
originserver
```

Примечания:

1. В примере в качестве порта, принимающего запросы из внешней сети по протоколу HTTP, используется порт 80.
2. Так как сервер Squid играет роль единственного обратного прокси-сервера, нужно выключить ICP, указав в качестве порта ICP значение 0.
3. `parent` (родительский прокси-сервер) – тип прокси-сервера в соответствии с иерархией серверов.

Для обратного проксирования нескольких внутренних серверов нужно, чтобы внешние запросы к ресурсам сети Интернет с разными доменными именами попадали на вход Squid, который бы ставил в соответствие каждому имени действительный адрес сервера во внутренней сети и в соответствии с этим перенаправлял запрос. Делается это с помощью механизма виртуальных хостов.

Для организации прокси для двух серверов (`www1.foo.bar` и `www2.foo.bar`), адреса которых в DNS указывают на машину со Squid-сервером нужно в конфигурационный файл `squid.conf` добавить следующую запись:

```
http_port 80 accel defaultsite=www1.foo.bar vhost
hosts_file /etc/hosts
```

Настройка `defaultsite` используется сервером для заполнения HTTP-заголовков. Для преобразования доменных имен в адреса серверов во внутренней сети следует использовать файл `/etc/hosts`:

```
10.0.0.1 www1.foo.bar
10.0.0.2 www2.foo.bar
```

8.11.6. Сбор статистики и ограничение полосы доступа

В состав Squid входит утилита кэш-менеджер, предназначенная для отображения статистики и загрузки сервера. Кэш-менеджер представляет собой CGI-приложение и должен выполняться под управлением сконфигурированного HTTP-сервера. Все настройки кэш-менеджера выполняются с помощью конфигурирования файла `squid.conf` (строки, которые относятся к кэш-менеджеру, обычно включают `cachemgr`).

Squid также обеспечивает возможность ограничения полосы пропускания для пользователей (для этого используются параметры `delay_pools` и `delay_class`).

8.11.7. Кеширование DNS-запросов

Squid содержит встроенный минисервер запросов DNS. Он выступает как посредник между Squid и внешними DNS-серверами. При запуске Squid производит начальное тестирование доступности DNS (можно отключить, используя опцию `-D`). Время кеширования удачного DNS-запроса по умолчанию составляет шесть часов.

9. ОГРАНИЧЕНИЕ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ

9.1. Ограничение полномочий пользователей по использованию консолей

9.1.1. Настройка ограничения в ЦУС

Модуль ЦУС «Блокировка терминала» позволяет ограничить определенным пользователям возможность использования определенных ТТУ. Модуль является интерфейсом для файла конфигурации `/etc/security/access.conf`.

Примечание. Должен быть установлен пакет `alterator-secsetup`:

```
# apt-get install alterator-secsetup
```

Для включения модуля необходимо установить отметку в поле «возможность блокировки включена» (рис. 207).

Для каждого отдельного пользователя системы можно заблокировать любые необходимые ТТУ, для этого в окне «Список ТТУ» необходимо отметить консоли, которые должны быть заблокированы для данного пользователя, перенести их в окно «Заблокированные ТТУ» и нажать на кнопку «Применить» (рис. 207).

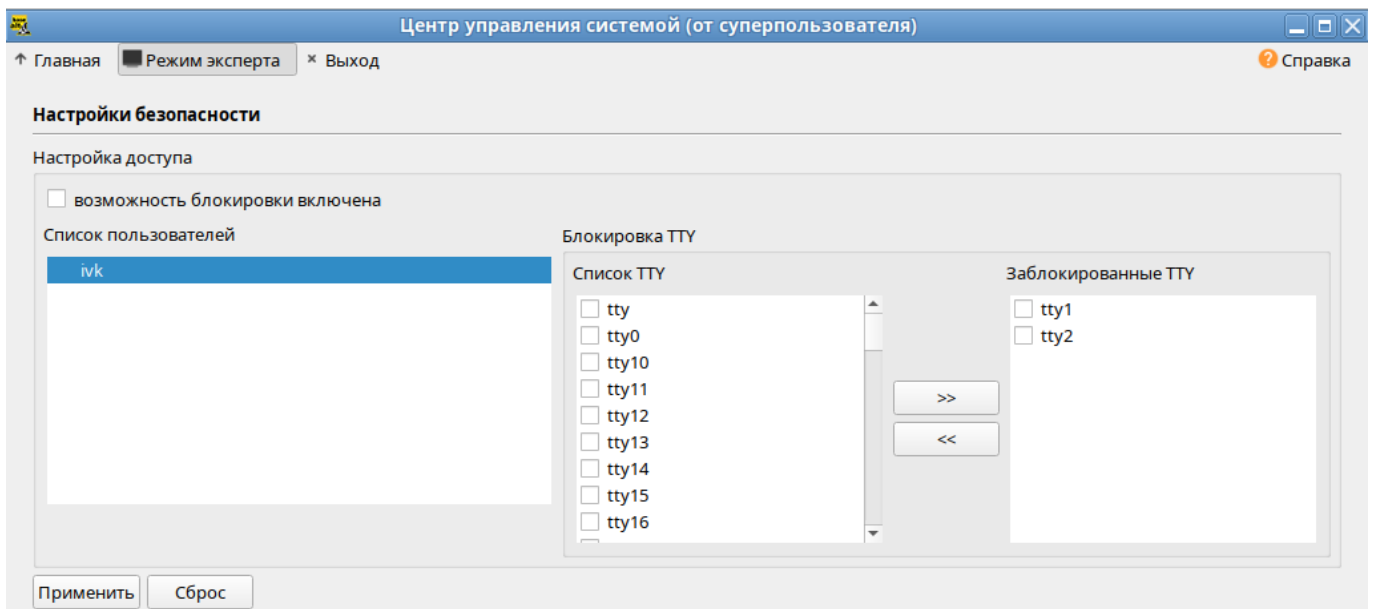


Рис. 207 – Ограничение полномочий пользователей по использованию консолей

9.1.2. Настройка ограничения в консоли

Чтобы ограничить консольный доступ для пользователей/групп с помощью модуля `pam_access.so` необходимо внести изменения в файл `/etc/security/access.conf`.

Примечание. Формат файла `/etc/security/access.conf`:

```
permission:users:origins
```

где:

- `permission` – знак «+» (плюс) – предоставление доступа или знак «-» (минус) – отказ в доступе;
- `users` – список пользователей или групп пользователей или ключевое слово ALL;
- `origins` – список ТТУ (для локального доступа), имен хостов, доменных имен, IP-адресов, ключевое слово ALL или LOCAL.

Чтобы ограничить доступ для всех пользователей, кроме пользователя `root`, следует внести следующие изменения:

```
# vim /etc/security/access.conf
-:ALL EXCEPT root: tty2 tty3 tty4 tty5 tty6
```

Доступ может быть ограничен для конкретного пользователя:

```
# vim /etc/security/access.conf
-:user: tty2 tty3 tty4 tty5 tty6
```

Доступ может быть ограничен для группы, содержащей несколько пользователей:

```
# vim /etc/security/access.conf
-:group: tty2 LOCAL
```

Далее необходимо сконфигурировать стек ПАМ для использования модуля `pam_access.so` для ограничения доступа на основе ограничений, определенных в файле `/etc/security/access.conf`. Для этого дописать в файл `/etc/pam.d/system-auth-local-only` строку `account required pam_access.so` после строки `account required pam_tcb.so`:

```
auth          required          pam_tcb.so shadow fork nullok
account       required          pam_tcb.so shadow fork
account       required          pam_access.so
password     required          pam_passwdqc.so config=/etc/passwdqc.conf
password     required          pam_tcb.so use_authok shadow fork nullok write_to=tcb
session      required          pam_tcb.so
```


9.2. Ограничение неуспешных попыток входа в информационную систему

Для ограничения неуспешных попыток входа используется модуль `pam_faillock`, который считает количество попыток доступа/неудачные попытки аутентификации, может запретить доступ/блокировать учетную запись в случае, если слишком много попыток ввода пароля завершилось неудачно или превышено количество попыток входа.

Можно заблокировать учетную запись: либо на определенный срок, либо пока ее не разблокирует администратор.

Добавление следующей строки в файл `/etc/pam.d/login` заблокирует все учетные записи, кроме `root`, на два часа, после четырех неудачных попыток входа в систему:

```
auth required pam_faillock.so authfail deny=4 unlock_time=7200
```

Добавление этой строки в файл `/etc/pam.d/sshd` заблокирует все учетные записи, кроме `root`, на два часа, после четырех неудачных попыток входа в систему по `ssh`.

В случае, если необходимо, чтобы модуль `pam_faillock` контролировал и учетную запись суперпользователя `root`, в настройки нужно добавить параметр `even_deny_root`. Добавление следующей строки в файл `/etc/pam.d/login` заблокирует все учетные записи, включая учетную запись суперпользователя `root`, после четырех неудачных попыток входа в систему:

```
auth required pam_faillock.so authfail deny=4 even_deny_root unlock_time=7200
```

Модуль `pam_faillock` может отображать количество неудачных попыток входа пользователей, сбрасывать индивидуальные счетчики, или очищать все счетчики.

Примечание. Установка искусственно завышенных счетчиков может использоваться для блокировки пользователей без изменения их паролей.

Запуск утилиты `faillock` без опций позволяет просмотреть количество неуспешных попыток входа в систему всех пользователей.

Количество неудачных попыток входа конкретного пользователя test, в зависимости от используемого модуля, можно увидеть с помощью утилиты:

```
# faillock --user test
```

Примечание. Для получения дополнительной информации смотрите страницы `man pam_faillock` и `faillock`.

Разблокировать учетную запись пользователя без таймаута:

```
# faillock --user test --reset
```

РАМ фиксирует все неудачные попытки входа в систему в syslog, если необходимо записывать все попытки входа в систему (успешные и неуспешные), то в файл `/etc/pam.d/login` нужно добавить строку:

```
account required pam_warn.so
```

9.3. Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы

В файле `/etc/security/limits.conf` определяются ограничения ресурсов системы для пользователя или группы пользователей. Формат файла:

```
<domain> <type> <item> <value>
```

Первое поле (`domain`) может содержать:

- имя пользователя;
- имя группы. Перед именем группы нужно указать символ «@»;
- символ «*». Данное ограничение будет ограничением по умолчанию;
- символ «%» – используется только с ограничением `maxlogins`. Группа, указанная после %, ограничивает число параллельных сеансов всех пользователей, которые являются членами группы. Если символ «%» используется отдельно, он идентичен использованию «*» с ограничением `maxsyslogins`;
- диапазон uid, заданный как `<min_uid>:<max_uid>`;
- диапазон gid, заданный как `@<min_gid>:<max_gid>`;
- gid, заданный как `%:<gid>` – используется только с ограничением `maxlogins`.

Второе поле – это тип ограничения: мягкое (`soft`) или жесткое (`hard`). Мягкое ограничение определяет число системных ресурсов, которое пользователь все еще может превысить, жесткое ограничение превысить невозможно. При попытке

сделать это, пользователь получит сообщение об ошибке. Символ «-» используется для одновременной установки как мягкого, так и жесткого ограничения.

Элементом ограничения (item) может быть:

- core – ограничение размера файла core (Кбайт);
- data – максимальный размер данных (Кбайт);
- fsize – максимальный размер файла (Кбайт);
- memlock – максимальное заблокированное адресное пространство (Кбайт);
- nofile – максимальное число открытых файлов;
- stack – максимальный размер стека (Кбайт);
- cpu – максимальное время процессора (минуты);
- nproc – максимальное число процессов;
- as – ограничение адресного пространства;
- maxlogins – максимальное число одновременных регистраций в системе;
- maxsyslogins – максимальное количество учетных записей;
- priority – приоритет запуска пользовательских процессов;
- locks – максимальное число файлов блокировки;
- sigpending – максимальное количество сигналов, которые можно передать процессу;
- msgqueue – максимальный размер памяти для очереди POSIX сообщений (байт);
- nice – максимальный приоритет, который можно выставить: [-20, 19];
- rtprio – максимальный приоритет времени выполнения.

Чтобы установить максимальное число процессов для пользователя user, в файл `limits.conf` нужно добавить записи:

```
user soft nproc 50
user hard nproc 60
```

Первая строка определяет мягкое ограничение (равное 50), а вторая – жесткое.

Следующие строки обеспечат одновременную работу не более 15 пользователей из каждой группы пользователей (group1 и group2):

```
%group1 - maxlogins 15
%group2 - maxlogins 15
```

В первом и втором случае из каждой группы пользователей одновременно работать смогут не более 15. При шестнадцатой регистрации пользователь из группы увидит сообщение:

```
There were too many logins for 'user'.
```

Следующая запись ограничит число параллельных сеансов доступа для каждой учетной записи пользователя:

```
* - maxlogins 5
```

Примечание. Ограничения также можно настраивать в ЦУС (раздел «Система → «Настройки ограничений» рис. 208). Для этого необходимо установить пакет:

```
# apt-get install alterator-limits
```

Для задания ограничений для пользователя необходимо указать имя пользователя в поле «Домен», выбрать тип ограничения в поле «Тип», выбрать ограничение в поле «Элемент», задать значение в поле «Ограничение» и нажать кнопку «Добавить». После того как все ограничения добавлены нажмите на кнопку «Применить».

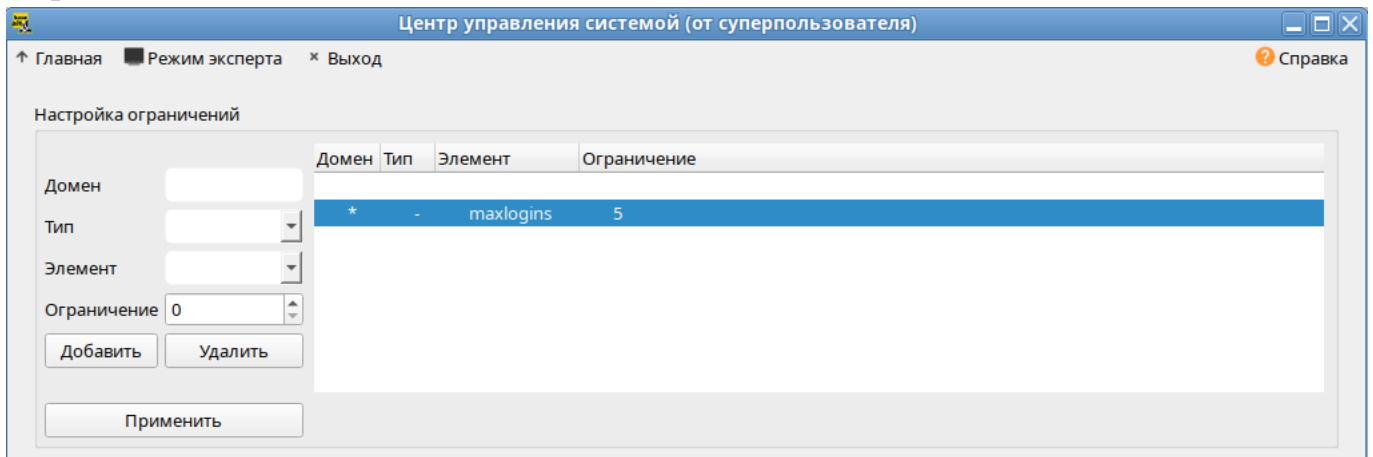


Рис. 208 – Установка ограничений ресурсов, доступных пользователю

9.4. Блокировка макросов в приложениях

Для того чтобы включить блокировку макросов в приложениях, необходимо в ЦУС перейти в раздел «Система» → «Настройки безопасности» (пакет alterator-secsetup).

В открывшемся окне следует отметить пункт «Блокировать макросы приложений» и нажать на кнопку «Применить» (рис. 209).

Макросы будут заблокированы.

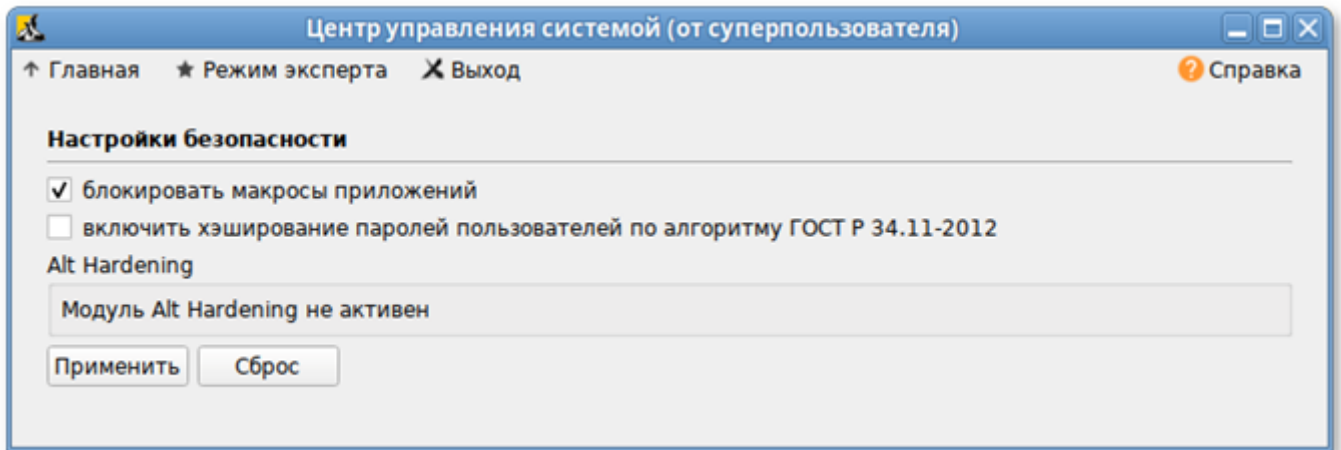


Рис. 209 – Блокировка макросов в приложениях

9.5. Настройка предупреждения пользователя при его входе в систему

Примечание. Для корректной работы функции предупреждения в системе должен быть установлен пакет zenity.

Для реализации функции предупреждения необходимо создать файл `user_login_message` в каталоге `/etc/X11/xinit` со следующим содержимым:

```
#!/bin/sh -e
[ $(id -u) -gt 0 ] || exit 0
[ -n $(which zenity) ] || exit 0
message="Предупреждение! В системе реализованы меры защиты информации, необходимо
соблюдать установленные оператором правила обработки информации. Для продолжения
работы нажмите 'Продолжить', если не хотите продолжения запуска пользовательской
сессии нажмите 'Выйти'"
exec zenity --warning --text "$message" --ok-label="Продолжить" --extra-button
"Выйти"
```

Для отображения пользователю другого сообщения - поправьте значение переменной "message".

Выполнить команду изменения прав на исполнение файла:

```
chmod +x /etc/X11/xinit/user_login_message
```

В файл конфигурации `/etc/X11/Xsession` сразу после строки

```
/etc/X11/xinit/xrootwarn || exit
```

добавить строку `/etc/X11/xinit/user_login_message || exit`

Выполнить перезагрузку ОС.

Теперь после ввода логина и пароля в окне загрузки, перед полным стартом сессии пользователь будет получать предупреждение с указанным в `/etc/X11/xinit/user_login_message` сообщением (рис. 210).

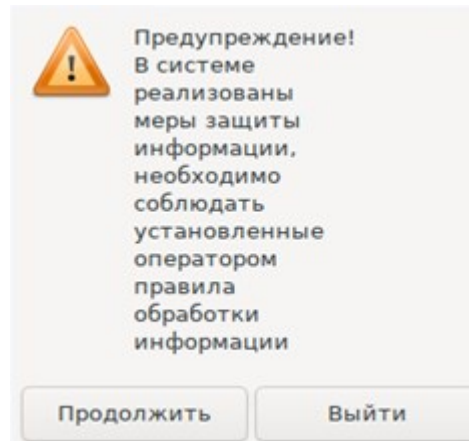


Рис. 210

9.6. Определение параметров уничтожения данных

Для пользователей нужно запретить использование команды `rm`. Для этого нужно выполнить команду:

```
# chmod o-x /bin/rm
```

Команда `srm` предназначена для удаления данных без возможности их восстановления. `srm` выполняет безопасную перезапись/переименование/удаление целевого файла(ов). Использование команды `srm` аналогично использованию `rm`.

Команда `shred` переписывает несколько раз файл, скрывая его содержимое, для того, чтобы сделать более трудоемким процесс восстановления данных даже в случае использования специального оборудования для восстановления:

```
shred [ОПЦИЯ] ФАЙЛ [...]
```

Стандартные опции для запуска команды:

- 1) `-f, --force` – изменить права для разрешения записи, если нужно;
- 2) `-n, --iterations=N` – переписать `N` раз вместо указанных (25) по умолчанию;
- 3) `-s, --size=N` – очистить `N` байт (возможны суффиксы вида К, М, G);
- 4) `-u, --remove` – обрезать и удалить файл после перезаписи;
- 5) `-v, --verbose` – показывать индикатор прогресса;
- 6) `-x, --exact` – не округлять размеры файлов до следующего целого блока;
- 7) `-z, --zero` – перезаписать в конце с нулями, чтобы скрыть перемешивание.

Если файл задан как -, перемешивать стандартный вывод.

Удаляет ФАЙЛЫ если указан `--remove (-u)`. По умолчанию файлы не удаляются, так как часто обрабатываются файлы-устройства вроде `/dev/hda`, а такие файлы нельзя удалять.

Команда `sfill` выполняет безопасную перезапись свободного пространства на разделе, в котором находится указанная директория и всех свободных индексных дескрипторов (`inode`) указанного каталога. Процесс удаления данных выглядит следующим образом:

- 1) 1 проход с `0xff` (все данные затираются значением `0xff`);
- 2) 5 случайных проходов с `/dev/urandom` используя RNG;
- 3) 27 проходов со значениями Питера Гутмана;
- 4) обрезает файл.

Стандартные опции для запуска команды:

- 1) `-d` – игнорировать специальные файлы `"."` и `".."`;
- 2) `-f` – быстрый (и небезопасный режим);
- 3) `-l` – выполнить только два прохода, с `0xff` и случайное заполнение;
- 4) `-l -l` – выполнить только случайное заполнение (один проход);
- 5) `-r` – выполнить в рекурсивном режиме, удалить все подкаталоги;
- 6) `-v` – подробный режим;
- 7) `-z` – последний проход заполняет нулями, а не случайными данными.

Пользователю запрещено определять параметры уничтожения данных. Эти параметры определяет администратор.

Для определения параметров уничтожения данных в системе созданы скрипты с предопределенными настройками уничтожения данных, для их переопределения администратор должен внести правки в файл `/etc/sysconfig/s_rm`.

П р и м е ч а н и е . Должен быть установлен пакет `altsp-test-scripts`.

Пользователи для удаления данных должны использовать команды `s_rm` и `s_fill`.

9.7. Модуль AltNa

AltNa – это модуль безопасности Linux, может использоваться для настройки блокировки возможности удаления открытого файла.

Модуль в настоящее время имеет три варианта защиты пользовательского пространства:

- игнорировать биты SUID в двоичных файлах (возможны исключения);
- запретить запуск выбранных интерпретаторов в интерактивном режиме;
- отключить возможность удаления открытых файлов в выбранных каталогах.

Для включения модуля AltNa нужно передать ядру параметр `altha=1`. Для этого в файле `/etc/sysconfig/grub2` в строке `GRUB_CMDLINE_LINUX_DEFAULT` следует добавить опцию: `altha=1`. Например:

```
# vim /etc/sysconfig/grub2
...
GRUB_CMDLINE_LINUX_DEFAULT='          resume=/dev/disk/by-uuid/187504b7-7f78-
486d-b383-1b638370d3eb panic=30 quiet loglevel=3 splash init_on_free=1
altha=1'
```

Обновить загрузчик, выполнив команду:

```
# update-grub
```

Перезагрузить систему.

Примечание. Для возможности управления настройками модуля AltNa в ЦУС, должен быть установлен пакет `alterator-secsetup`:

```
# apt-get install alterator-secsetup
```

9.7.1. Запрет бита исполнения (SUID)

При включенном подмодуле `altha.nosuid` биты SUID во всех двоичных файлах, кроме явно перечисленных, игнорируются в масштабе всей системы.

Для включения запрета бита исполнения следует установить значение переменной `kernel.altha.nosuid.enabled` равным 1:

```
# sysctl -w kernel.altha.nosuid.enabled=1
```

И добавить, если это необходимо, исключения (список включенных двоичных файлов SUID, разделенных двоеточиями), например:

```
#                               sysctl                               -w
kernel.altha.nosuid.exceptions="/bin/su:/usr/libexec/hashe-priv/hashe-priv"
```


Проверка состояния режима запрета бита исполнения выполняется командой:

```
# sysctl -n kernel.altha.nosuid.enabled  
1
```

Результат выполнения команды:

- 1 – режим включен;
- 0 – режим выключен.

Для включения запрета бита исполнения в ЦУС необходимо перейти в раздел «Система» → «Настройки безопасности», в открывшемся окне отметить пункт «Отключить влияние suid бита на привилегии порождаемого процесса», внести изменения в список исключений и нажать кнопку «Применить» (рис. 211).

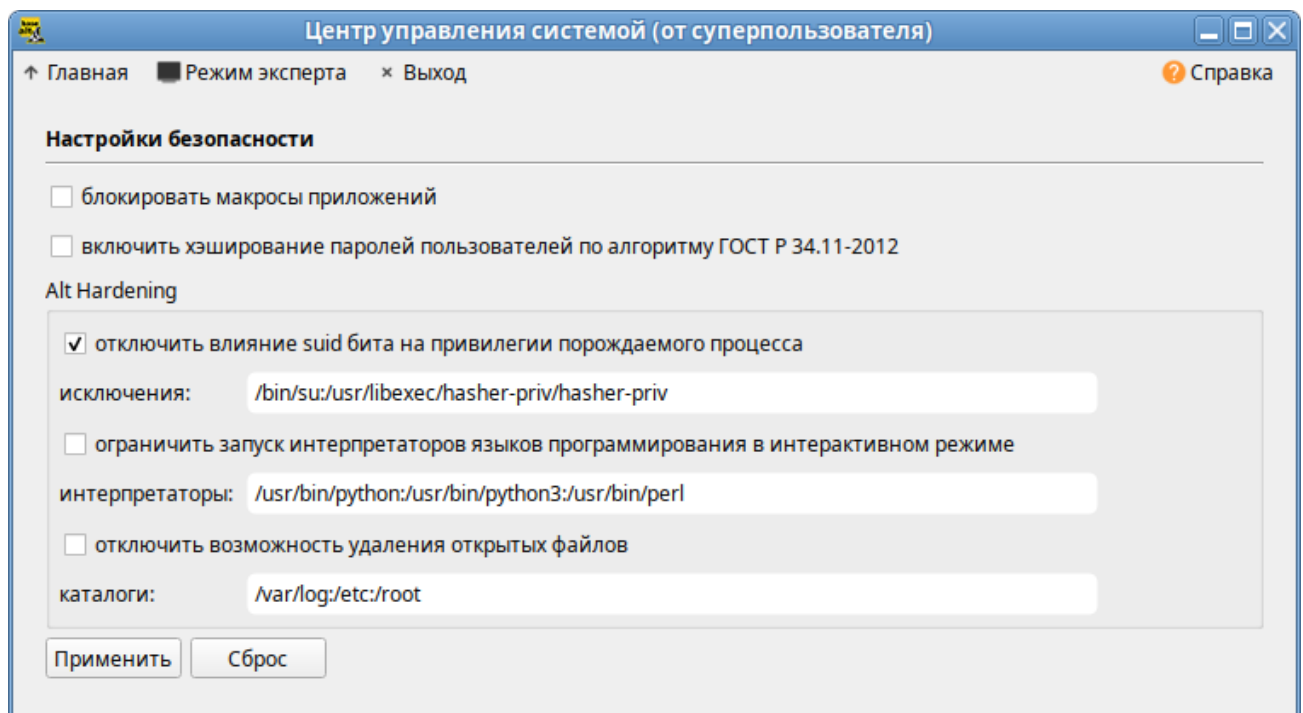


Рис. 211 – Отключение влияния бита SUID на привилегии порождаемого процесса

9.7.2. Блокировка интерпретаторов (запрет запуска скриптов)

При включении блокировки интерпретаторов блокируется несанкционированное использование интерпретатора для выполнения кода напрямую из командной строки.

Для включения режима блокировки интерпретаторов следует установить значение переменной `kernel.altha.rstrscript.enabled` равным 1:

```
# sysctl -w kernel.altha.rstrscript.enabled=1
```

Переменная `kernel.altha.rstrscript.interpreters` должна содержать разделенный двоеточиями список ограниченных интерпретаторов. Для изменения значения переменной `kernel.altha.rstrscript.interpreters` выполнить команду:

```
# sysctl -w kernel.altha.rstrscript.interpreters=
"/usr/bin/python:/usr/bin/python3:/usr/bin/perl:/usr/bin/tclsh"
```

Примечание. В этой конфигурации все скрипты, начинающиеся с `#!/usr/bin/env python`, будут заблокированы.

Проверка состояния режима блокировки интерпретаторов выполняется командой:

```
# sysctl -n kernel.altha.rstrscript.enabled
1
```

Результат выполнения команды:

- 1 – режим включен;
- 0 – режим выключен.

Для получения списка заблокированных интерпретаторов выполнить команду:

```
# sysctl -n kernel.altha.rstrscript.interpreters
/usr/bin/python:/usr/bin/python3:/usr/bin/perl:/usr/bin/tclsh
```

Для включения режима блокировки интерпретаторов в ЦУС необходимо перейти в раздел «Система» → «Настройки безопасности» (рис. 211). В открывшемся окне следует отметить пункт «Ограничить запуск интерпретаторов языков программирования в интерактивном режиме» и нажать кнопку «Применить». Поле «Интерпретаторы» должно содержать разделенный запятыми список ограниченных интерпретаторов.

9.7.3. Отключение возможности удаления открытых файлов

Для отключения возможности удаления открытых файлов следует установить значение переменной `kernel.altha.oload.enabled` равным 1:

```
# sysctl -w kernel.altha.oload.enabled=1
```

Переменная `kernel.altha.oload.dirs` должна содержать разделенный двоеточиями список каталогов, например: `/var/lib/something:/tmp/something`.

Для изменения значения переменной `kernel.altha.oload.dirs` следует выполнить команду:

```
# sysctl -w kernel.altha.oload.dirs="/var/lib/something:/tmp/something"
```

Проверка состояния режима выполняется командой:

```
# sysctl -n kernel.altha.oload.enabled  
1
```

Результат выполнения команды:

- 1 – режим включен;
- 0 – режим выключен.

При необходимости устанавливать эти переменные автоматически при каждой загрузке ОС, нужно добавить их в файл `/etc/sysctl.conf`. После редактирования `sysctl.conf` применить изменения, без перезагрузки ОС, можно выполнив команду:

```
# sysctl -p
```

Для отключения возможности удаления открытых файлов в ЦУС необходимо перейти в раздел «Система» → «Настройки безопасности» (рис. 211). В открывшемся окне следует отметить пункт «Отключить возможность удаления открытых файлов» и нажать кнопку «Применить».

10. ДОМЕННАЯ ИНФРАСТРУКТУРА НА БАЗЕ АЛЬТ ДОМЕН

10.1. Основные сведения о логической модели «Альт Домен»

Домен – группа компьютеров, пользователей, принтеров и других объектов, совместно использующих общую БД каталога.

Дерево доменов – иерархическая система доменов, имеющая единый корень (корневой домен).

Лес доменов – множество деревьев доменов, находящихся в различных формах доверительных отношений.

Сервер – компьютер, выполняющий определенные роли в домене.

Контроллер домена – сервер, хранящий каталог и обслуживающий запросы пользователей к каталогу. Помимо хранения данных контроллер домена может выступать в качестве одной из FSMO-ролей.

Организационное подразделение (OU) – субконтейнер в домене, который может содержать различные объекты: другие контейнеры, группы, аккаунты пользователей и компьютеров. OU представляет собой единицу административного управления внутри домена, на который администратор может назначить объекты групповых политик и назначить разрешения другим пользователям.

Группы – объекты, являющиеся участниками системы безопасности (security principals) и предназначенные для управления доступом к ресурсам. Каждой группе присваивается уникальный идентификатор безопасности (Security Identifier, SID), который сохраняется в течение всего срока службы.

Состав «Альт Домен»:

- контроллер домена (DC) на базе дистрибутива ОС Альт СП Сервер;
- модуль для ввода компьютера в домен;
- модуль удаленного управления базой данных конфигурации (ADMC) – управляет объектами в домене и групповыми политиками, реализован как графический инструмент;
- модуль редактирования настроек клиентской конфигурации (GPUИ) – позволяет редактировать настройки групповых политик;

- шаблоны групповых политик;
- модуль для применения конфигурации на целевой Linux-ОС (gpupdate).

Разворачивание домена производится в следующем порядке:

- создание первого контроллера в домене;
- присоединение сервера в роли контроллера домена к существующему домену;
- присоединение сервера или рабочей станции в роли рядового участника существующего домена.

10.2. Разворачивание домена

Параметры домена:

- имя домена – test.alt;
- контроллер домена (ОС Альт СП Сервер) – dc1.test.alt (192.168.0.132);
- дополнительный контроллер (ОС Альт СП Сервер) – dc2.test.alt (192.168.0.133);
- контроллер только для чтения (ОС Альт СП Сервер) – rodc.test.alt (192.168.0.134);
- рабочая станция 1 (ОС Альт СП) – host-01.test.alt (192.168.0.135);
- рабочая станция 2 (ОС Альт СП) – host-02.test.alt (192.168.0.125);
- рабочая станция 3 (ОС Windows) – PK1.test.alt (192.168.0.109);
- имя пользователя-администратора – Administrator;
- пароль администратора – Pa\$\$word.

10.2.1. Подготовка системы к установке сервера «Альт Домен»

В этом подразделе перечислены требования для установки сервера (контроллера домена). Перед установкой необходимо убедиться, что система соответствует этим требованиям.

Примечание. Для установки сервера «Альт Домен» нужны привилегии суперпользователя.

Примечание. В условиях реальной эксплуатации рекомендуется использовать два или более DC для обеспечения отказоустойчивости.

10.2.1.1. Системные требования к серверу (контроллеру домена)

10.2.1.1.1. RAM

Для демонстрационной/тестовой системы рекомендуется 2 Гбайт ОЗУ.

Для производственной установки рекомендуется не менее 4 Гбайт ОЗУ, а затем 2 Гбайт на каждую дополнительную 1000 пользователей.

Примечание. Параметр, который оказывает наибольшее влияние на требования к памяти, – это количество одновременных открытых сеансов.

10.2.1.1.2. Размеры хранилища

10 Гбайт достаточно для доменов с несколькими сотнями пользователей.

При планировании размера хранилища также необходимо учесть:

- уровни журналов и политику хранения журналов;
- использование изображений/аватаров для идентификации пользователей;
- количество пользователей, машин и групп;
- место под резервные копии.

10.2.1.1.3. CPU

Для нескольких сотен пользователей достаточно 4 vCPUs.

Некоторые процессы Samba не являются многопоточными, поэтому увеличение числа процессоров не повысит производительность.

Чтобы сбалансировать нагрузку, необходимо создать второй контроллер домена в репликации с первым и применить политику балансировки нагрузки на уровне клиента.

Необходимое количество контроллеров домена зависит от нескольких параметров:

- количество сторонних приложений LDAP, подключенных к AD;
- качество кода сторонних LDAP-приложений, подключенных к AD;
- количество запросов к файловым серверам.

10.2.1.1.4. DNS

Не следует использовать существующий домен, если вы не являетесь владельцем домена. Рекомендуется использовать зарезервированный домен

верхнего уровня RFC2606 (<https://tools.ietf.org/html/rfc2606>) для частных тестовых установок, например, `alt.test`.

Имя домена для разворачиваемого DC должно состоять минимум из двух компонентов, разделенных точкой.

ВАЖНО

Необходимо избегать суффиксов `.local`. При указании домена, имеющего суффикс `.local`, потребуется на сервере и подключаемых компьютерах под управлением Linux отключить службу `avahi-daemon`.

Примечание. Имя, как контроллера домена, так и всех ПК членов домена, не должно превышать 15 символов (ограничение связано с параметром `sAMAccountName` в Active Directory).

10.2.1.2. Синхронизация времени

Для аутентификации Kerberos необходима точная синхронизация времени между рабочими станциями членов домена и контроллером домена. Максимально допустимое отклонение времени по умолчанию составляет 5 минут. Если член домена или DC имеет большую разницу во времени, доступ будет запрещен. В результате пользователь не сможет получить доступ к общим папкам или выполнить запрос к каталогу.

На всех DC домена должен быть настроен сервер времени NTP.

Samba поддерживает как `ntpd`, так и `chrony` в качестве сервера NTP. Демон синхронизирует время с внешними источниками и позволяет клиентам получать время с сервера, на котором запущен демон.

Из рис. 212 видно, что только DC с ролью «Эмулятор PDC» получает свое время от внешних серверов времени, все остальные DC получают время от эмулятора PDC, все рабочие станции получают время от любого DC. Клиенты Windows в конечном итоге получают свое время от DC эмулятора PDC через DC, и если DC эмулятора PDC отключается, другие DC будут продолжать его искать, и время может смещаться. В качестве обходного пути следует установить одинаковые внешние серверы времени на всех DC. В этом случае, если эмулятор PDC отключится и его нельзя будет легко перезапустить, нужно передать или захватить роль эмулятора PDC другому DC.

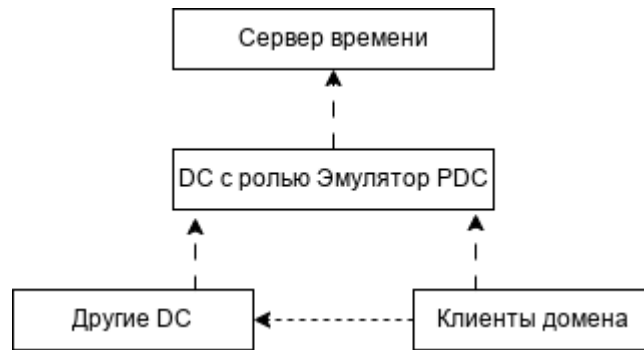


Рис. 212 – Схема синхронизации времени в домене

10.2.1.3. Требования к портам

Для корректной работы службы Samba на контроллере домена должны быть открыты порты, указанные в таблице 12.

Т а б л и ц а 12 – Порты, используемые контроллером домена AD

Служба	Порт	Протокол	Примечание
DNS	53	TCP и UDP	Для DNS от контроллера домена к контроллеру домена и от клиента к контроллеру домена. Может быть предоставлен внутренним DNS-сервером Samba или DNS-сервером Bind9
Kerberos	88	TCP и UDP	Для аутентификации Kerberos
NTP	123	UDP (опционально)	Если на контроллере домена настроен и работает NTP
End Point Mapper (DCE/RPC Locator Service)	135	TCP	Для операций клиента с контроллером домена и контроллеров домена с операциями контроллера домена
NetBIOS Name Service	137	UDP	
NetBIOS Datagram	138	UDP	Для службы репликации файлов между контроллерами домена
NetBIOS Session	139	TCP	Для службы репликации файлов между контроллерами домена
LDAP	389	TCP и UDP	Для обработки регулярных запросов от клиентских компьютеров к контроллерам домена
SMB over TCP	445	TCP	Для службы репликации файлов
Kerberos	464	TCP и UDP	Используется <code>kadmin</code> для установки и смены пароля Kerberos
LDAPS	636	TCP	Если в файле <code>smb.conf</code> установлен параметр <code>tls enabled = yes</code> (по умолчанию)
Global Catalog	3268	TCP	Для глобального каталога от клиента к контроллеру домена
Global Catalog SSL	3269	TCP	Если в файле <code>smb.conf</code> установлен параметр <code>tls enabled = yes</code> (по умолчанию)

Окончание таблицы 12

Служба	Порт	Протокол	Примечание
Dynamic RPC Ports	49152-65535	TCP	Диапазон соответствует диапазону портов, используемому в Windows Server 2008 и более поздних версиях. Чтобы вручную установить диапазон портов в Samba, необходимо задать требуемый диапазон в параметре <code>rpc server port</code> в файле <code>smb.conf</code> . Подробности смотрите в описании параметра на справочной странице <code>man smb.conf</code>

10.2.2. Создание первого контроллера домена

Для управления службой DNS Samba поддерживает работу с двумя DNS-бэкендами:

1) SAMBA_INTERNAL – встроенный сервер имен:

- используется по умолчанию при подготовке нового домена, присоединении к существующему домену или переносе домена NT4 в AD;
- прост в настройке и не требует дополнительного ПО или знаний о DNS;
- следует использовать для простых настроек DNS.

2) BIND9_DLZ – использует Samba AD для хранения информации о зоне:

- требуется BIND 9.8 или более поздняя версия, установленная и настроенная локально на контроллере домена Samba;
- необходимы знания о DNS-сервере BIND и о том, как настроить службу;
- следует использовать для сложных сценариев DNS, которые нельзя настроить во внутреннем DNS.

Примечание. Внутренний DNS-сервер Samba не управляет кешем, поэтому он будет отправлять запрос серверу пересылки для каждого DNS-запроса, который не соответствует его домену. Бэкенд Bind_DLZ использует кеш Bind для рекурсивных запросов. Запросы на сам домен каждый раз передаются модулю DLZ, кеша на этом уровне у него нет.

ВАЖНО

Бэкенд DNS BIND9_FLATFILE не поддерживается.

10.2.2.1. Параметры команды разворачивания домена

Команда `samba-tool domain provision` имеет множество опций, которые можно использовать для предоставления дополнительной информации при интерактивной установке сервера. Эти опции также можно использовать в скриптах.

Ниже описаны некоторые опции (таблица 13). Для получения более подробной информации следует обратиться к man странице `samba-tool(8)`.

Т а б л и ц а 13 – Основные опции для `samba-tool domain provision`

Опция	Описание
<code>-d DEBUGLEVEL,</code> <code>--debuglevel=DEBUGLEVEL</code>	Включить отладку
<code>--interactive</code>	Запрашивать ввод данных у пользователя (интерактивное создание домена)
<code>--domain=DOMAIN</code>	Имя домена NetBIOS (имя рабочей группы)
<code>--domain-guid=GUID</code>	Установить <code>domainguid</code> (иначе используется случайное значение)
<code>--domain-sid=SID</code>	Установить <code>domainsid</code> (иначе используется случайное значение)
<code>--ntds-guid=GUID</code>	Установить GUID объекта NTDS (иначе используется случайное значение)
<code>--host-name=HOSTNAME</code>	Установить имя хоста
<code>--host-ip=IPADDRESS</code>	Установить IPv4 IP-адрес
<code>--host-ip6=IP6ADDRESS</code>	Установить IPv6 IP-адрес
<code>--adminpass=PASSWORD</code>	Пароль основного администратора домена (иначе используется случайное значение)
<code>--krbtgtpass=PASSWORD</code>	Пароль <code>krbtgt</code> (иначе используется случайное значение)
<code>--dns-backend=NAME_SERVER_BACKEND</code>	Бэкенд DNS-сервера: <code>SAMBA_INTERNAL</code> – встроенный сервер имен (по умолчанию), <code>BIND9_FLATFILE</code> – использует текстовую базу данных <code>bind9</code> для хранения информации о зоне, <code>BIND9_DLZ</code> – использует Samba AD для хранения информации о зоне, <code>NONE</code> – полностью пропускает настройку DNS (не рекомендуется)
<code>--dnspass=PASSWORD</code>	Пароль <code>dns</code> (иначе используется случайное значение)
<code>--server-role=ROLE</code>	Позволяет указать тип серверной роли: <code>domain controller</code> , <code>dc</code> (по умолчанию), <code>member server</code> , <code>member</code> или <code>standalone</code>
<code>--function-level=FOR-FUN-LEVEL</code>	Позволяет указать уровень домена и леса: 2000, 2003, 2008, 2008_R2 (по умолчанию) или 2016
<code>--base-schema=BASE-SCHEMA</code>	Версия базовой схемы домена (по умолчанию 2019)
<code>--use-rfc2307</code>	Позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux
<code>--machinepass=PASSWORD</code>	Пароль для машины (иначе используется случайное значение)
<code>--plaintext-secrets</code>	Сохранять конфиденциальные данные в виде обычного текста на диске (по умолчанию конфиденциальные данные шифруются)
<code>--realm=REALM</code>	Задаёт область Kerberos (LDAP), и DNS имя домена
<code>--option=OPTION</code>	Позволяет установить параметры <code>smb.conf</code> из командной строки
<code>-s FILE, --configfile=FILE</code>	Позволяет указать файл конфигурации

10.2.2.2. Установка пакетов

Установить пакет `task-samba-dc` для Samba DC на базе Heimdal Kerberos:

```
# apt-get install task-samba-dc
```

Примечание. Этот шаг можно пропустить, если при установке ОС на этапе «Установка системы» был выбран профиль «Альт Домен (контроллер домена)» (рис. 213)

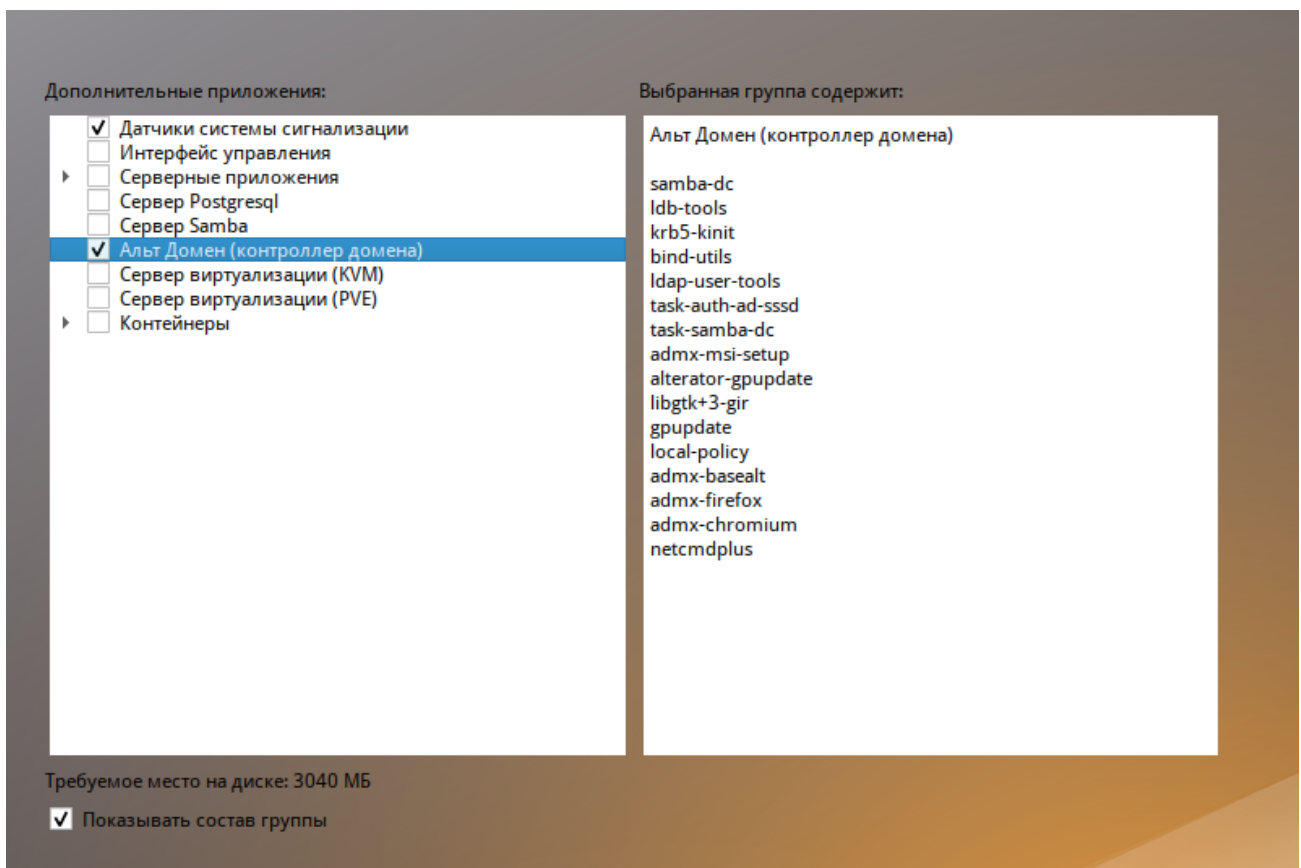


Рис. 213 – Выбор профиля «Альт Домен (контроллер домена)» при установке ОС

Так как Samba в режиме контроллера домена использует свой сервер LDAP, свой центр распределения ключей Kerberos и свой сервер DNS (если не включен плагин `BIND9_DLZ`), перед установкой необходимо остановить конфликтующие службы `krb5kdc` и `slapd`, а также `bind`:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl disable $service; systemctl stop $service; done
```

Выключить автозагрузку служб и отключить службы можно также в ЦУС в разделе «Система» → «Системные службы» (см. п. 8.7.2).

10.2.2.3. Внутренний DNS-сервер Samba (SAMBA_INTERNAL)

Контроллер домена предоставляет внутренний DNS-сервер, который поддерживает основные функции, необходимые для домена. Он прост в настройке и не требует дополнительного программного обеспечения или знаний о DNS. Создание домена с внутренним DNS-сервером рекомендуется для простых настроек DNS.

Внутренний DNS-сервер Samba имеет следующие недостатки:

- нельзя использовать как кеширующий сервер (caching resolver);
- не поддерживает рекурсивные запросы;
- не поддерживает подпись транзакции с общим ключом (TSIG) (shared-key transaction signature);
- нет зоны-заглушки (stub zones);
- не поддерживает передачу зоны DNS (zone transfers);
- не поддерживает балансировку нагрузки циклического перебора между контроллерами домена (Round Robin load balancing among DC's).

Внутренний DNS-сервер может разрешать только DNS-зоны домена. Чтобы включить рекурсивные запросы других зон, следует в параметре `dns forwarder` в файле `smb.conf` указать один или несколько IP-адресов DNS-серверов, поддерживающих рекурсивное разрешение. Например:

```
dns forwarder = 192.168.0.190
```

Примечание. Samba 4.5 и более поздние версии в параметре `dns forwarder` поддерживают несколько IP-адресов, разделенных пробелами. Старые версии поддерживают один IP-адрес. Обращение ко второму и последующим DNS-серверам произойдет только в том случае, если первый не вернул никакого ответа.

Примечание. Внешний DNS-сервер можно указать при создании домена.

При создании домена с внутренним DNS-сервером нужно использовать параметр `--dns-backend=SAMBA_INTERNAL` или не указывать этот параметр вообще.

10.2.2.3.1. Установка имени контроллера домена

Для сервера должно быть установлено правильное имя узла и домена.

Для установки имени узла и домена следует выполнить команды:

```
# hostnamectl set-hostname <имя узла>
# domainname <имя домена>
```

Например:

```
# hostnamectl set-hostname dcl.test.alt
# domainname test.alt
```

Примечание. После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

10.2.2.3.2. Настройка файла /etc/resolvconf.conf

Для корректного распознавания всех локальных DNS-запросов в файле /etc/resolvconf.conf должна присутствовать строка:

```
name_servers=127.0.0.1
```

Иначе в конец этого файла следует добавить строку:

```
name_servers=127.0.0.1
```


и перезапустить сервис resolvconf:

```
# resolvconf -u
```

10.2.2.3.3. Восстановление к начальному состоянию Samba

Необходимо очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удален):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

 **Перед созданием домена необходимо обязательно удалить /etc/samba/smb.conf:**

```
rm -f /etc/samba/smb.conf
```

10.2.2.3.4. Разворачивание домена

10.2.2.3.4.1. Интерактивное создание домена

Для запуска интерактивной установки необходимо выполнить команду:

```
# samba-tool domain provision
```

В ответе на первые два вопроса нужно указать доменное имя и имя рабочей группы:

```
Realm [TEST.ALT]:
Domain [TEST]:
```

Примечание. Чтобы принять значение по умолчанию, необходимо нажать клавишу <Enter>.

Далее нужно указать тип серверной роли и бэкенд DNS-сервера:

```
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)
[SAMBA_INTERNAL]:
```

При запросе «DNS forwarder IP address» можно указать внешний DNS-сервер, чтобы DC мог разрешать внешние доменные имена:

```
DNS forwarder IP address (write 'none' to disable forwarding)
[127.0.0.1]: 8.8.8.8
```

Задать пароль для администратора:

```
Administrator password:
Retype password:
```

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трех групп из четырех возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль, не полностью соответствующий требованиям, – это одна из причин завершения развертывания домена с ошибкой.

Начнется процесс конфигурации:

```
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=test,DC=alt
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers and extended rights
Adding users container
```

```

Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=test,DC=alt
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
The Kerberos KDC configuration for Samba AD is located at
/var/lib/samba/private/kdc.conf
A Kerberos configuration suitable for Samba AD has been generated at
/var/lib/samba/private/krb5.conf
Merge the contents of this file with your system krb5.conf or replace
it with this one. Do not create a symlink!
Once the above files are installed, your Samba AD server will be ready
to use
Server Role:          active directory domain controller
Hostname:             dc1
NetBIOS Domain:      TEST
DNS Domain:           test.alt
DOMAIN SID:           S-1-5-21-3617232745-2316959539-2936900449

```

Запустить службу samba и добавить ее в автозагрузку:

```
# systemctl enable --now samba
```

Примечание. Если служба samba после установки никаким способом не запускается, необходимо перезагрузить сервер.

Примечание. Пример файла /etc/samba/smb.conf после создания домена с SAMBA_INTERNAL:

```

Global parameters
[global]
    dns forwarder = 8.8.8.8
    netbios name = DC1
    realm = TEST.ALT
    server role = active directory domain controller
    workgroup = TEST
    idmap_ldb:use rfc2307 = yes

[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

[netlogon]
    path = /var/lib/samba/sysvol/test.alt/scripts
    read only = No

```

Далее следует перейти к подразделу п. 10.2.2.5 «Настройка Kerberos».

10.2.2.3.4.2. В пакетном режиме

Для пакетной установки необходимо как минимум указать следующие параметры домена:

- 1) `--realm REALM_NAME` – имя области Kerberos (LDAP), и DNS имя домена;
- 2) `--domain=DOMAIN` – имя домена (имя рабочей группы);
- 3) `--adminpass=PASSWORD` – пароль основного администратора домена;
- 4) `--option="dns forwarder=forwarder_ip_address"` – внешний DNS-сервер, чтобы DC мог разрешать внешние доменные имена;
- 5) `--server-role=ROLE` – тип серверной роли;
- 6) `--dns-backend=NAME_SERVER_BACKEND` – тип серверной роли;
- 7) `--use-rfc2307` – позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux.

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трех групп из четырех возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль, не полностью соответствующий требованиям, – это одна из причин завершения развертывания домена с ошибкой.

Примечание. В таблице 13 описаны некоторые опции команды `samba-tool domain provision`. Полный список параметров можно увидеть, запустив команду:

```
# samba-tool domain provision --help
```

Пример команды создания контроллера домена `test.alt` в пакетном режиме:

```
# mkdir -p /var/lib/samba/sysvol
```

Если уровень не указан, то домен разворачивается на уровне `2008_R2`.

Для разворачивания домена на другом уровне, уровень необходимо явно указать, например:

```
# samba-tool domain provision --realm=test.alt -domain=test \
--adminpass='Pa$$word' --dns-backend=SAMBA_INTERNAL \
--option="dns forwarder=8.8.8.8" \
--option="ad dc functional level = 2016" \
--server-role=dc --function-level=2016
```

Примечание. Если необходим уровень `2012_R2`, то следует сначала развернуть домен на уровне `2008_R2`, а затем повысить его до `2012_R2` (см. п. 10.2.5.1).

Далее следует запустить службу samba и добавить ее в автозагрузку:

```
# systemctl enable --now samba
```

Примечание. Если служба samba после установки никаким способом не запускается, необходимо перезагрузить сервер.

Далее следует перейти к разделу «Настройка Kerberos».

10.2.2.3.4.3. Создание домена в ЦУС

При инициализации домена в веб-интерфейсе ЦУС следует в модуле «Домен» указать «Имя домена», отметить пункт «Active Directory», указать IP-адреса внешних DNS-серверов, задать пароль администратора домена и нажать кнопку «Применить» (рис. 214).

Имя домена:

Примечание: имя домена должно соответствовать [RFC 1035](#):

- Имя домена должно состоять из одного или нескольких компонентов, разделённых точками.
- Компоненты имени домена должны начинаться со строчной или прописной латинской буквы, заканчиваться на латинскую букву или цифру, содержать латинские буквы, цифры и символ «-».
- Компонент имени домена не должен превышать 63 символов.
- Имя домена не должно содержать компоненты «localhost», «localdomain» и «local», которые зарезервированы для служебных целей.
- Рекомендуется указывать домен как минимум из двух компонентов, разделённых точками.

Примеры: *domain.loc, school-33.domain, department.company*

Тип домена:

ALT-домен
(домен, основанный на OpenLDAP и MIT Kerberos. Рекомендуется для аутентификации рабочих станций под управлением ALT Linux)
Этот тип невозможно использовать, поскольку не установлен пакет alt-domain-server.

Active Directory
(домен для контроллера домена Samba AD. Рекомендуется для аутентификации рабочих станций под управлением Windows и Linux)

Дополнительные параметры:

DNS-серверы: (адреса IP внешних серверов DNS)

Пароль администратора: (пароль администратора домена)

Повторите пароль: (повторите фразу)

Текущее состояние:

Служба: %(_ NOT OK (samba service is stopped))

Имя домена: --
 Realm: --
 Имя DC: --
 Сервер LDAP: --
 Сервер KDC: --

FreeIPA
(домен для контроллера домена FreeIPA. Рекомендуется для аутентификации рабочих станций под управлением Linux)
Этот тип невозможно использовать, поскольку не установлен пакет freeipa-server, freeipa-server-dns.

Только DNS
(обслуживание только запросов DNS)

Внимание: изменение имени домена вступит в силу только после перезагрузки компьютера

Восстановить файл конфигурации по умолчанию (krb5.conf).

Рис. 214 – Окно модуля «Домен»

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трех групп из четырех возможных: латинских букв

в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. , не полностью соответствующий требованиям, – это одна из причин завершения развертывания домена с ошибкой.

После успешного создания домена, будет выведена информация о домене (рис. 215).

Перезагрузить сервер для применения изменений.

Active Directory
 (домен для контроллера домена Samba AD. Рекомендуется для аутентификации рабочих станций под управлением и Windows и Linux)

Дополнительные параметры:

DNS-серверы: (адреса IP внешних серверов DNS)

Пароль администратора: (пароль администратора домена)

Повторите пароль: (повторите фразу)

Текущее состояние:

Служба: ОК
 Имя домена: test.alt
 Realm: TEST.ALT
 Имя DC: dc1.test.alt
 Сервер LDAP: dc1.test.alt (192.168.0.132)
 Сервер KDC: 192.168.0.132

Рис. 215 – Информационное окно «Текущее состояние»

10.2.2.4. Домен с BIND9_DLZ

В состав Samba входит модуль BIND9_DLZ, позволяющий использовать в качестве DNS-сервера решение с открытым исходным кодом BIND 9.

BIND 9 представляет собой полнофункциональную реализацию протокола DNS, включающую поддержку DNSSEC, DNS over HTTPS (DoH) и DNS over TLS (DoT).

Служба DNS может разворачиваться как на отдельном сервере, так и на контроллере домена совместно с Samba.

Работа с внешним сервером DNS осуществляется с помощью бэкенда BIND9_DLZ и используется в следующих случаях:

- сложная схема зон DNS;
- поддержка больше одного сервера форвардинга (параметр `dns forwarder` на бэкенде INTERNAL работает только с одним адресом).

Если планируется настроить контроллер домена с использованием серверной части BIND9_DLZ, необходимо сначала установить и настроить DNS-сервер BIND.

10.2.2.4.1. Настройка DNS-сервера BIND

На сервере должны быть установлены пакеты bind и bind-utils:

```
# apt-get install bind bind-utils
```

Примечание. Во избежании появления ошибки при запуске bind:

```
мая 03 14:25:13 dc1 named[3825]: samba_dlz: Failed to configure
zone 'test.alt'
мая 03 14:25:13 dc1 named[3825]: loading configuration: already
exists
мая 03 14:25:13 dc1 named[3825]: exiting (due to fatal error)
мая 03 14:39:44 dc1 named[4309]: Loading 'AD DNS Zone' using
driver dlopen
```

не следует, при установке системы, задавать полное имя для DC (dc1.test.alt).

Примечание. Пакет bind содержит различные утилиты, связанные с DNS, например:

- named-checkconf – проверка синтаксиса файлов конфигурации;
- named-checkzone – проверка файлов зон DNS;
- rndc – инструмент управления службой DNS.

Пакет bind-utils содержит следующие утилиты, связанные с DNS:

- dig – многофункциональный инструмент для опроса DNS-серверов;
- host – позволяет получить информацию о DNS-связях между доменными и IP-адресами;
- nslookup – позволяет получить информацию DNS об удаленном сервере;
- nsupdate – инструмент для динамического обновления записей DNS.

Основные файлы настройки DNS:

- /etc/named.conf – основной файл конфигурации, содержит в себе ссылки на остальные конфигурационные файлы;
- /etc/bind/options.conf – файл для глобальных настроек службы;
- /etc/bind/rndc.conf – получить информацию DNS об удаленном сервере;
- /etc/bind/local.conf – файл для настроек зоны DNS;
- /var/lib/samba/bind-dns/named.conf – инструмент для динамического обновления записей DNS.

В таблице 14 описаны некоторые параметры конфигурационного файла /etc/bind/options.conf. Для получения более подробной информации следует обратиться к man странице named.conf(5).

Т а б л и ц а 14 – Основные параметры конфигурационного файла
/etc/bind/options.conf

Опция	Описание
directory	Указывает каталог расположения таблиц зон
listen-on	Определяет адреса IPv4, на которых сервер прослушивает DNS-запросы
listen-on-v6	Определяет адреса IPv6, на которых сервер прослушивает DNS-запросы
allow-query	IP-адреса и подсети от которых будут обрабатываться запросы. Если параметр не задан, сервер отвечает на все запросы
allow-transfer	Устанавливает возможность передачи зон для slave-серверов
allow-query-cache	IP-адреса и подсети, которые могут получить доступ к кешу этого сервера
allow-recursion	IP-адреса и подсети от которых будут обрабатываться рекурсивные запросы (для остальных будут выполняться итеративные запросы). Если параметр не задан, сервер выполняет рекурсивные запросы для всех сетей
pid-file	Указывает путь к файлу, в который сервер записывает идентификатор процесса
tkey-gssapi-keytab	Устанавливает файл таблицы ключей KRB5, который будет использоваться для обновлений GSS-TSIG. Это файл таблицы ключей KRB5, который можно использовать для обновлений GSS-TSIG. Если этот параметр установлен, а tkey-gssapi-credential не установлен, обновления разрешены с любым ключом, соответствующим участнику в указанной вкладке ключей
minimal-responses	Контролирует, добавляет ли сервер записи в разделы полномочий и дополнительных данных. При значении yes сервер добавляет записи в авторитетные и дополнительные разделы только тогда, когда такие записи требуются протоколом DNS (например, при возврате делегирования или отрицательных ответах)
max-cache-ttl	Указывает максимальное время (в секундах), в течение которого сервер кеширует обычные (положительные) ответы. Максимальный срок кеша по умолчанию – 04800 (одна неделя)
forward	Позволяет указать, каким образом сервер обрабатывает запрос клиента. При значении first DNS-сервер будет пытаться разрешать имена с помощью DNS-серверов, указанных в параметре forwarders. Если разрешить имя с помощью данных серверов не удалось, то попытаться разрешить имя самостоятельно. Если указать значение none, сервер не будет пытаться разрешить имя самостоятельно
forwarders	DNS-сервер, на который будут перенаправляться запросы клиентов
dnssec-validation	Включает проверку DNSSEC в именованных файлах. Если установлены значения auto (по умолчанию) и yes, проверка DNSSEC включена. Если установлено значение no, проверка DNSSEC отключена
recursion	Определяет нужно ли выполнять рекурсивные запросы, если просит клиент, NO – не выполнять. Если ответ найден в кеше, то возвращается из кеша
type	Указывает тип зоны, описываемой в текущем разделе. Тип зоны может принимать следующие значения: <ul style="list-style-type: none"> - forward – указывает зону переадресации, которая переадресовывает запросы, пришедшие в эту зону; - hint – указывает вспомогательную зону; - master – указывает работать в качестве мастер сервера для текущей зоны; - slave – указывает работать в качестве подчиненного сервера для текущей зоны

Настройка BIND9 для работы с «Альт Домен»:

1) отключить chroot:

```
# control bind-chroot disabled
```

2) отключить KRB5RCACHETYPE:

```
# grep -q KRB5RCACHETYPE /etc/sysconfig/bind || echo
'KRB5RCACHETYPE="none"' >> /etc/sysconfig/bind
```

3) подключить плагин BIND_DLZ:

```
# grep -q 'bind-dns' /etc/bind/named.conf || echo 'include
"/var/lib/samba/bind-dns/named.conf";' >> /etc/bind/named.conf
```

4) отредактировать файл /etc/bind/options.conf:

- в раздел «options» добавить строки:

```
tkey-gssapi-keytab "/var/lib/samba/bind-dns/dns.keytab";
minimal-responses yes;
```

- в параметре forwarders указать сервера, куда будут перенаправляться запросы, на которые нет информации в локальной зоне (если этой информации нет в файле /etc/bind/resolvconf-options.conf):

```
forward first;
forwarders { 8.8.8.8; };
```

- в параметр listen-on добавить IP-адрес DNS-сервера, на котором он будет принимать запросы;

- раскомментировать параметр allow-query и указать в нем подсети, из которых разрешено подавать запросы;

- раскомментировать параметр allow-recursion и указать в нем подсети из которых будут обрабатываться рекурсивные запросы;

- в раздел «logging» добавить строку:

```
category lame-servers {null;};
```

Пример файла /etc/bind/options.conf:

```
options {
    version "unknown";
    directory "/etc/bind/zone";
    dump-file "/var/run/named_dump.db";
    statistics-file "/var/run/named.stats";
    recursing-file "/var/run/recursing";
```

```
// disables the use of a PID file
pid-file none;
tkey-gssapi-keytab "/var/lib/samba/bind-dns/dns.keytab";
minimal-responses yes;

listen-on { 127.0.0.1; 192.168.0.152; };
listen-on-v6 { ::1; };

include "/etc/bind/resolvconf-options.conf";

allow-query { localnets; 192.168.0.0/24; };
allow-recursion { localnets; 192.168.0.0/24; };

//max-cache-ttl 86400;

};

logging {
    category lame-servers {null;};
};
```

5) в файле `/etc/bind/resolvconf-options.conf` в параметре `forwarders` должен быть указан DNS-сервер, на который будут перенаправляться запросы клиентов;

б) выполнить остановку `bind`:


```
# systemctl stop bind
```

Если в роли DNS-сервера Samba используется Bind, то при создании домена нужно использовать параметр `--dns-backend=BIND9_DLZ`.

10.2.2.4.2. Восстановление к начальному состоянию Samba

Необходимо очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удален):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

	Перед созданием домена необходимо обязательно удалить <code>/etc/samba/smb.conf</code> :
	<code>rm -f /etc/samba/smb.conf</code>

10.2.2.4.3. Разворачивание домена

10.2.2.4.3.1. Интерактивное создание домена

Для запуска интерактивной установки необходимо выполнить команду:

```
# samba-tool domain provision
```

В ответе на первые два вопроса нужно указать доменное имя и имя рабочей группы:

```
Realm [TEST.ALT]:
Domain [TEST]:
```

Примечание. Чтобы принять значение по умолчанию, необходимо нажать «Enter».

Далее нужно указать тип серверной роли и бэкенд DNS-сервера:

```
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)
[SAMBA_INTERNAL]: BIND9_DLZ
```

Задать пароль для администратора:

```
Administrator password:
Retype password:
```

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трех групп из четырех возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль, не полностью соответствующий требованиям, – это одна из причин завершения развертывания домена с ошибкой.

Начнется процесс конфигурации:

```
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=test,DC=alt
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers and extended rights
```

```

Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=test,DC=alt
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
See /var/lib/samba/bind-dns/named.conf for an example
configuration include file for BIND
and /var/lib/samba/bind-dns/named.txt for further documentation
required for secure DNS updates
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
The Kerberos KDC configuration for Samba AD is located at
/var/lib/samba/private/kdc.conf
A Kerberos configuration suitable for Samba AD has been generated
at /var/lib/samba/private/krb5.conf
Merge the contents of this file with your system krb5.conf or
replace it with this one. Do not create a symlink!
Once the above files are installed, your Samba AD server will be
ready to use
Server Role:          active directory domain controller
Hostname:             dc1
NetBIOS Domain:      TEST
DNS Domain:           test.alt
DOMAIN SID:          S-1-5-21-3684382553-2825304832-3399765044

```

10.2.2.4.3.2. В пакетном режиме

Для пакетной установки необходимо указать следующие параметры:

- 1) `--realm REALM_NAME` – имя области Kerberos (LDAP), и DNS имя домена;
- 2) `--domain=DOMAIN` – имя домена (имя рабочей группы);
- 3) `--adminpass=PASSWORD` – пароль основного администратора домена;
- 4) `--server-role=ROLE` – тип серверной роли;
- 5) `--dns-backend=NAME_SERVER_BACKEND` – бэкенд DNS-сервера;
- 6) `--use-rfc2307` – позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux.

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трех групп из четырех возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль не полностью соответствующий требованиям это одна из причин завершения развертывания домена ошибкой.

Примечание. В таблице 13 описаны некоторые опции команды `samba-tool domain provision`. Полный список параметров можно увидеть, запустив команду:

```
# samba-tool domain provision -help
```

Так как в роли DNS-сервера Samba используется Bind, то при создании домена нужно использовать параметр `--dns-backend=BIND9_DLZ`.

Пример команды создания контроллера домена test.alt в пакетном режиме:

```
# samba-tool domain provision --realm=test.alt \
--domain test --adminpass='Pa$$word' \
--dns-backend=BIND9_DLZ --server-role=dc
```

Если уровень не указан, то домен разворачивается на уровне `2008_R2`. Для разворачивания домена на другом уровне, уровень необходимо явно указать, например:

```
# samba-tool domain provision --realm=test.alt \
--domain=test --adminpass='Pa$$word' \
--dns-backend=BIND9_DLZ \
--option="ad dc functional level = 2016" \
--server-role=dc -function-level=2016
```

Примечание. Если необходим уровень `2012_R2`, то следует сначала развернуть домен на уровне `2008_R2`, а затем повысить его до `2012_R2` (см. п. 10.2.5.1).

10.2.2.4.4. Запуск служб samba и bind

Установить службы `samba` и `bind` запускаемыми по умолчанию и запустить их:

```
# systemctl enable --now samba
# systemctl enable --now bind
```

Примечание. Если служба `samba` после установки никаким способом не запускается, необходимо перезагрузить сервер.

Примечание. Пример файла `/etc/samba/smb.conf` после создания домена с `BIND9_DLZ`:

```
# Global parameters
[global]
    netbios name = DC1
    realm = TEST.ALT
    server role = active directory domain controller
```

```

server services = s3fs, rpc, nbt, wrepl, ldap, cldap,
kdc, drepl, winbindd, ntp_signd, kcc, dnsupdate
workgroup = TEST

```

```
[sysvol]
```

```

path = /var/lib/samba/sysvol
read only = No

```

```
[netlogon]
```

```

path = /var/lib/samba/sysvol/test.alt/scripts
read only = No

```

10.2.2.4.5. Проверка зон

Следующие примеры запрашивают службу DNS о локальном хосте (127.0.0.1).

Проверка зоны перенаправления localhost:

```

# host -t A localhost 127.0.0.1

Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:
localhost has address 127.0.0.1

```

Проверка реверсивной зоны 0.0.127.in-addr.arpa:

```

# host -t PTR 127.0.0.1 127.0.0.1

Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:
1.0.0.127.in-addr.arpa domain name pointer localhost.

```

10.2.2.5. Настройка Kerberos

Внести изменения в файл `/etc/krb5.conf`. Следует раскомментировать строку `default_realm` и содержимое разделов `realms` и `domain_realm`, и указать название домена (обратите внимание на регистр символов), в строке `dns_lookup_realm` должно быть установлено значение `false`:

```
includedir /etc/krb5.conf.d/
```

```
[logging]
```

```

# default = FILE:/var/log/krb5libs.log
# kdc = FILE:/var/log/krb5kdc.log
# admin_server = FILE:/var/log/kadmind.log

```

```
[libdefaults]
```

```
dns_lookup_kdc = true
```

```

dns_lookup_realm = false
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
default_realm = TEST.ALT
# default_ccache_name = KEYRING:persistent:%{uid}

```

```

[realms]
TEST.ALT = {
default_domain = test.alt
}

```

```

[domain_realm]
dc = TEST.ALT

```

Примечание. В момент создания домена, Samba конфигурирует шаблон файла `krb5.conf` для домена в каталоге `/var/lib/samba/private/`. Можно просто заменить этим файлом файл, находящийся в каталоге `/etc/`:

```
# cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

10.2.2.6. Настройка NTP-сервера

Настройка сервера времени `chrony` в качестве NTP-сервера:

- установить пакет `chrony`:

```
# apt-get install chrony
```

- включить доступ к серверу `chrony`:

```
# control chrony server
```

- установить синхронизацию с российским пулом NTP:

```
sed -i -r 's/^(pool.*)/#\1\npool ru.pool.ntp.org iburst/'
/etc/chrony.conf
```

- или указать серверы NTP в директиве `server` или `pool` в файле конфигурации

NTP `/etc/chrony.conf`:

```
pool pool.ntp.org iburst
```

- включить и запустить службу по умолчанию:

```
# systemctl enable --now chronyd
```

- убедиться в нормальной работе NTP-сервера:

```
# systemctl status chronyd.service
```

Примечание. Параметр `iburst` используется для ускорения начальной синхронизации.

10.2.2.7. Проверка работоспособности домена

Просмотр общей информации о домене:

```
# samba-tool domain info 127.0.0.1
Forest           : test.alt
Domain           : test.alt
Netbios domain   : TEST
DC name          : dc1.test.alt
DC netbios name  : DC1
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
```

Просмотр предоставляемых служб:

```
# smbclient -L localhost -Uadministrator
Password for [TEST\administrator]:

      Sharename      Type      Comment
      -----      -
      sysvol         Disk
      netlogon       Disk
      IPC$           IPC       IPC Service (Samba 4.19.7)
SMB1 disabled -- no workgroup available
```

Создаваемые по умолчанию общие ресурсы netlogon и sysvol нужны для функционирования контроллера домена и создаются в smb.conf в процессе развертывания/модернизации.

Проверка конфигурации DNS:

1) проверка наличия nameserver 127.0.0.1 в /etc/resolv.conf

(для SAMBA_INTERNAL):

```
# cat /etc/resolv.conf
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/ifaces/<interface>/resolv.conf instead.
search test.alt
nameserver 127.0.0.1
```

```
# host test.alt
test.alt has address 192.168.0.132
```

2) проверка имен хостов:

- адрес _kerberos._udp.* адрес домена с точкой:

```
# host -t SRV _kerberos._udp.test.alt.
_kerberos._udp.test.alt has SRV record 0 100 88 dc1.test.alt
```

ЛКНВ.11100-01 90 03

- адрес `_ldap._tcp.*` адрес домена с точкой:

```
# host -t SRV _ldap._tcp.test.alt.
_ldap._tcp.test.alt has SRV record 0 100 389 dc1.test.alt.
```

- адрес `адрес хоста.*` адрес домена с точкой:

```
# host -t A dc1.test.alt.
dc1.test.alt has address 192.168.0.132
```

Если имена не находятся, следует проверить выключение службы `bind` (если не включен плагин `BIND9_DLZ`).

Проверка Kerberos (имя домена должно быть в верхнем регистре):

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
Warning: Your password will expire in 41 days on Ср 03 июл 2024
11:18:36
```

Просмотр полученного билета:

```
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@TEST.ALT

Valid starting          Expires                Service principal
22.05.2024 11:28:23 22.05.2024 21:28:23  krbtgt/TEST.ALT@TEST.ALT
renew until 29.05.2024 11:28:20
```

10.2.3. Присоединение к домену в роли контроллера домена

Для обеспечения отказоустойчивости и балансировки нагрузки в домен могут добавляться дополнительные контроллеры домена.

Системные требования к дополнительному DC такие же, как и для первого контроллера домена (см. п. 10.2.1.1).

Примечание. В терминологии контроллеров домена нет понятия PDC/BDC, т. е. все контроллеры равны, но один из них выступает владельцем ролей FSMO.

Заведение дополнительного контроллера домена выполняется путем присоединения дополнительного DC к существующему домену.

Команда присоединения к домену в роли контроллера домена:

```
# samba-tool domain join <dnsdomain> [DC|RODC|MEMBER] [options]
```

Некоторые параметры, используемые в команде `samba-tool domain join`:

- 1) `--realm REALM_NAME` – имя области Kerberos (LDAP), и DNS имя домена;
- 2) `--dns-backend=NAME SERVER-BACKEND` – бэкенд DNS-сервера:
 - `SAMBA_INTERNAL` – встроенный сервер имен (по умолчанию);
 - `BIND9_DLZ` – использует Samba AD для хранения информации о зоне;
 - `NONE` – полностью пропускает настройку DNS (этот DC не будет DNS-сервером);

Примечание. На втором DC необходимо иметь DNS-бэкенд аналогичный первому DC.

Примечание. При использовании `SAMBA_INTERNAL`, необходимо указать значение `dns forwarder`, чтобы на новом сервере была настроена пересылка запросов:

```
--option="dns forwarder=forwarder_ip_address"
```

Форвардером может быть как вышестоящий DNS-сервер организации, так и публичные от `google` или `yandex`, например:

```
--option="dns forwarder=8.8.8.8"
```

- 3) `--option='idmap_ldb:use rfc2307 = yes'` – если первый контроллер домена создавался с ключом `--rfc2307`, то и для текущего необходимо это учесть, указав данный параметр;
- 4) `--site=SITE` – привязка контроллера домена к определенному сайту AD;
- 5) `--option="interfaces= lo eth0" --option="bind interfaces only=yes"` – привязка Samba к указанным сетевым интерфейсам сервера (если их несколько); указание данной опции позволяет `samba-tool` зарегистрировать корректный IP-адрес при присоединении;
- 6) `--option="ad dc functional level = LEVEL"` – функциональный уровень AD. Возможные значения: `2008_R2` (по умолчанию), `2012`, `2012_R2`.

Примечание. При присоединении к существующему домену рекомендуется указывать функциональный уровень не выше текущего уровня домена.

Примечание. Для получения дополнительной информации о параметрах команды `samba-tool domain join` можно воспользоваться командой:

```
# samba-tool domain join -help
```

Для сервера, на котором будет разворачиваться контроллер домена, должен быть назначен статический IP-адрес и установлено правильное имя узла.

Установить имя узла можно, выполнив команду:

```
# hostnamectl set-hostname dc2.test.alt
```

Примечание. После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

10.2.3.1. Заведение дополнительного DC с бэкендом SAMBA_INTERNAL

Все действия выполняются на узле dc2.test.alt (192.168.0.133), если не указано иное.

Примечание. Для выполнения операции присоединения к домену требуется пароль администратора домена.

Этапы настройки сервера и присоединения к домену в роли контроллера домена с бэкендом SAMBA_INTERNAL:

1) установить пакет task-samba-dc, который установит все необходимое:

```
# apt-get install task-samba-dc
```

2) на добавляемом DC в /etc/resolv.conf обязательно должен быть добавлен первый DC как nameserver:

```
# echo "name_servers=192.168.0.132" >> /etc/resolvconf.conf
# echo "search_domains=test.alt" >> /etc/resolvconf.conf
# resolvconf -u
# cat /etc/resolv.conf
search test.alt
nameserver 192.168.0.132
nameserver 8.8.8.8
```

3) остановить конфликтующие службы krb5kdc и slapd, а также bind:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl
disable $service; systemctl stop $service; done
```

4) очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удален):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

- 5) на существующем контроллере домена завести IP-адрес для дополнительного DC (команда выполняется на узле dc1.test.alt):

⚠ Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

```
# samba-tool dns add 192.168.0.132 test.alt DC2 A \
192.168.0.133 -Uadministrator
Password for [TEST\administrator]:
Record added successfully
```

- 6) на добавляемом DC установить следующие параметры в файле конфигурации клиента Kerberos (/etc/krb5.conf):

```
[libdefaults]
default_realm = TEST.ALT
dns_lookup_realm = false
dns_lookup_kdc = true
```

- 7) для проверки настройки запросить билет Kerberos для администратора домена:

```
# kinit administrator@TEST.AL
Password for administrator@TEST.ALT:
```

⚠ Имя домена должно быть указано в верхнем регистре.

- 8) убедиться, что билет получен:

```
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: administrator@TEST.ALT

Valid starting Expires Service principal
22.05.2024 13:35:08 22.05.2024 23:35:08
krbtgt/TEST.ALT@TEST.ALT
renew until 29.05.2024 13:35:05
```

- 9) ввести дополнительный DC в домен test.alt в качестве контроллера домена:

```
# samba-tool domain join test.alt DC \
-Uadministrator@TEST.ALT --realm=test.alt \
--option="dns forwarder=8.8.8.8"
```

При успешном завершении будет выведена информация о присоединении к домену:

```
Joined domain TEST (SID S-1-5-21-80639820-2350372464-
3293631772) as a DC
```


10) сделать службу samba запускаемой по умолчанию и запустить ее:

```
# systemctl enable --now samba
```

10.2.3.2. Заведение дополнительного DC с бэкендом BIND9_DLZ

Все действия выполняются на узле dc2.test.alt (192.168.0.133), если не указано иное.

Примечание. Для выполнения операции присоединения к домену требуется пароль администратора домена.

Этапы настройки сервера и присоединения к домену в роли контроллера домена с бэкендом BIND9_DLZ:

1) установить пакет task-samba-dc, который установит все необходимое:

```
# apt-get install task-samba-dc
```

2) установить и настроить DNS-сервер BIND (см. «Настройка DNS-сервера BIND» п. 10.2.2.4.1);

3) на добавляемом DC в /etc/resolv.conf обязательно должен быть добавлен первый DC как nameserver:

```
# echo "name_servers=192.168.0.132" >> /etc/resolvconf.conf
# echo "search_domains=test.alt" >> /etc/resolvconf.conf
# resolvconf -u
# cat /etc/resolv.conf
search test.alt
nameserver 192.168.0.132
nameserver 8.8.8.8
```

4) остановить конфликтующие службы krb5kdc и slapd, а также bind:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl
disable $service; systemctl stop $service; done
```

5) очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удален):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

- 6) на существующем контроллере домена завести IP-адрес для дополнительного DC (команда выполняется на узле dc1.test.alt):

⚠ Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

```
# samba-tool dns add 192.168.0.132 test.alt DC2 A 192.168.0.133
-Uadministrator
Password for [TEST\administrator]:
Record added successfully
```

- 7) на добавляемом DC установить следующие параметры в файле конфигурации клиента Kerberos (/etc/krb5.conf):

```
[libdefaults]
default_realm = TEST.ALT
dns_lookup_realm = false
dns_lookup_kdc = true
```

- 8) для проверки настройки запросить билет Kerberos для администратора домена:

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
```

⚠ Имя домена должно быть указано в верхнем регистре.

- 9) убедиться, что билет получен:

```
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: administrator@TEST.ALT
```

```
Valid starting Expires Service principal
22.05.2024 13:35:08 22.05.2024 23:35:08 krbtgt/TEST.ALT@TEST.ALT
renew until 29.05.2024 13:35:05
```

- 10) ввести дополнительный DC в домен test.alt в качестве контроллера домена:

```
# samba-tool domain join test.alt DC --realm=test.alt \
--dns-backend=BIND9_DLZ -Uadministrator@TEST.ALT
```

При успешном завершении будет выведена информация о присоединении к домену:

```
Joined domain TEST (SID S-1-5-21-80639820-2350372464-
3293631772) as a DC
```

11) сделать службы samba и bind запускаемыми по умолчанию и запустить их:

```
# systemctl enable --now samba
# systemctl enable --now bind
```

10.2.3.3. Проверка результатов присоединения

Примечание. После присоединения к домену службе синхронизации данных может понадобиться до 15 минут для автоматического формирования подключений для репликации.

Проверка корректности присоединения:

1) проверить работу DNS (в списке адресов должен отображаться IP-адрес добавленного контроллера домена):

```
$ host -t A test.alt
test.alt has address 192.168.0.132
test.alt has address 192.168.0.133
```

2) проверить статус репликации между контроллерами домена. Для этого на добавленном DC выполнить команду:

```
# samba-tool drs showrepl
```

В случае успешного выполнения репликации в каждом из блоков в разделах «INBOUND NEIGHBORS» и «OUTBOUND NEIGHBORS» отображаются сообщения вида:

```
Default-First-Site-Name\DC1 via RPC
DSA object GUID: 10e22808-960e-4cb3-8724-abd2223555cd
Last attempt @ Sat Jun 15 10:27:21 2024 EET was successful
0 consecutive failure(s).
Last success @ Sat Jun 15 10:27:21 2024 EET
```

В пункте «Last attempt» должны стоять актуальные дата и время, идентичные указанным в строке «Last success» (отображает время последней репликации). Также должно быть «0 consecutive failure(s)».

Подробнее о настройке репликации см. п. 10.6.7.

3) на добавляемом DC создать нового пользователя домена:

```
# samba-tool user add testuser --random-password
User 'testuser' added successfully
```

4) убедиться, что учетная запись созданного пользователя доступна на первом контроллере домена:

```
# samba-tool user list | grep testuser
testuser
```

10.2.3.4. Настройка NTP-сервера

Настроить NTP для работы в режиме сервер (см. п. 10.2.2.6).

10.2.4. Контроллер домена на чтение (RODC)

При присоединении к домену для контроллера может быть выбрана роль RODC (read-only domain controller).

Основная цель контроллера домена, доступного только на чтение (RODC – read-only domain controller) – возможность безопасной установки собственного контроллера домена в удаленных филиалах, в которых сложно обеспечить физическую защиту сервера. Контроллер домена RODC содержит копию базы «Альт Домен», доступную только на чтение. Это означает, что никто, даже при получении физического доступа к такому контроллеру домена, не сможет изменить данные в «Альт Домен» (в том числе сбросить пароль администратора домена).

Основные отличия RODC от обычных контроллеров домена, доступных для записи (RWDC):

- RODC хранит копию базы «Альт Домен», доступную только для чтения. Клиенты не могут вносить изменения в базу такого контроллера домена;
- RODC не реплицирует данные «Альт Домен» на другие контроллеры домена (RWDC) (используется односторонняя репликация);
- контроллер RODC хранит полную копию базы «Альт Домен», за исключением хешей паролей объектов «Альт Домен» и других атрибутов, содержащих чувствительную информацию;
- при получении контроллером RODC запроса на аутентификацию от пользователя, он перенаправляет этот запрос на ближайший RWDC контроллер;
- контроллер RODC может кешировать учетные данные некоторых пользователей (это ускоряет аутентификацию и позволяет пользователям авторизоваться на контроллере домена, даже при отсутствии связи с RWDC);
- DNS служба на RODC работает только на чтение.

Требования, которые должны быть выполнены для разворачивания RODC:

- на сервере должен быть назначен статический IP-адрес;

- уровень леса и домена должен соответствовать 2008R2. Это можно проверить, выполнив следующую команду на контроллере домена:

```
# samba-tool domain level show
Domain and forest function level for domain 'DC=test,DC=alt'

Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
```

- в качестве DNS-сервера должен быть указан ближайший RWDC контроллер.

10.2.4.1. Установка и настройка RODC

Для сервера, на котором будет разворачиваться контроллер домена, должен быть назначен статический IP-адрес и установлено правильное имя узла.

Все дальнейшие действия выполняются на узле rodс.test.alt (192.168.0.134), если не указано иное.

Этапы настройки сервера и присоединения к домену в роли RODC:

- 1) установить пакет task-samba-dc, который установит все необходимое:

```
# apt-get install task-samba-dc
```

- 2) на добавляемом DC в /etc/resolv.conf обязательно должен быть добавлен первый DC как nameserver:

```
# echo "name_servers=192.168.0.132" >> /etc/resolvconf.conf
# echo "search_domains=test.alt" >> /etc/resolvconf.conf
# resolvconf -u
# cat /etc/resolv.conf
search test.alt
nameserver 192.168.0.132
nameserver 8.8.8.8
```

- 3) остановить конфликтующие службы krb5kdc и slapd, а также bind:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl
disable $service; systemctl stop $service; done
```

- 4) очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удален):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

5) на существующем контроллере домена завести IP-адрес для RODC:

⚠ Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

```
# samba-tool dns add 192.168.0.132 test.alt \
RODC A 192.168.0.134 -Uadministrator
Password for [TEST\administrator]:
Record added successfully
```

6) на RODC установить следующие параметры в файле конфигурации клиента

Kerberos /etc/krb5.conf):

```
[libdefaults]
default_realm = TEST.ALT
dns_lookup_realm = false
dns_lookup_kdc = true

[realms]
TEST.ALT = {
kdc = rodc.test.alt
kdc = dc1.test.alt
default_domain = TEST.ALT
}
```

7) для проверки настройки запросить билет Kerberos для администратора домена:

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
```

⚠ Имя домена должно быть указано в верхнем регистре.

Убедиться, что билет получен:

```
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: administrator@TEST.ALT

Valid starting          Expires                Service principal
22.05.2024             14:06:04              23.05.2024           00:06:04
krbtgt/TEST.ALT@TEST.ALT
renew until 23.05.2024 14:06:01
```

8) ввести данный DC в домен test.alt в качестве контроллера домена, доступного только для чтения (RODC):

```
# samba-tool domain join test.alt RODC \
-Uadministrator@TEST.ALT --realm=test.alt
```

Если все нормально, в конце будет выведена информация о присоединении к домену:

```
Joined domain TEST (SID S-1-5-21-578923263-1107570656-1287136478) as an RODC
```

Примечание. При использовании SAMBA_INTERNAL, необходимо указать значение `dns forwarder`, чтобы на новом сервере была настроена пересылка запросов. Форвардером может быть, как вышестоящий DNS-сервер организации, так и публичные от google или yandex.

Если первый контроллер домена создавался с ключом `--rfc2307`, то и для текущего необходимо это учесть, указав параметр:

```
--option='idmap_ldb:use rfc2307 = yes'
```

9) сделать службу `samba` запускаемой по умолчанию и запустить ее:

```
# systemctl enable --now samba
```

Примечание. Для получения дополнительной информации о параметрах команды `samba-tool domain join` можно воспользоваться командой:

```
# samba-tool domain join -help
```

10.2.4.2. Политики репликации и кэширования паролей на RODC

На RODC можно задать список пользователей, чьи хеши паролей можно или нельзя реплицировать на данный контроллер домена.

Примечание. Все пользователи в кеше RODC смогут аутентифицироваться на этом контроллере домена, даже если отсутствует связь с RWDC.

По умолчанию в домене создаются две новые глобальные группы:

- 1) «Allowed RODC Password Replication Group»;
- 2) «Denied RODC Password Replication Group».

Первая группа по умолчанию пуста, а во второй содержатся административные группы безопасности, пароли пользователей которых нельзя реплицировать и кэшировать на RODC. В группу «Denied RODC Password Replication Group» по умолчанию входят группы (рис. 216):

- «Cert Publishers»;
- «Domain Admins»;
- «Domain Controllers»;
- «Enterprise Admins»;

- «Group Policy Creator Owners»;
- «Read-only Domain Controllers»;
- «Schema Admins»;
- учетная запись «krbtgt».

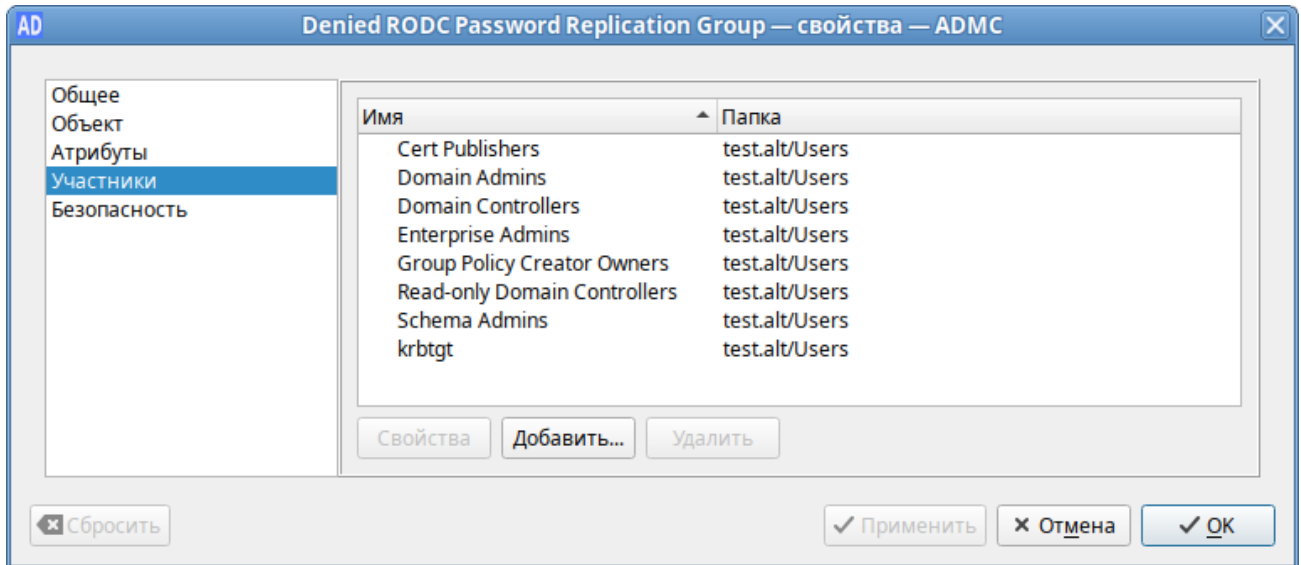


Рис. 216 – Список участников «Denied RODC Password Replication Group» в ADMS

Список участников группы «Denied RODC Password Replication Group» можно получить, выполнив команду:

```
# samba-tool group listmembers "Denied RODC Password Replication Group"
Read-only Domain Controllers
Domain Admins
Enterprise Admins
Domain Controllers
Schema Admins
krbtgt
Group Policy Creator Owners
Cert Publishers
```

Список участников группы «Allowed RODC Password Replication Group» можно получить, выполнив команду:

```
# samba-tool group listmembers "Allowed RODC Password Replication Group"
```

В группу «Allowed RODC Password Replication Group» обычно добавляются группы пользователей филиала, в котором находится RODC.

Для предварительной загрузки данных учетных записей на контроллере RODC используется команда:

```
# samba-tool rodc preload (<SID>|<DN>|<accountname>)+ ... [опции]
```

Возможные опции:

- `--server` – обычный контроллер домена, который будет выступать источником данных при репликации;
- `--file` – имя файла со списком реплицируемых объектов, либо «-» для ввода списка через стандартный поток ввода (stdin);
- `--ignore-errors` – игнорировать ошибки репликации при загрузке нескольких объектов.

Эта команда запускает процесс репликации данных указанных объектов с переданного в параметре `--server` контроллера домена. Для идентификации объектов могут использоваться идентификаторы безопасности (SID), DN или имена учетных записей SAM (samAccountName).

Для передачи списка объектов может использоваться:

- перечисление объектов списком через пробел;
- файл (одна строка соответствует одному объекту);
- stdin (одна строка соответствует одному объекту).

10.2.4.3. Проверка репликации пароля пользователя на сервере RODC

Тестирование репликации пароля пользователя на сервере RODC:

- 1) на обычном контроллере домена (в примере DC1) создать пользователя и добавить его в группу «Allowed RODC Password Replication Group» (пароли пользователей/групп, входящих в группу «Allowed RODC Password Replication Group» разрешено реплицировать на RODC):

```
# samba-tool user create ivanov --given-name='Иван' \
--surname='Иванов' --mail-address='ivanov@test.alt'
```

```
New Password:
```

```
Retype Password:
```

```
User 'ivanov' added successfully
```

```
# samba-tool user setexpiry ivanov --noexpiry
```

```
# samba-tool group addmembers \
```

```
'Allowed RODC Password Replication Group' ivanov
```

```
Added members to group Allowed RODC Password Replication Group
```

- 2) на RODC проверить возможность загрузки кеша пароля, выполнив команду:

```
# samba-tool rodc preload ivanov --server=dc1.test.alt
Replicating DN CN=Иван Иванов,CN=Users,DC=test,DC=alt
Exop on[CN=Иван Иванов,CN=Users,DC=test,DC=alt] objects[1]
linked_values[0]
```

Пример получения билета при отсутствии связи с RWDC (пользователь ivanov есть в кеше RODC, а пользователь kim – нет):

```
$ kinit ivanov
Password for ivanov@TEST.ALT:

$ kinit kim
kinit: A service is not available that is required to process the
request while getting initial credentials
```

10.2.5. Редактирование существующего домена

10.2.5.1. Повышение уровня схемы, функционального уровня домена

Просмотреть текущий уровень домена и леса можно, выполнив команду:

```
# samba-tool domain level show
Domain and forest function level for domain 'DC=test,DC=alt'
Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
```

Для повышения уровня домена необходимо выполнить следующие действия:

- 1) указать функциональный уровень домена, который будет поддерживаться контроллером домена, в параметре `ad dc functional level` файла

`/etc/samba/smb.conf`. Возможные значения:

- 2008_R2 – аналог функционального уровня Windows 2008 R2 (по умолчанию);
- 2012 – аналог функционального уровня Windows 2012;
- 2012_R2 – аналог функционального уровня Windows 2012 R2;
- 2016 – аналог функционального уровня Windows 2016;

2) обновить схему домена, выполнив команду:

```
# samba-tool domain schemaupgrade --schema=<SCHEMA>
```

где SCHEMA – схема, до которой необходимо выполнить обновление (по умолчанию 2019);

3) подготовить функциональный уровень домена, выполнив команду:

```
# samba-tool domain functionalprep --function-level=<FUNCTION_LEVEL>
```

где FUNCTION_LEVEL – функциональный уровень, к которому нужно подготовиться (по умолчанию 2016);

4) указать функциональные уровни домена и леса, выполнив команду:

```
# samba-tool domain level raise --domain-level=<DOMAIN_LEVEL> \
--forest-level=<FOREST_LEVEL>
```

где:

- FOREST_LEVEL – уровень работы леса (возможные значения: 2003, 2008, 2008_R2, 2012, 2012_R2, 2016);

- DOMAIN_LEVEL – уровень работы домена (возможные значения: 2003, 2008, 2008_R2, 2012, 2012_R2, 2016).

Примечание. При установке значения параметра `ad dc functional level` в файле `/etc/samba/smb.conf` вручную, защита от несовпадения функций между контроллерами домена снижается. Поэтому на всех контроллерах домена должна использоваться одна и та же версия Samba, чтобы гарантировать, что поведение, наблюдаемое клиентом, будет одинаковым независимо от того, к какому контроллеру домена осуществляется соединение.

Пример повышения уровня домена до 2016:

- в раздел `[global]` файла `/etc/samba/smb.conf` добавить строку:

```
ad dc functional level = 2016
```

- перезагрузить службу каталогов:

```
# systemctl restart samba.service
```

- обновить схему домена:

```
# samba-tool domain schemaupgrade --schema=2019
```

- подготовить функциональный уровень домена:

```
# samba-tool domain functionalprep --function-level=2016
```

- повысить функциональные уровни домена и леса до 2016:

```
# samba-tool domain level raise --domain-level=2016 --forest-level=2016
```

```
Domain function level changed!
Forest function level changed!
All changes applied successfully!
```

- убедиться, что уровни домена и леса повышены:

```
# samba-tool domain level show
Domain and forest function level for domain 'DC=test,DC=alt'
Forest function level: (Windows) 2016
Domain function level: (Windows) 2016
Lowest function level of a DC: (Windows) 2016
```

10.2.5.2. Включение RFC2307 после разворачивания домена

Примечание. До запуска этой процедуры следует убедиться, что она необходима.


Проверка того, что расширения NIS установлены в домене:

```
# ldbsearch -H /var/lib/samba/private/sam.ldb -s base -b
CN=ybservers,CN=ypServ30,CN=RpcServices,CN=System,DC=test,DC=alt
cn

# record 1
dn:
CN=ybservers,CN=ypServ30,CN=RpcServices,CN=System,DC=test,DC=alt
cn: ybservers

# returned 1 records
# 1 entries
# 0 referrals
```

Если команда `ldbsearch` возвращает одну запись (returned 1 records), расширения NIS установлены и больше ничего делать не нужно.

 Обновление схемы может привести к поломке домена. Прежде чем обновлять схему, необходимо убедиться в наличии рабочей резервной копии.

Для установки расширения NIS необходимо выполнить следующие действия:

1) найти контроллер домена с ролью (FSMO) хозяина схемы:

```
# samba-tool fsmo show | grep SchemaMasterRole
SchemaMasterRole          owner:                               CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
```

В выводе команды показано имя DC, которому принадлежит эта роль.

Все дальнейшие действия следует выполнять на этом DC;

2) остановить службу samba:

```
# systemctl stop samba
```

3) создать копию файла схемы ypServ30.ldif, например:

```
# cp /usr/share/samba/setup/ypServ30.ldif /tmp/
```

4) заменить переменные в скопированном файле LDIF именем домена (DN), именем NetBIOS и доменом NIS вашей установки, например:

```
# sed -i -e 's/\${DOMAINDN}/DC=test,DC=alt/g' -e
's/\${NETBIOSNAME}/DC/g' -e 's/\${NISDOMAIN}/test/g'
/tmp/ypServ30.ldif
```

5) импортировать измененный файл LDIF в локальную базу данных Samba

```
/var/lib/samba/private/sam.ldb:
```

```
# ldbmodify -H /var/lib/samba/private/sam.ldb
/tmp/ypServ30.ldif --option="dsdb:schema update allowed"=true
```

6) в файл /etc/samba/smb.conf в секцию [global] добавить параметр:

```
idmap_ldb:use rfc2307 = yes
```

7) запустить службу каталогов:

```
# systemctl start samba
```

Samba реплицирует обновленную схему на все контроллеры домена в лесу.

10.2.5.3. Изменение DNS бэкенда контроллера домена Active Directory

Samba позволяет переключаться между бэкендом INTERNAL_DNS и BIND9_DLZ на контроллере домена без потери данных.

10.2.5.3.1. Миграция с Samba INTERNAL на BIND9_DLZ

Для переключения с Samba INTERNAL на BIND9_DLZ на контроллере домена необходимо выполнить следующие шаги:

1) установить и настроить DNS-сервер BIND (см.п. 10.2.2.4.1);

2) остановить службу samba:

```
# systemctl stop samba
```

3) выполнить миграцию:

```
# samba_upgradedns --dns-backend=BIND9_DLZ
```

4) отключить модуль SAMBA_INTERNAL в файле smb.conf:

- если в файле нет параметра server services, добавить в секцию global строку:

```
server services = -dns
```

- если в секции `global` есть параметр `server services`, удалить опцию `dns`, например:

```
server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc,
drepl, winbindd, ntp_signd, kcc, dnsupdate
```

5) запустить службу `bind` и сделать ее запускаемой по умолчанию:

```
# systemctl enable --now bind
```

6) запустить службу `samba`:

```
# systemctl start samba
```

10.2.5.3.2. Миграция с BIND9_DLZ на Samba INTERNAL

Для переключения с `BIND9_DLZ` на `Samba INTERNAL` на контроллере домена необходимо выполнить следующие шаги:

1) остановить службу `bind` и убрать ее из автозагрузки:

```
# systemctl disable --now bind
```

2) остановить службу `samba`:

```
# systemctl stop samba
```

3) выполнить миграцию:

```
# samba_upgradedns --dns-backend=SAMBA_INTERNAL
```

4) отключить модуль `BIND9_DLZ` в файле `/etc/samba/smb.conf`:

- если в параметре `server services` есть только опция `-dns`, удалить этот параметр из файла (удалить всю строку):

```
server services = -dns
```

- если в секции `global` есть параметр `server services`, добавить в него опцию `dns`, например:

```
server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc,
drepl, winbindd, ntp_signd, kcc, dnsupdate, dns
```

5) запустить службу `samba`:

```
# systemctl start samba
```

Примечание. Так как `INTERNAL DNS` – это одна из настроек по умолчанию для параметра `server services`, удаление параметра `server services` включает все серверы по умолчанию, включая `DNS-сервер`.

10.2.6. Отладочная информация

10.2.6.1. Настройка уровня журналирования Samba

Дополнительные сведения см. в п. 10.6.14.3.

10.2.6.2. Управление процессами

Для проверки выполнения процессов Samba можно использовать утилиту ps:

```
# ps axf | grep -E "samba|smbd|winbindd"
...
3078 ? S 0:00 /usr/sbin/samba --no-process-group
3091 ? S 0:00 \_ /usr/sbin/samba --no-process-group
3092 ? S 0:00 | \_ /usr/sbin/samba --no-process-group
3096 ? S 0:00 | \_ /usr/sbin/samba --no-process-group
3101 ? Ss 0:00 | \_ /usr/sbin/smbd -D --option=server role
check:inhibit=yes --foreground
3138 ? S 0:00 | \_ /usr/sbin/smbd -D --option=server role
check:inhibit=yes --foreground
3139 ? S 0:00 | \_ /usr/sbin/smbd -D --option=server role
check:inhibit=yes --foreground
3149 ? S 0:00 | \_ /usr/sbin/smbd -D --option=server role
check:inhibit=yes --foreground
3150 ? S 0:00 | \_ /usr/sbin/smbd -D --option=server role
check:inhibit=yes --foreground
...
3127 ? Ss 0:00 | \_ /usr/sbin/winbindd -D --option=server role
check:inhibit=yes --foreground
3140 ? S 0:00 | \_ /usr/sbin/winbindd -D --option=server role
check:inhibit=yes --foreground
...
```

Все процессы samba, smbd и winbindd должны быть дочерними процессами одного процесса samba.

Если структура процесса не отображается:

- следует проверить файлы журнала Samba. Для подробного вывода можно увеличить уровень журнала (см. п. 10.6.14.3);
- можно запустить Samba в интерактивном режиме и посмотреть на результат:

```
# samba -i
```

10.2.6.3. DNS

10.2.6.3.1. Устранение неполадок, связанных с серверной частью DNS

10.2.6.3.1.1. Внутренний DNS-сервер Samba (SAMBA_INTERNAL)

Если клиенты не могут разрешать записи из зоны DNS AD, необходимо убедиться, что на клиенте указан IP-адрес DNS-сервера, способного разрешать зону AD DNS.

Если конфигурация клиента правильная, следует убедиться, что DNS-сервер Samba работает.

Если DNS-сервер Samba не запускается, необходимо убедиться, что ни один другой процесс не использует TCP- и UDP-порт 53:

- проверить файлы журнала Samba на наличие ошибок, связанных с DNS;
- убедиться, что никакой другой процесс не прослушивает TCP- и UDP-порт 53, например:

```
# ss -tulpn | grep ":53"
```

Если порт 53 занят другим процессом, необходимо:

- остановить службу, прослушивающую порт 53, и отключить ее автоматический запуск во время загрузки;
- перезапустить Samba.

10.2.6.3.1.2. Samba с BIND9_DLZ

Каталог `/var/lib/samba/bind-dns` создается только в том случае, если произошло одно из следующих трех событий:

- при создании контроллера домена использовался параметр `--dns-backend=BIND9_DLZ`;
- при подключении к домену использовался параметр `--dns-backend=BIND9_DLZ`;
- домен был обновлен до Bind9 с помощью команды `samba_upgradedns` и опции `--dns-backend=BIND9_DLZ`.

10.2.7. Удаление контроллера домена

В некоторых ситуациях необходимо навсегда удалить контроллер домена из домена. Если для обычного участника домена достаточно просто удалить соответствующую учетную запись, то чтобы удалить контроллер из домена требуется понизить его роль (demoting).

Если роль контроллера домена будет понижена неправильно, домен может стать нестабильным. Например:

- могут начаться сбои репликации;

- оставшиеся контроллеры домена могут замедлять свою работу из-за таймаутов и неудачных попыток репликации;
- вход в систему доменных пользователей может завершиться ошибкой или занять больше времени.

10.2.7.1. Понижение роли онлайн-контроллера домена

Если удаляемый контроллер домена все еще работает правильно, для понижения его роли необходимо выполнить следующие действия (в примере понижается роль DC3):

- 1) авторизоваться на контроллере домена под локальным пользователем;
- 2) убедиться, что контроллер не владеет никакими ролями FSMO:

```
# samba-tool fsmo show
SchemaMasterRole          owner:          CN=NTDS
Settings, CN=DC1, CN=Servers, CN=Default-First-Site-
Name, CN=Sites, CN=Configuration, DC=test, DC=alt
InfrastructureMasterRole  owner:          CN=NTDS
Settings, CN=DC2, CN=Servers, CN=Default-First-Site-
Name, CN=Sites, CN=Configuration, DC=test, DC=alt
RidAllocationMasterRole  owner:          CN=NTDS
Settings, CN=DC1, CN=Servers, CN=Default-First-Site-
Name, CN=Sites, CN=Configuration, DC=test, DC=alt
PdcEmulationMasterRole   owner:          CN=NTDS
Settings, CN=DC1, CN=Servers, CN=Default-First-Site-
Name, CN=Sites, CN=Configuration, DC=test, DC=alt
DomainNamingMasterRole   owner:          CN=NTDS
Settings, CN=DC1, CN=Servers, CN=Default-First-Site-
Name, CN=Sites, CN=Configuration, DC=test, DC=alt
DomainDnsZonesMasterRole  owner:          CN=NTDS
Settings, CN=DC1, CN=Servers, CN=Default-First-Site-
Name, CN=Sites, CN=Configuration, DC=test, DC=alt
ForestDnsZonesMasterRole  owner:          CN=NTDS
Settings, CN=DC1, CN=Servers, CN=Default-First-Site-
Name, CN=Sites, CN=Configuration, DC=test, DC=alt
```

Если контроллеру домена принадлежит одна или несколько ролей FSMO, передать их другому контроллеру домена;

- 3) вывести objectGUID контроллера домена:

```
#          ldbsearch          -H          /var/lib/samba/private/sam.ldb
'(invocationId=*)' --cross-ncs objectguid | grep -A1 DC3
dn:  CN=NTDS  Settings, CN=DC3, CN=Servers, CN=Default-First-Site-
Name, CN=Sites, CN=Configuration, DC=test, DC=alt
objectGUID: 512f03b4-7042-434d-93c0-61dd6a2ea895
```

Для того чтобы убедиться, что все записи DNS были удалены после понижения роли контроллера домена, необходимо знать имя хоста, IP-адрес и objectGUID контроллера домена;

4) понизить DC:

```
# samba-tool domain demote -Uadministrator
Using dcl.test.alt as partner server for the demotion
Password for [TEST\administrator]:
Deactivating inbound replication
Asking partner server dcl.test.alt to synchronize from us
Changing userControl and container
Removing Sysvol reference: CN=DC3,CN=Enterprise,CN=Microsoft
System Volumes,CN=System,CN=Configuration,DC=test,DC=alt
Removing Sysvol reference: CN=DC3,CN=test.alt,CN=Microsoft
System Volumes,CN=System,CN=Configuration,DC=test,DC=alt
Removing Sysvol reference: CN=DC3,CN=Domain System Volumes
(SYSVOL share),CN=File Replication
Service,CN=System,DC=test,DC=alt
Removing Sysvol reference: CN=DC3,CN=Topology,CN=Domain System
Volume,CN=DFSR-GlobalSettings,CN=System,DC=test,DC=alt
updating ForestDnsZones.test.alt keeping 2 values, removing 1
values
updating test.alt keeping 6 values, removing 1 values

...
Demote successful
```

5) остановить службу samba:

```
# systemctl stop samba
```

6) если этот контроллер работал, как доменный сервер DNS:

- остановить службу DNS:

```
# systemctl stop bind
```

- убедиться, что члены домена и контроллеры домена больше не используют этот хост для разрешения зон DNS.

10.2.7.2. Понижение автономного контроллера домена

В определенных ситуациях, например, при сбое оборудования, из домена необходимо удалить контроллер домена, который больше недоступен. В этом случае понизить уровень контроллера домена можно на оставшемся работающем контроллере домена Samba.

ВАЖНО

Эта процедура должна выполняться только в том случае, если контроллер домена, который нужно понизить, больше не подключен к домену, и его нельзя понизить так, как описано в п. 10.2.7.1. Это гарантирует, что все изменения, такие как изменения пароля, будут реплицированы на другой контроллер домена. В противном случае такие изменения будут потеряны. Список изменений можно получить с помощью Samba-инструмента `ldapcmp`. При описанной ниже процедуре все изменения (например, изменения паролей) не будут реплицированы на работающий DC.

ВАЖНО

Нельзя понизить статус автономного удаленного контроллера домена с контроллера домена, на котором работает Samba 4.4 или более ранней версии.

Для понижения статуса неработающего контроллера домена необходимо выполнить следующие действия (в примере понижается статус DC3):

- 1) авторизоваться на работающем контроллере домена;
- 2) убедиться, что понижаемый контроллер не владеет никакими ролями

FSMO:

```
# samba-tool fsmo show
```

```
SchemaMasterRole          owner:          CN=NTDS
Settings, CN=DC1, CN=Servers, CN=Default-First-Site-
Name, CN=Sites, CN=Configuration, DC=test, DC=alt
InfrastructureMasterRole  owner:          CN=NTDS
Settings, CN=DC2, CN=Servers, CN=Default-First-Site-
Name, CN=Sites, CN=Configuration, DC=test, DC=alt
RidAllocationMasterRole   owner:          CN=NTDS
Settings, CN=DC1, CN=Servers, CN=Default-First-Site-
Name, CN=Sites, CN=Configuration, DC=test, DC=alt
PdcEmulationMasterRole   owner:          CN=NTDS
Settings, CN=DC1, CN=Servers, CN=Default-First-Site-
Name, CN=Sites, CN=Configuration, DC=test, DC=alt
DomainNamingMasterRole   owner:          CN=NTDS
Settings, CN=DC1, CN=Servers, CN=Default-First-Site-
Name, CN=Sites, CN=Configuration, DC=test, DC=alt
DomainDnsZonesMasterRole  owner:          CN=NTDS
Settings, CN=DC1, CN=Servers, CN=Default-First-Site-
Name, CN=Sites, CN=Configuration, DC=test, DC=alt
ForestDnsZonesMasterRole  owner:          CN=NTDS
Settings, CN=DC1, CN=Servers, CN=Default-First-Site-
Name, CN=Sites, CN=Configuration, DC=test, DC=alt
```

Если понижаемому контроллеру домена принадлежит одна или несколько ролей FSMO, захватить их локальным контроллером домена;

3) убедиться, что понижаемый контроллер домена отключен;

4) вывести objectGUID контроллера домена:

```
# ldbsearch -H /var/lib/samba/private/sam.ldb \
 '(invocationId=*)' --cross-ncs objectguid | grep -A1 DC3
dn: CN=NTDS Settings,CN=DC3,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
objectGUID: 512f03b4-7042-434d-93c0-61dd6a2ea895
```

Для того чтобы убедиться, что все записи DNS были удалены после понижения роли контроллера домена, необходимо знать имя хоста, IP-адрес и objectGUID контроллера домена;

5) понизить статус удаленного контроллера домена:

```
# samba-tool domain demote --remove-other-dead-server=DC3
```

б) если пониженный контроллер работал как доменный сервер DNS, убедиться, что члены домена и контроллеры домена больше не используют этот хост для разрешения зон DNS.

ВАЖНО

Не следует подключать к сети контроллер, выведенный по данной процедуре. Иначе домен станет несогласованным.

10.2.7.3. Проверка

Действия, описанные в этом разделе, предназначены только для проверки и ручного удаления оставшихся записей, если процесс понижения контроллера не удался.

На машине, введенной в домен, запустить модуль удаленного управления базой данных конфигурации (ADMC) (подробнее см. п. 10.4.5). Выбрать запись Domain Controllers и убедиться, что пониженный контроллер домена был удален (рис. 217).

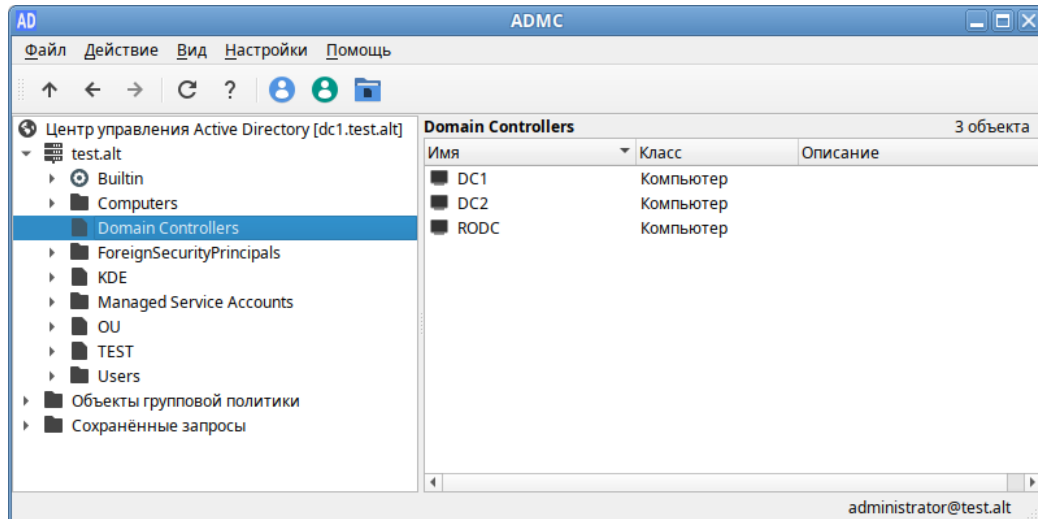


Рис. 217 –ADMC. Просмотр списка контроллеров домена

Проверить, что контроллер домена был понижен, можно также в RSAT (см. п. 10.4.2.3). Для этого на машине Windows введенной в домен:

- 1) открыть приложение «Active Directory – пользователи и компьютеры», перейти к записи «Контроллеры домена» и убедиться, что пониженный контроллер домена был удален (рис. 218).

Если запись все еще присутствует в списке, ее можно удалить вручную, выбрав в контекстном меню записи пункт «Удалить»;

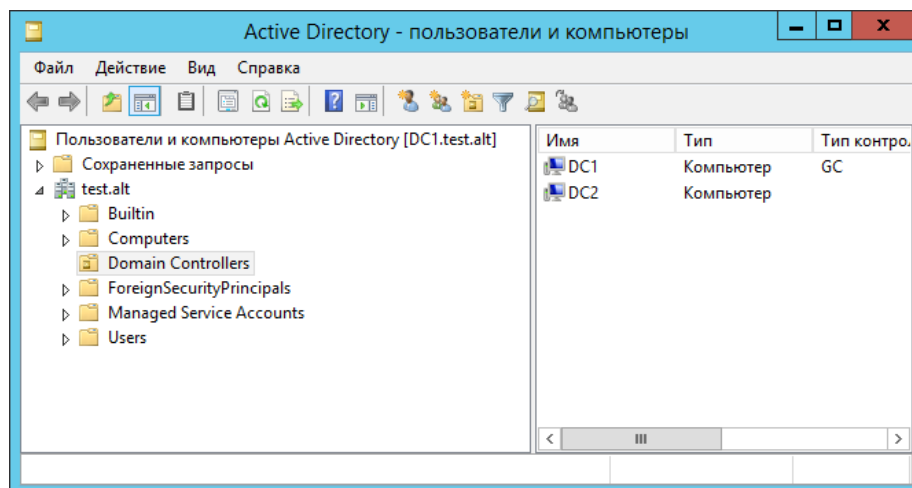


Рис. 218 – Окно приложения «Active Directory – пользователи и компьютеры»

- 2) открыть приложение «Active Directory – сайты и службы», и убедиться, что контроллер домена с пониженным статусом больше не указан ни в одной записи сайта Active Directory (рис. 219).

Если запись все еще присутствует в списке, ее можно удалить вручную, выбрав в контекстном меню записи пункт «Удалить»;

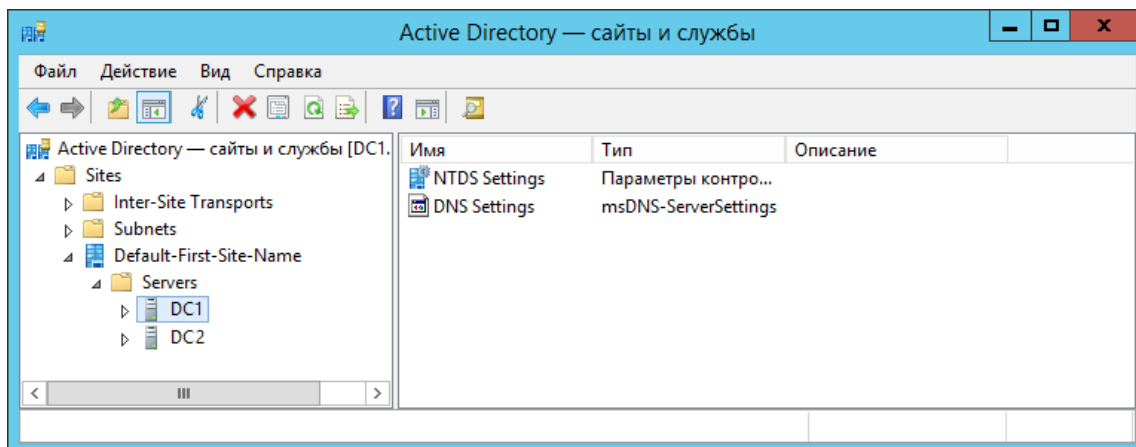


Рис. 219 – Окно приложения «Active Directory – сайты и службы»

3) открыть приложение «DNS», и убедиться, что имя хоста, IP-адрес и objectGUID контроллера домена больше не используются ни в одной записи DNS в любой зоне AD DNS (рис. 220).

Если записи все еще присутствуют в списке, их можно удалить вручную, выбрав в контекстном меню записи пункт «Удалить».

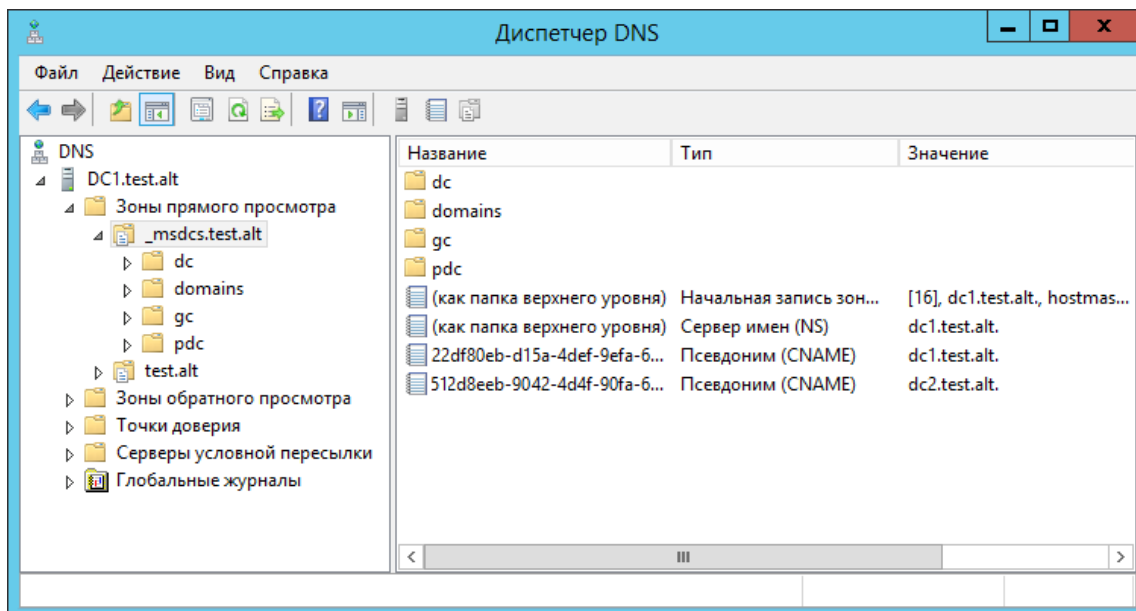


Рис. 220 – Окно «Диспетчер DNS»

10.3. Клиенты «Альт Домена»

Клиентами «Альт Домена» могут быть серверы и рабочие станции под управлением Windows, Linux («Альт», Astra Linux) и других операционных систем, поддерживающих стандартные протоколы LDAP, Kerberos, DNS и SMB.

ВАЖНО

Аутентификация в домене рабочих станций под управлением Astra Linux и других ОС под управлением Linux, возможна, но поддержка механизмов применения групповых политик в таких ОС ограничена и требует соответствующее ПО, не входящее в комплект «Альт Домен».

10.3.1. SSSD vs Winbind

Существует несколько способов включения операционных систем на базе ядра Linux в «Альт Домен». В этом разделе описаны функции и возможности двух вариантов интеграции: решение на основе Samba Winbind и решение на базе SSSD.

Машины под управлением ОС «Альт» рекомендуется вводить в «Альт Домен» с помощью SSSD, но есть несколько исключений:

- 1) если в сети уже развернуты системы Linux, которые уже используют Samba Winbind для целей интеграции;
- 2) если используется AD с включенным протоколом NTLM (так как SSSD не поддерживает протокол NTLM);
- 3) если SSSD не поддерживает определенную функцию, которую поддерживает Winbind (например, SSSD не поддерживает доверительные отношения между лесами при прямом подключении к «Альт Домен»).

Ниже рассмотрены преимущества и недостатки интеграции на основе Samba Winbind (рис. 221) и на базе SSSD (рис. 222).

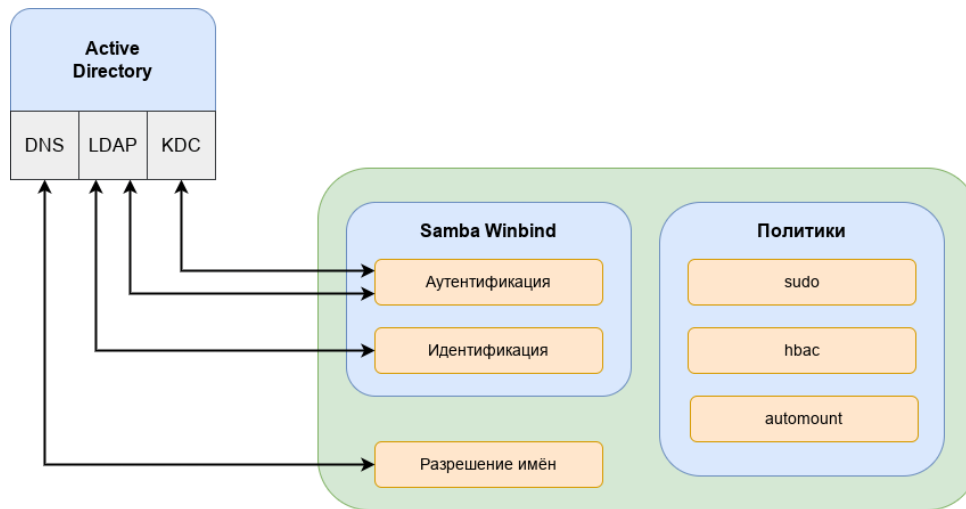


Рис. 221 – Схема интеграции на основе Samba Winbind

Преимущества варианта интеграции с использованием Samba Winbind:

- Samba Winbind эмулирует клиент Windows в системе Linux и использует преимущества собственных протоколов Windows и расширений протокола LDAP;
- Winbind понимает концепцию доменов и лесов, а также работает с доверием между доменами и лесами;
- Winbind может обнаруживать серверы, используя DNS;
- Winbind может переключиться на другой сервер, если контроллер домена AD становится недоступным;
- Winbind может динамически выполнять сопоставление идентификаторов на основе идентификаторов объектов «Альт Домен» (SID) или использовать атрибуты POSIX, хранящиеся в «Альт Домен» (если эти расширения были загружены);
- Winbind хорошо интегрируется с клиентом Samba FS и CIFS;
- безопасность соединения основана на идентификации клиентской системы и ключах Kerberos, выданных этой системе.

Ограничения Samba Winbind:

- политики не управляются централизованно и должны распространяться вне группы;
- может подключаться только к «Альт Домен».

SSSD – это группа служб, которые являются частью ядра операционной системы Linux и работают вместе для обеспечения аутентификации, поиска удостоверений и возможностей управления доступом для системы Linux. SSSD может взаимодействовать с «Альт Домен», FreeIPA, MS AD или любыми другими стандартными реализациями сервера LDAP и/или Kerberos (рис. 222, рис. 223).

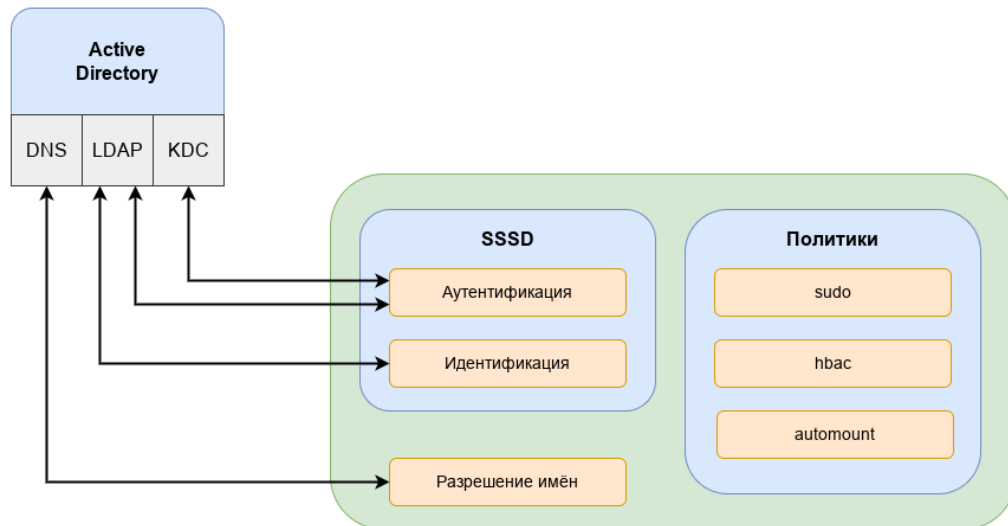


Рис. 222 – Схема интеграции на базе SSSD

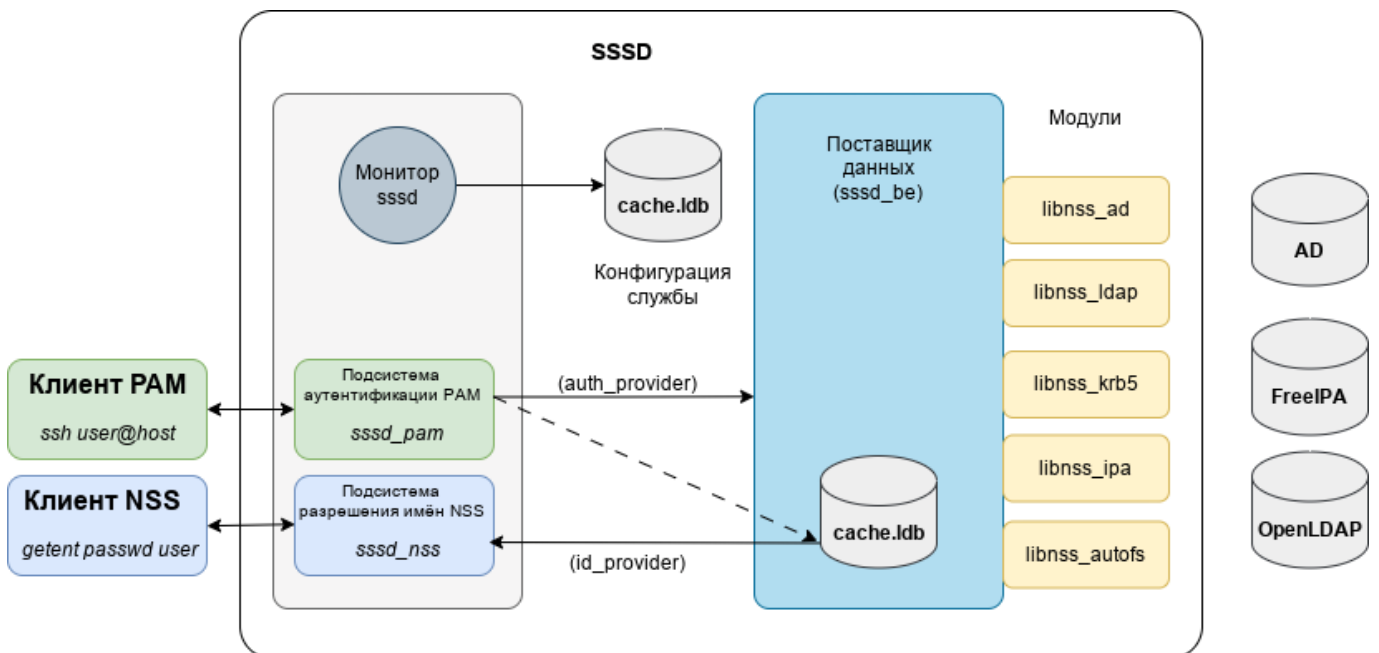


Рис. 223 – Схема интеграции конфигураций на базе SSSD

Единственным серьезным ограничением для интеграции с использованием SSSD является поддержка (старого) протокола NTLM. SSSD не реализует этот протокол, потому что по современным стандартам NTLM больше не является безопасным для развертывания. Наилучшей практикой является отказ от использования NTLM.

Преимущества SSSD (рис. 223):

- возможность загрузки и применения политик управления доступом на основе хоста с использованием объектов групповой политики, управляемых в «Альт Домен»;
- может взаимодействовать с разными источниками идентификации, а не только с «Альт Домен»;
- поддерживает очистку DNS (т. е. обнаруживает, были ли удалены или обновлены записи DNS для серверов);
- предоставляет расширенные интерфейсы идентификации на локальной шине сообщений (D-Bus). Этот интерфейс можно использовать для лучшей интеграции приложений, работающих в ОС Linux, с корпоративными источниками идентификации, такими как AD и FreeIPA.

Сравнение Winbind и SSSD представлено в таблице 15.

Т а б л и ц а 15 – Сравнение Winbind и SSSD

Категория	Описание	Winbind	SSSD
Аутентификация	Проверка подлинности с использованием Kerberos	Да	Да
	Проверка подлинности LDAP	Да	Да
	Поддержка нескольких доменов AD	Да	Да
	Поддержка лесов AD	Да	Да
	Поддержка гетерогенных сетей AD/FreeIPA	Нет	Да
Безопасность	Простота настройки безопасной конфигурации	Нет	Да
	Система имеет идентификатор и ее ключ используется для защиты доступа к центральному серверу	Да	Да
	Поддержка NTLM	Да	Нет
Поиск и сопоставление идентификаторов	Динамическое сопоставление идентификаторов AD SID	Да	Да
	Использование преимуществ конкретных расширений и протоколов AD	Да	Да

Окончание таблицы 15

Категория	Описание	Winbind	SSSD
DNS	Обновление и очистка DNS AD	Нет	Да
	Поддержка сайтов AD DNS	Да	Да
Обмен файлами	Интеграция с Samba FS	Да	Да
	Интеграция с клиентом CIFS	Да	Да
Служба печати	Сервер печати CUPS с использованием Kerberos	Да	Да
Политики	Централизованное управление контролем доступа на основе хоста через GPO	Нет	Да
Интеграция с другими сервисами и приложениями	Интеграция с основными утилитами, такими как SSH, sudo, automount	Нет	Да
	Расширенные интерфейсы идентификации по локальной шине сообщений D-Bus	Нет	Да
	Специальные функции для приложений (Docker, Cockpit, GSS Proxy и др.)	Нет	Да

10.3.2. Подготовка системы к вводу в домен

10.3.2.1. Установка пакетов

Установить пакет task-auth-ad-sssd:

```
# apt-get install task-auth-ad-sssd
```

Примечание. Этот шаг можно пропустить, если при установке ОС на этапе «Установка системы» был выбран профиль «Клиент Альт Домен» (рис. 224).

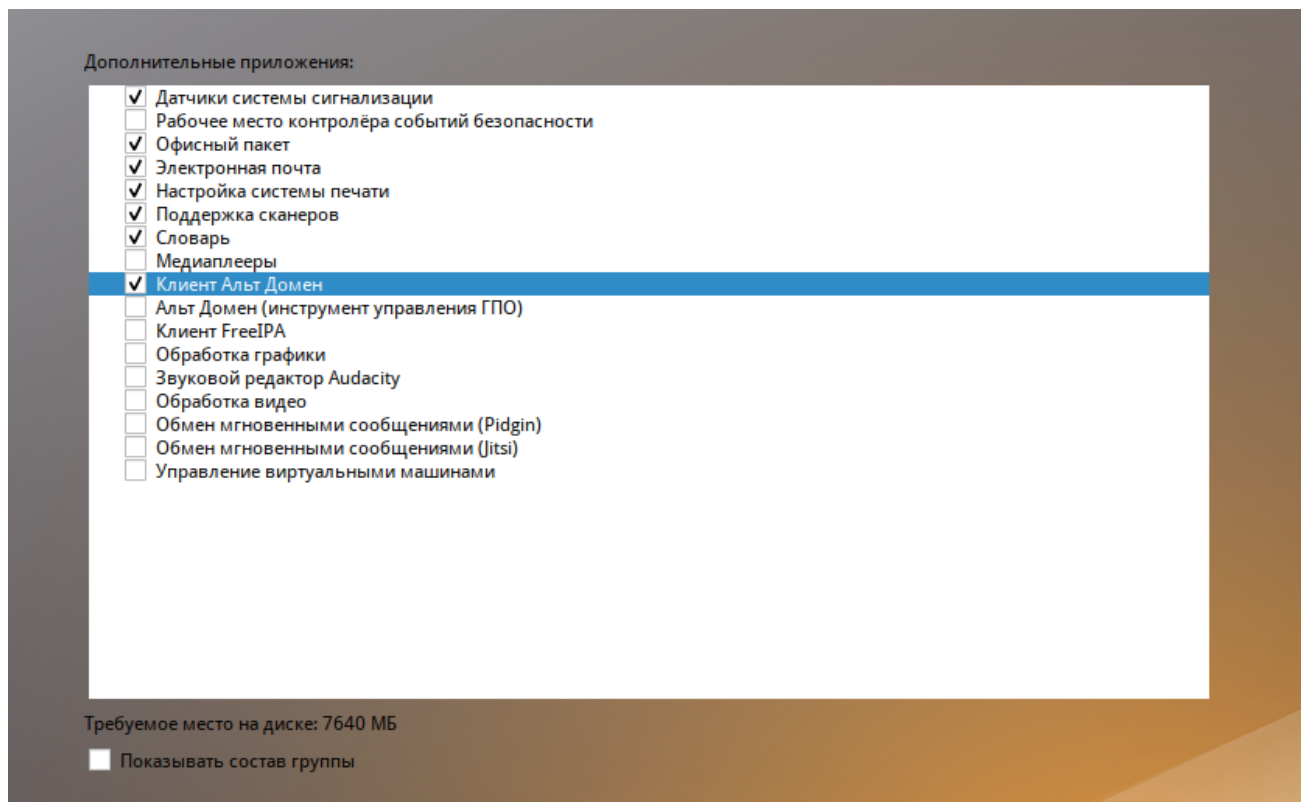


Рис. 224 – Выбор профиля «Клиент Альт Домен» при установке ОС

10.3.2.2. Синхронизация времени

Синхронизация времени с контроллером домена производится автоматически.

10.3.2.3. Настройка DNS

«Альт Домен» использует DNS для обнаружения других контроллеров домена и служб, таких как Kerberos. Поэтому, члены и серверы домена «Альт Домен» должны иметь возможность разрешать зоны DNS.

Для ввода компьютера в домен, на нем должен быть доступен сервер DNS, имеющий записи про контроллер домена. При получении IP-адреса по DHCP данные о сервере DNS также должны быть получены от DHCP-сервера.

Ниже приведен пример настройки сетевого интерфейса со статическим IP-адресом.

10.3.2.3.1. Настройка клиентов для использования DNS-серверов вручную

Настройку сети можно выполнить как в графическом интерфейсе, так и в консоли.

В ЦУС в разделе «Сеть» → «Ethernet интерфейсы» задать имя компьютера, указать в поле «DNS-серверы» DNS-сервер домена и в поле «Домены поиска» – домен для поиска (рис. 225).

Примечание. После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

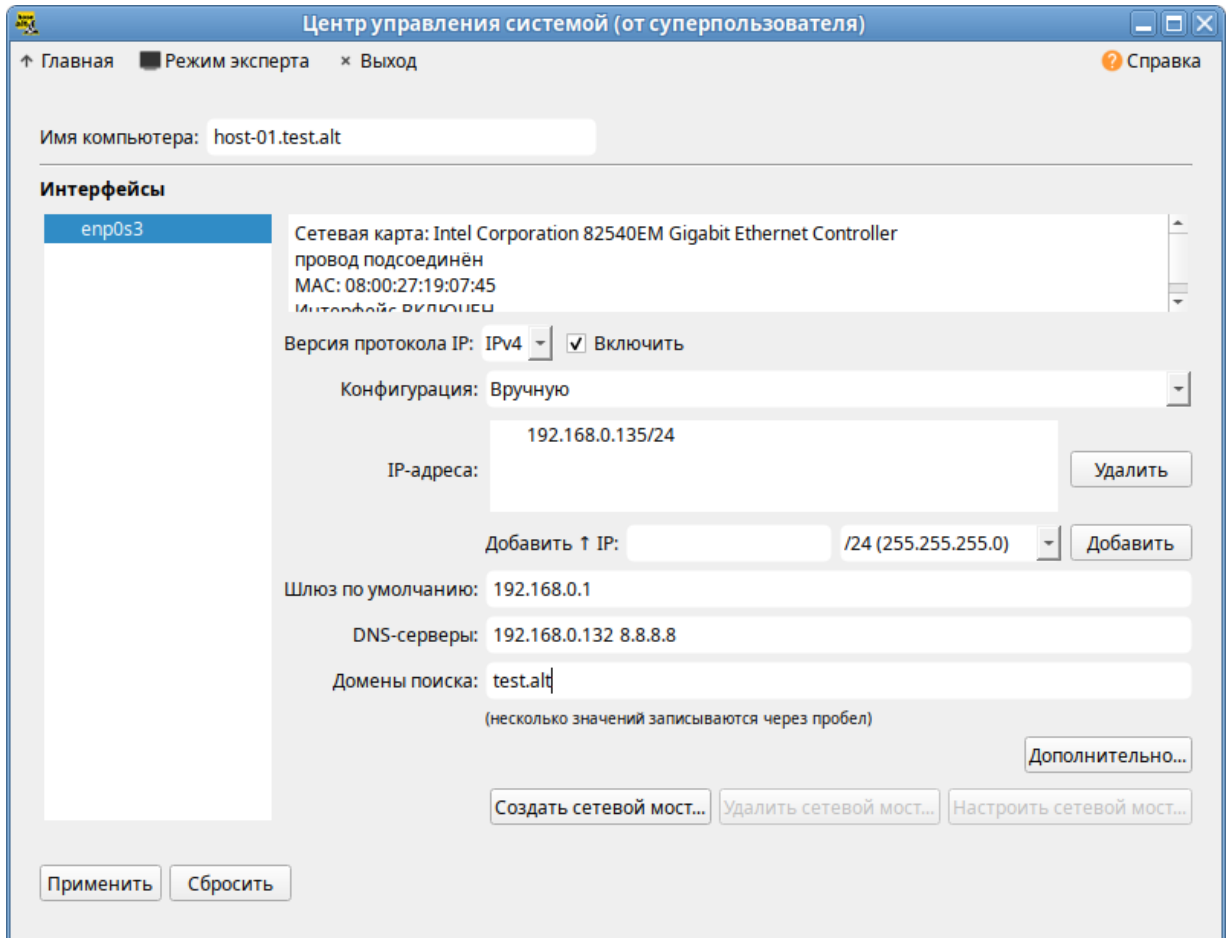


Рис. 225 – Окно «Центр управления системой»

В консоли:

- 1) задать имя компьютера:

```
# hostnamectl set-hostname host-01.test.alt
```

- 2) в качестве первичного DNS должен быть указан DNS-сервер домена.

Для этого необходимо создать файл

`/etc/net/ifaces/enp0s3/resolv.conf` со следующим содержимым:

```
nameserver 192.168.0.132
```

где `192.168.0.132` – IP-адрес DNS-сервера домена;

- 3) указать службе `resolvconf` использовать DNS контроллера домена и домен

для поиска. Для этого в файле `/etc/resolvconf.conf`

добавить/отредактировать следующие параметры:

```
interface_order='lo lo[0-9]* lo.* enp0s3'
```

```
search_domains=test.alt
```

где `enp0s3` – интерфейс, на котором доступен контроллер домена,
`test.alt` – домен;

4) обновить DNS адреса:

```
# resolvconf -u
```

Примечание. После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

В результате выполненных действий в файле `/etc/resolv.conf` должны появиться строки:

```
search test.alt
nameserver 192.168.0.132
```

10.3.2.3.2. Проверка разрешения DNS

Для проверки того, что настройки DNS верны и машины могут разрешать IP-адреса и имена, можно использовать команды `nslookup` и `host`.

Прямой поиск:

```
# nslookup dc1.test.alt
Server:          192.168.0.132
Address: 192.168.0.132#53

Name:   dc1.test.alt
Address: 192.168.0.132

# host dc1.test.alt
dc1.test.alt has address 192.168.0.132
```

Обратный поиск:

```
# nslookup 192.168.0.132
132.0.168.192.in-addr.arpa    name = dc1.alt.test.

# host 192.168.0.132
132.0.168.192.in-addr.arpa domain name pointer dc1.alt.test.
```

Следует обратить внимание, что в «Альт Домен» обратная зона не настраивается автоматически.

«Альт Домен» использует записи SRV для поиска служб, таких как Kerberos и LDAP. Проверка разрешения SRV-записей:

```
$ nslookup
> set type=SRV
> _ldap._tcp.test.alt
```

ЛКНВ.11100-01 90 03

```
Server:      192.168.0.132
Address:    192.168.0.132#53
```

```
_ldap._tcp.test.alt service = 0 100 389 dc2.test.alt.
_ldap._tcp.test.alt service = 0 100 389 dc1.test.alt.
> exit
```

или:

```
$ host -t SRV _ldap._tcp.test.alt
_ldap._tcp.test.alt has SRV record 0 100 389 dc1.test.alt.
_ldap._tcp.test.alt has SRV record 0 100 389 dc2.test.alt.
```

10.3.3. Присоединение к домену в роли участника

10.3.3.1. Параметры команды system-auth

Для ввода клиентских машин в «Альт Домен», в дистрибутивах ОС Альт СП

используется команда `system-auth`:

```
# system-auth <Действие> <Опции>
```

В таблице 16 приведено описание опций этой команды.

Т а б л и ц а 16 – Опции команды `system-auth`

Параметр	Описание
Действие	
<code>status</code>	Показать текущую схему аутентификацию
<code>list</code>	Вывести список доступных схем аутентификации
<code>write</code>	Установить заданные параметры аутентификации
Опция	
<code>-d</code>	Включить отладку
<code>--winbind</code>	Использовать Samba Winbind для подключения системы к домену (если этот параметр не указан, будет использован SSSD)
<code>--gpo</code>	Включить групповые политики на машине
<code>--createcomputer=OU/SubOU</code>	Субконтейнер в домене (организационная единица/подразделение), куда будет помещена машина при вводе в домен
<code>--windows2003</code>	Ввести станцию в домен windows 2003
<code>--version</code>	Вывести версию программы

Примеры использования:

- вывести текущую схему аутентификации:

```
# system-auth status
ad TEST.ALT HOST-01 TEST
```

- использовать локальную аутентификацию:

```
# system-auth write local
```

- использовать доменную аутентификацию (по умолчанию используется билет Kerberos):

```
# system-auth write ad <Домен> <Имя компьютера> <Рабочая группа>
<Имя пользователя> [<Пароль>] [--windows2003] [--
createcomputer="COMPUTEROU/SubCOMPUTEROU/SubSubCOMPUTEROU"] [--
winbind] [--gpo]
```

10.3.3.2. Подключение к домену с помощью SSSD

В этом разделе описывается использование демона служб безопасности системы (SSSD) для подключения системы к «Альт Домен».

SSSD используется для доступа к пользовательскому каталогу для аутентификации и авторизации через общую структуру с кэшированием пользователей, чтобы разрешить автономный вход в систему. SSSD легко настраивается. Он обеспечивает интеграцию подключаемых модулей аутентификации (PAM) и службы переключения имен (NSS), базу данных для хранения локальных пользователей, а также расширенных пользовательских данных, полученных с центрального сервера.

Дополнительные ресурсы:

- man realm;
- man sssd-ad;
- man sssd.

10.3.3.2.1. Ввод в домен в командной строке

Для ввода компьютера в домен необходимо выполнить команду:

```
# system-auth write ad test.alt host-01 test 'administrator' 'Pa$$word'
Joined 'HOST-01' to dns domain 'test.alt'
```

где:

- test.alt – имя домена;
- host-01 – имя компьютера, вводимого в домен;
- test – рабочая группа;
- administrator – имя пользователя, имеющего право вводить машины в домен;
- Pa\$\$word – пароль пользователя, имеющего право вводить машины в домен.

Перезагрузить рабочую станцию для применения всех настроек.

10.3.3.2.2. Ввод в домен в ЦУС

Для ввода компьютера в домен в ЦУС необходимо выбрать пункт «Пользователи» → «Аутентификация» (пакет alterator-auth).

В окне модуля «Аутентификация» следует выбрать пункт «Домен Active Directory», заполнить поля («Домен», «Рабочая группа», «Имя компьютера»), выбрать пункт «SSSD» (в единственном домене) и нажать кнопку «Применить» (рис. 226).

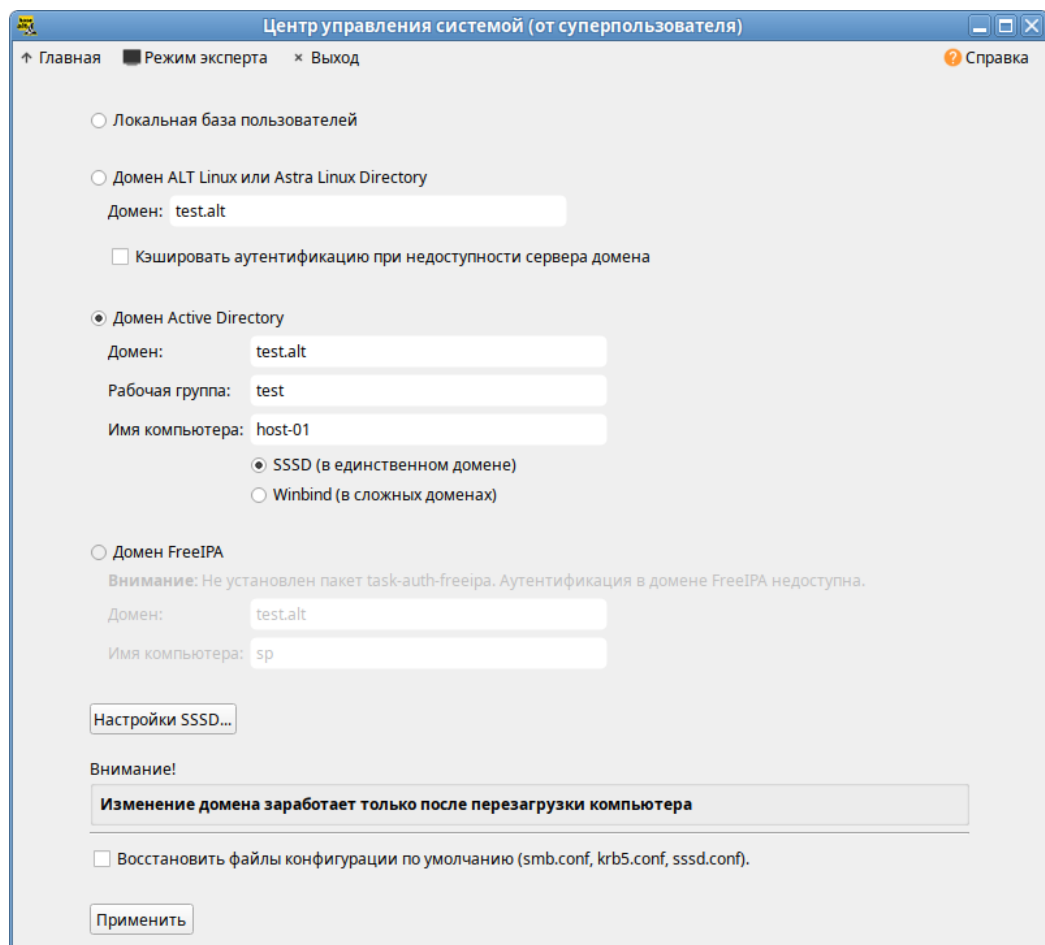


Рис. 226 – Окно модуля «Аутентификация»

В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку «ОК» (рис. 227).

При успешном подключении к домену, отобразится соответствующая информация (рис. 228).

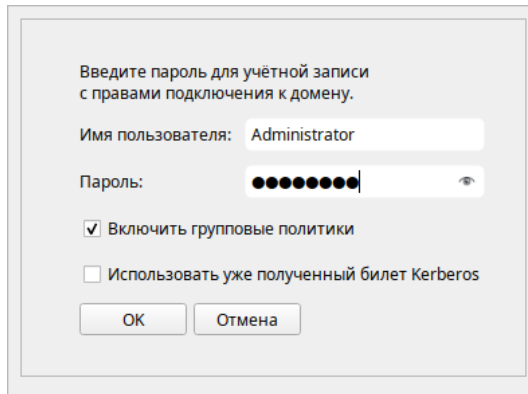


Рис. 227 – Окно ввода имени пользователя и пароля

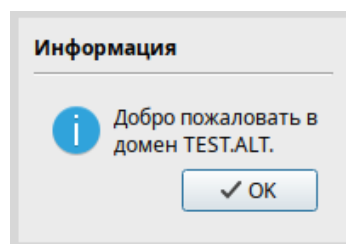


Рис. 228 – Информационное окно

Примечание. Если на машине установлен пакет `alterator-grupdate`, при подключении машины к домену можно включить групповые политики. Для включения групповых политик необходимо в окне ввода учетных записей пользователя с правами подключения к домену отметить пункт «Включить групповые политики» (рис. 227).

Перезагрузить рабочую станцию для применения всех настроек.

10.3.3.2.3. Проверка результатов присоединения

Проверка корректности подключения:

- 1) для проверки возможности поиска доменных пользователей отобразить сведения о пользователе домена (`ivanov` – пользователь в домене):

```
# getent passwd ivanov
ivanov:*:1187401105:1187400513:Иван
Иванов:/home/TEST.ALT/ivanov:/bin/bash
```

- 2) проверить возможность получения информации о домене:

```
# net ads info
LDAP server: 192.168.0.132
LDAP server name: dc1.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
```

```
LDAP port: 389
Server time: Ср, 27 мар 2024 10:36:51 EET
KDC server: 192.168.0.132
Server time offset: 2
Last machine account password change: Ср, 20 мар 2024 11:13:27
EET
```

3) проверить, действителен ли пароль учетной записи компьютера:

```
# net ads testjoin
Join is OK
```

Примечание. Список пользователей можно посмотреть на сервере командой:

```
# samba-tool user list
```

Примечание. О настройке SSSD см. п. 10.6.14 и п. 10.5.5.2.

10.3.3.3. Подключение к домену с использованием Winbind

В этом разделе описывается использование Samba Winbind для подключения системы к «Альт Домен».

Дополнительные ресурсы:

- man realm;
- man winbindd.

10.3.3.3.1. Ввод в домен в командной строке

Для ввода компьютера в домен необходимо выполнить команду:

```
# system-auth write ad test.alt host-02 test 'administrator'
'Pa$$word' --winbind
Joined 'HOST-02' to dns domain 'test.alt'
```

где:

- test.alt – имя домена;
- host-02 – имя компьютера, вводимого в домен;
- test – рабочая группа;
- administrator – имя пользователя, имеющего право вводить машины в домен;
- Pa\$\$word – пароль пользователя, имеющего право вводить машины в домен.

Перезагрузить рабочую станцию для применения всех настроек.

10.3.3.3.2. Ввод в домен в ЦУС

Для ввода компьютера в домен в ЦУС необходимо выбрать пункт «Пользователи» → «Аутентификация» (пакет alterator-auth).

В окне модуля «Аутентификация» следует выбрать пункт «Домен Active Directory», заполнить поля («Домен», «Рабочая группа», «Имя компьютера»), выбрать пункт «Winbind (в сложных доменах)» и нажать кнопку «Применить» (рис. 229).

В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку «ОК» (рис. 230).

При успешном подключении к домену отобразится соответствующая информация (рис. 231).

Перезагрузить рабочую станцию для применения всех настроек.

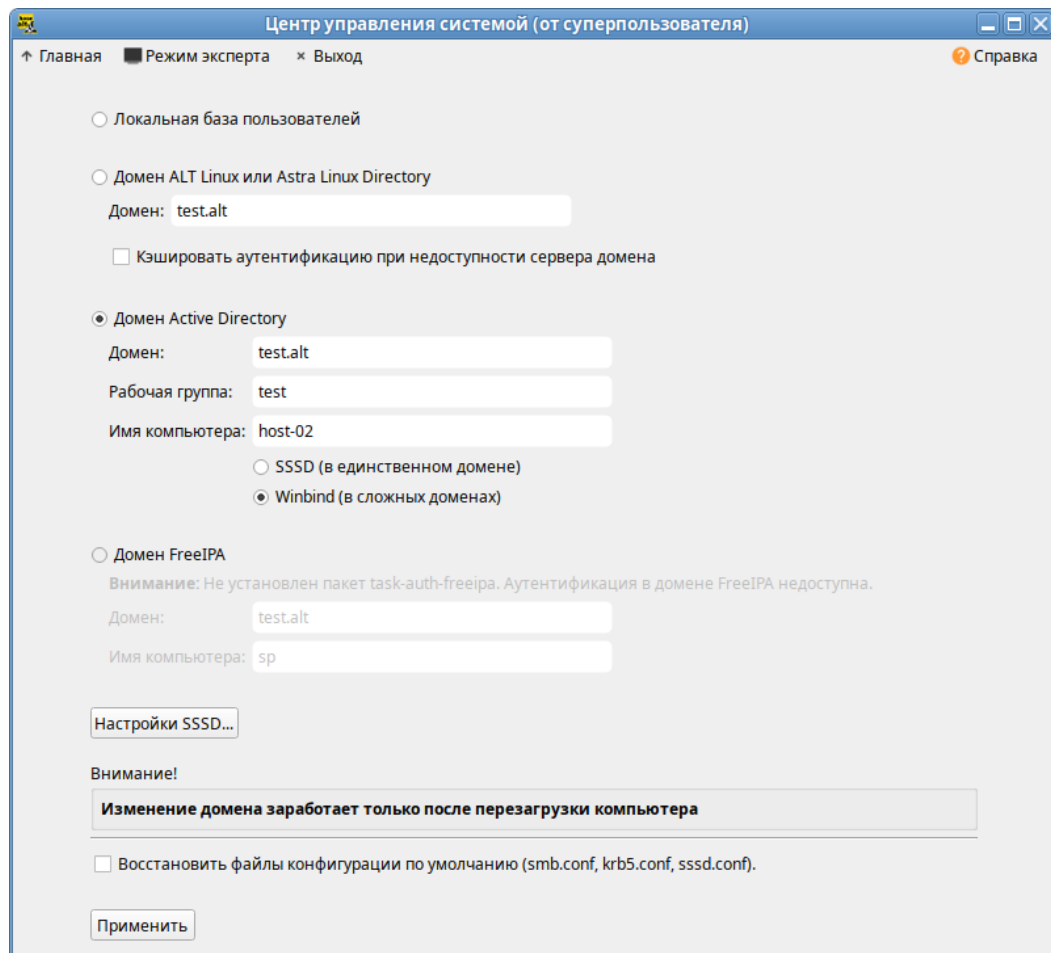


Рис. 229 – Ввод в домен в «Центр управления системой»

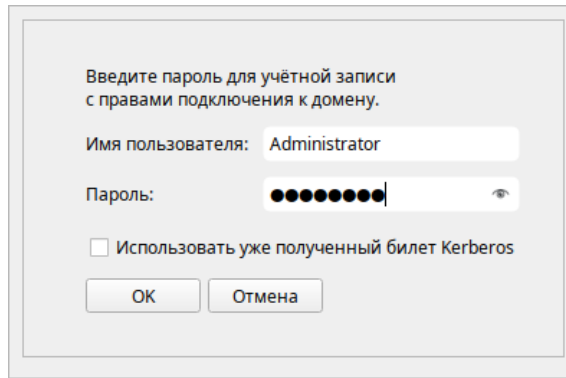


Рис. 230 – Окно ввода имени пользователя и пароля

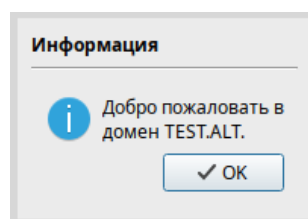


Рис. 231 – Информационное окно

10.3.3.3.3. Проверка результатов присоединения

Проверка корректности подключения:

- 1) для проверки возможности поиска доменных пользователей отобразить сведения о пользователе домена (ivanov – пользователь в домене):

```
# getent passwd ivanov
ivanov:*:1187401105:1187400513:Иван
Иванов:/home/TEST.ALT/ivanov:/bin/bash
```

- 2) проверить возможность получения информации о домене:

```
# net ads info

LDAP server: 192.168.0.132
LDAP server name: dc1.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
LDAP port: 389
Server time: Cp, 27 мар 2024 10:36:51 EET
KDC server: 192.168.0.132
Server time offset: 2
Last machine account password change: Cp, 20 мар 2024 11:13:27
EET
```

- 3) проверить, действителен ли пароль учетной записи компьютера:

```
# net ads testjoin
Join is OK
```

Примечание. Список пользователей можно посмотреть на сервере командой:

```
# samba-tool user list
```

10.3.3.4. Вход пользователя

После ввода системы в домен список локальных пользователей в окне входа в систему будет скрыт автоматически.

Примечание. Определить будет ли показан список пользователей на экране приветствия/входа в систему LightDM можно с помощью control:

```
# control lightdm-greeter-hide-users
```

В команду можно передать следующие параметры:

- show – показать список доступных пользователей в greeter;
- hide – не перечислять пользователей в greeter.

Для регистрации в системе необходимо ввести логин учетной записи пользователя домена и нажать клавишу <Enter> или кнопку «Войти» (рис. 232). В открывшемся окне ввести пароль, соответствующий этой учетной записи и нажать кнопку «Войти» (рис. 233).

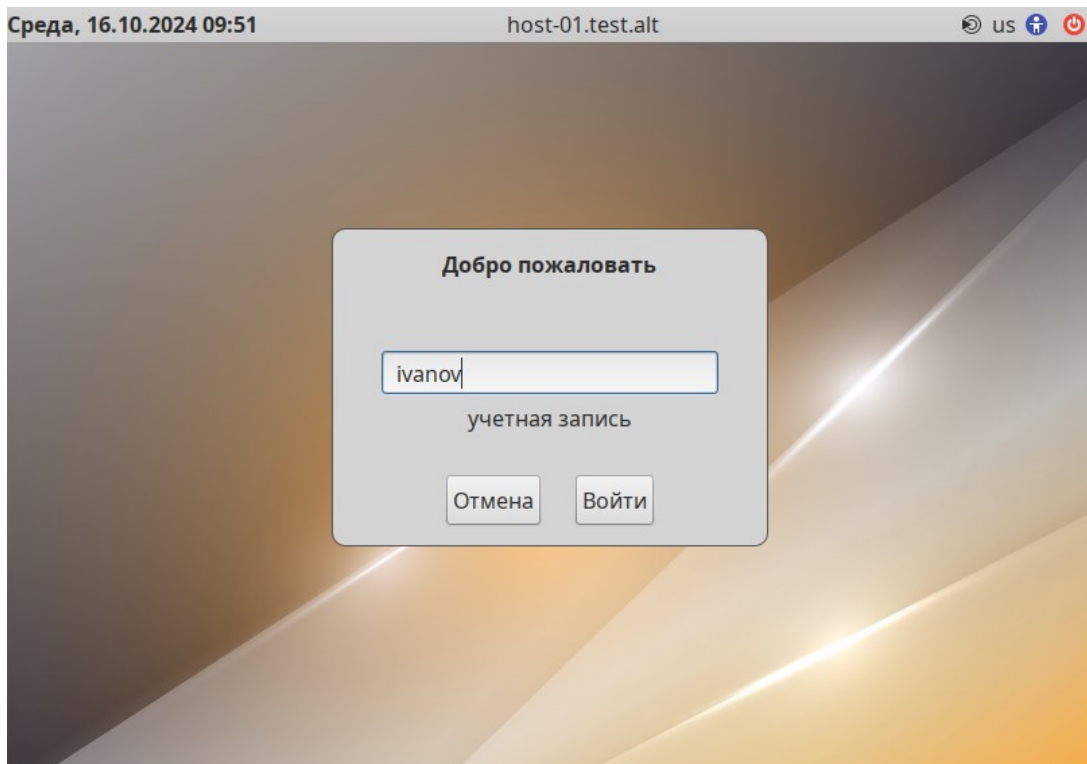


Рис. 232 – Ввод логина учетной записи пользователя домена

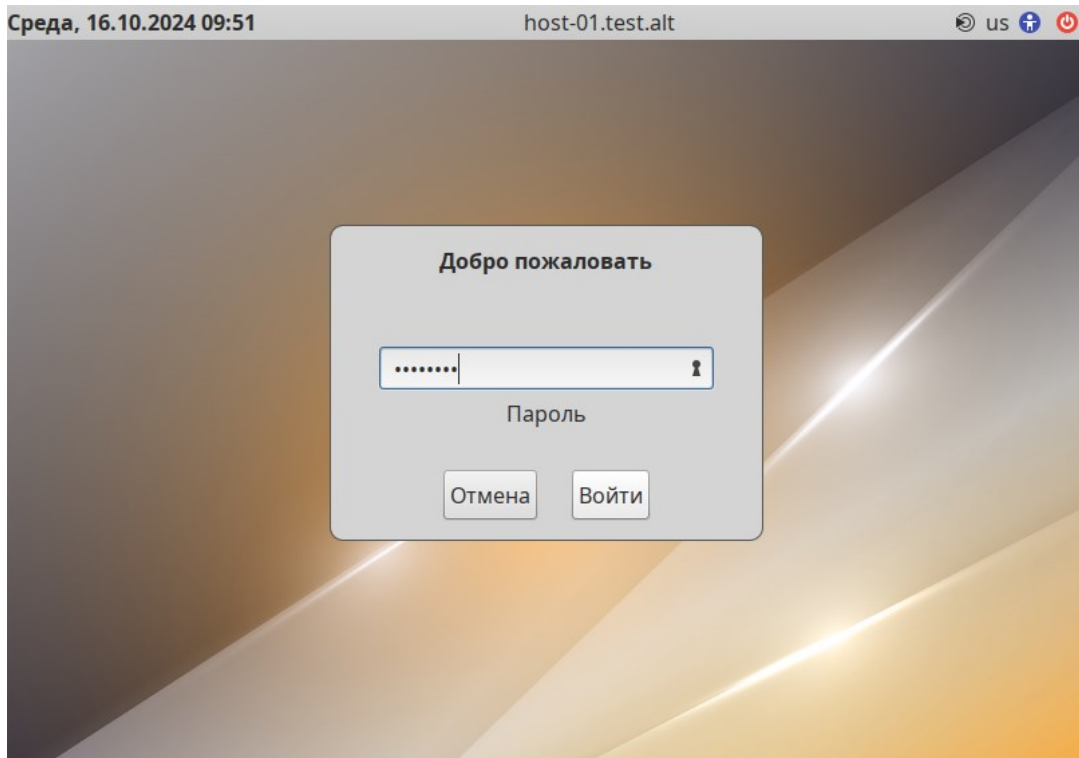


Рис. 233 – Ввод пароля

Чтобы настроить автоматическое заполнение поля «Имя пользователя» именем последнего пользователя, входившего в систему, в файле `/etc/lightdm/lightdm-gtk-greeter.conf` (группа `[greeter]`), необходимо указать:

```
enter-username = true
```

Примечание. В случае использования в окне логина символов верхнего регистра (например, `Irina.Soboleva` вместо `irina.soboleva`) или лишних символов (не используемых для стандартного имяобразования в Linux) может наблюдаться некорректное поведение системы (например, не выставляются переменные окружения `XDG_RUNTIME_DIR` и `DBUS_SESSION_BUS_ADDRESS`). Для возможности использовать для входа привычные способы написания (с доменным суффиксом, точками, символами верхнего регистра) необходимо выполнить команду:

```
# control pam_canonicalize_user enabled
```

или в файле `/etc/pam.d/system-auth-common` раскомментировать строку:

```
auth required pam_canonicalize_user.so
```

Модуль PAM `pam_canonicalize_user.so` использует введенное имя пользователя в качестве ключа для запроса базы данных паролей и заменяет имя пользователя на возвращенное значение.

10.3.4. Отладочная информация

10.3.4.1. Настройка уровня журналирования Samba

Дополнительные сведения см. в п. 10.6.14.3.

10.3.4.2. Ошибка при подключении к IP-адресу 127.0.0.1

Используя настройки по умолчанию, команда `net` подключается к IP-адресу 127.0.0.1. Если Samba не прослушивает петлевой интерфейс, соединение не устанавливается. Например:

```
# net rpc rights list -U administrator
Could not connect to server 127.0.0.1
Connection failed: NT_STATUS_CONNECTION_REFUSED
```

Чтобы решить эту проблему, необходимо настроить Samba для дополнительного прослушивания интерфейса `loopback`.

Примечание. Чтобы временно обойти проблему, можно передать параметр `-I <IP-адрес>` или `-S <Имя хоста>` в команду `net`:

```
# net rpc rights list -U administrator -I 192.168.0.132
Password for [TEST\administrator]:
SeMachineAccountPrivilege  Add machines to domain
SeTakeOwnershipPrivilege  Take ownership of files or other objects
...
```

10.3.4.3. `getent` не показывает доменных пользователей и группы

Используя команды `getent passwd` и `getent group` нельзя увидеть доменных пользователей и группы. Этот функционал отключен по умолчанию для того, чтобы сократить нагрузку на серверы. Поэтому для проверки необходимо указать точное имя пользователя:

```
# getent passwd <имя_пользователя>
```

Примечание. Список пользователей можно посмотреть на сервере командой:

```
# samba-tool user list
```

Если команда `getent passwd <имя_пользователя>` ничего не возвращает, следует попробовать выполнить команду:

```
# getent passwd <рабочая_группа>\<имя_пользователя>
```

Например:

```
# getent passwd "TEST\ivanov"
```


Если эта команда работает, а первая нет, то необходимо добавить следующую строку в файл `smb.conf`:

```
winbind use default domain = yes
```

10.3.5. Удаление клиента домена

Чтобы вывести систему из домена, можно воспользоваться командой `realm leave`. Эта команда удалит конфигурацию домена из SSSD и локальной системы:

```
# realm leave test.alt
```

По умолчанию удаление выполняется от имени администратора (для «Альт Домен» – `administrator`). Если для присоединения к домену использовалась учетная запись другого пользователя, может потребоваться выполнить удаление от имени этого пользователя. Чтобы указать пользователя следует использовать параметр `-U`:

```
# realm leave test.alt -U <пользователь>
```

Сначала команда пытается подключиться без использования учетных данных, но при необходимости запрашивает пароль.

Следует обратить внимание, что, когда клиент удаляется из домена, учетная запись компьютера не удаляется из каталога; удаляется только конфигурация локального клиента. Если необходимо удалить учетную запись компьютера, следует запустить команду с параметром `--remove`:

```
# realm leave --remove test.alt
```

Для получения дополнительной информации см. справочную страницу `man realm (8)`.

Примечание. После вывода из домена схема аутентификации пользователей в системе должна переключиться на локальную базу:

```
# control system-auth  
local
```

Примечание. Для того чтобы в окне входа отображался список доступных пользователей необходимо в файле `/etc/lightdm/lightdm.conf` закомментировать строку в группе `[SeatDefaults]`:

```
#greeter-hide-users=true
```

10.3.6. Повторная регистрация клиента

В этом разделе рассмотрена процедура повторной регистрации клиента в «Альт Домен» с тем же именем хоста. Повторная регистрация может потребоваться, если клиентский компьютер был уничтожен и потерял связь с серверами домена, например, из-за аппаратного сбоя клиента.

Перед повторным вводом в домен необходимо убедиться в том, что машина удалена из домена. Чтобы запись в домене была автоматически удалена при выводе машины из домена, необходимо использовать команду:

```
# realm leave --remove <домен>
```

Возможно также понадобится удалить закешированные записи:

```
# sss_cache -E
```

После вывода машины из домена следует убедиться в корректности имени машины и восстановить файлы `/etc/samba/smb.conf`, `/etc/sss/sss.conf` и `/etc/krb5.conf` к виду по умолчанию и повторно ввести машину в домен.

Примечание. Привести файлы к виду по умолчанию можно в модуле ЦУС «Аутентификация». В окне модуля «Аутентификация» следует установить отметку в поле «Восстановить файлы конфигурации по умолчанию (`smb.conf`, `krb5.conf`, `sss.conf`)» и нажать кнопку «Применить» (рис. 234).

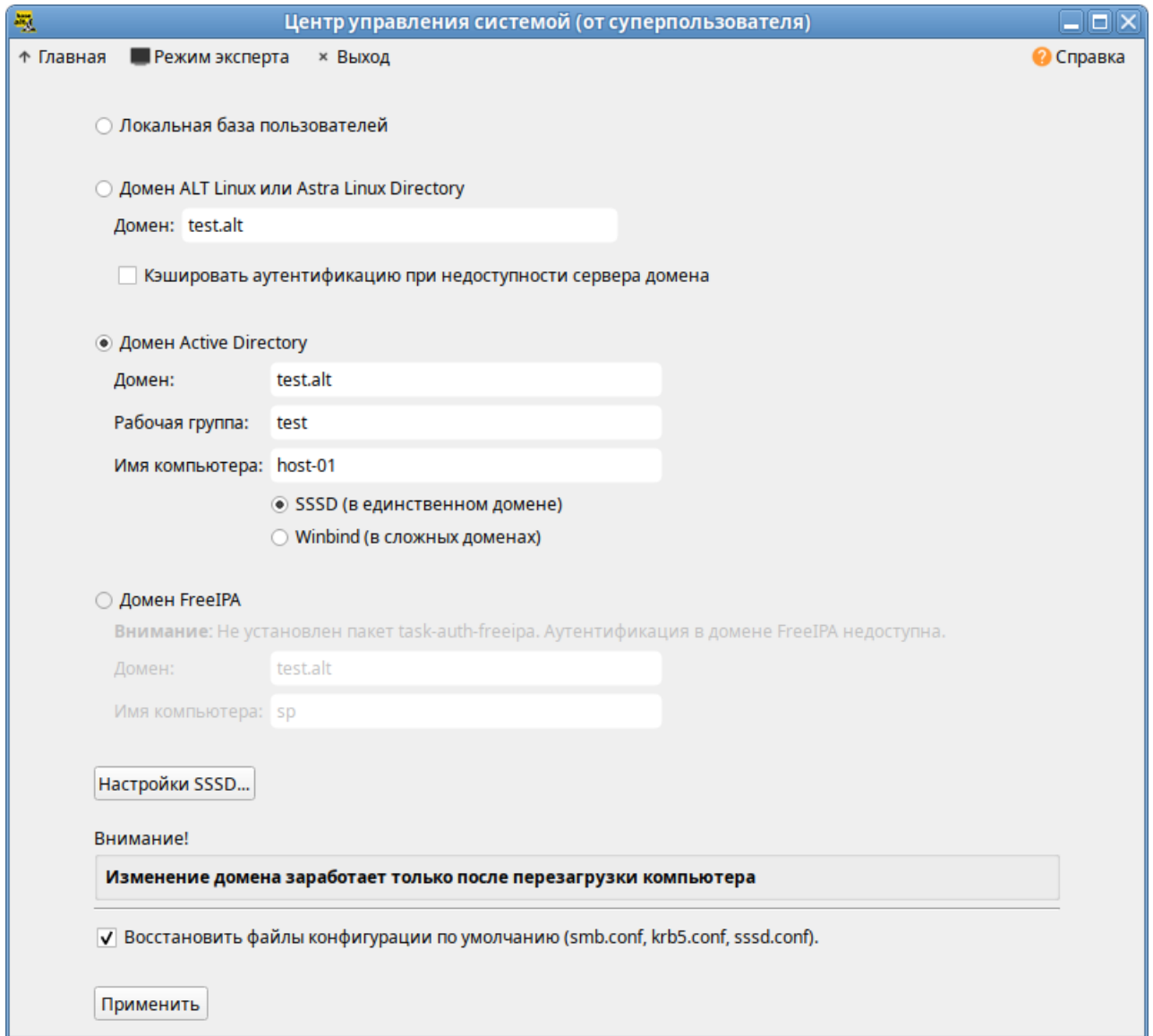


Рис. 234 – Ввод в домен в «Центр управления системой»

10.3.7. Настройка аутентификации доменных пользователей на DC

ВАЖНО

На текущий момент (samba 4.19.7, groupdate 0.10.6) данный метод не позволяет применять групповые политики на контроллере домена.

ВАЖНО

На текущий момент (samba 4.19.7, sssd 2.9.4) для каталога `/var/lib/samba/sysvol` SID'ы домена некорректно транслируются в UNIX user id и group id.

Контроллер домена в рамках доменной инфраструктуры является, в том числе, еще одной машиной и имеет соответствующий машинный аккаунт. После применения настроек, описанных в этом разделе, машина с контроллером домена сможет выполнять, в том числе, и функции обычного члена домена, такие как:

- аутентификация доменными пользователями (в том числе по SSH);
- применение групповых политик;
- все, что поддерживает обычная клиентская машина (в качестве клиента SSSD или Winbind).

ВАЖНО

В качестве клиента на контроллере домена рекомендуется использовать Winbind. Использование SSSD нежелательно.

10.3.7.1. Winbind

10.3.7.1.1. Установка пакетов

На контроллере домена необходимо установить пакеты `task-auth[ЕЛВ1]-ad-winbind` и `gpupdate`:

```
# apt-get install task-auth-ad-winbind gpupdate
```

10.3.7.1.2. Изменение файлов конфигурации

10.3.7.1.2.1. Настройка Kerberos (krb5.conf)

В файле `/etc/krb5.conf` должны быть заданы следующие параметры:

```
dns_lookup_realm = false
default_realm = TEST.ALT
```

Пример файла `/etc/krb5.conf`:

```
[logging]

[libdefaults]
dns_lookup_kdc = true
dns_lookup_realm = false
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
default_realm = TEST.ALT

[realms]

[domain_realm]
```

10.3.7.1.2.2. Настройка Samba (smb.conf)

В файле `/etc/samba/smb.conf` должны быть заданы следующие параметры:

```
kerberos method = dedicated keytab
dedicated keytab file = /etc/krb5.keytab
```

Значения остальных параметров в файле должны соответствовать аналогичному файлу на обычных клиентах домена.

Пример файла `/etc/samba/smb.conf`:

```
[global]
    dns forwarder = 8.8.8.8
    netbios name = DC1
    kerberos method = dedicated keytab
    dedicated keytab file = /etc/krb5.keytab
    realm = TEST.ALT
    server role = active directory domain controller
    workgroup = TEST
    idmap_ldb:use rfc2307 = yes
    template shell = /bin/bash
    template homedir = /home/TEST.ALT/%U

    wins support = no
    winbind use default domain = yes
    winbind enum users = no
    winbind enum groups = no
    winbind refresh tickets = yes
    winbind offline logon = yes

[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

[netlogon]
    path = /var/lib/samba/sysvol/test.alt/scripts
    read only = No
```

10.3.7.1.2.3. Настройка NSS (nsswitch.conf)

В файле `/etc/nsswitch.conf` должны быть заданы следующие параметры:

```
passwd: files winbind systemd
shadow: tcb files winbind
group: files [SUCCESS=merge] winbind role systemd
```

Пример файла `/etc/nsswitch.conf`:

```
passwd:    files winbind systemd
shadow:    tcb files winbind
group:     files [SUCCESS=merge] winbind role systemd
gshadow:   files
```

```

hosts:          files myhostname dns

ethers:         files
netmasks:      files
networks:      files
protocols:     files
rpc:           files
services:      files

automount:     files
aliases:       files

```

10.3.7.1.3. Настройка аутентификации

Необходимо переключить PAM-стек на использование для аутентификации

Winbind-модуля:

```
# control system-auth winbind
```

10.3.7.2. SSSD

10.3.7.2.1. Установка пакетов

На контроллере домена должны быть установлены пакеты task-auth-ad-sssd и groupdate:

```
# apt-get install task-auth-ad-sssd groupdate
```

10.3.7.2.2. Изменение файлов конфигурации

10.3.7.2.2.1. Настройка Kerberos (krb5.conf)

В файле /etc/krb5.conf должны быть заданы следующие параметры:

```
includedir /etc/krb5.conf.d/
dns_lookup_realm = false
default_realm = TEST.ALT
```

Пример файла /etc/krb5.conf:

```
includedir /etc/krb5.conf.d/
[logging]
```

```
[libdefaults]
dns_lookup_kdc = true
dns_lookup_realm = false
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
default_realm = TEST.ALT
```

```
[realms]
```

```
[domain_realm]
```

10.3.7.2.2. Настройка SSSD (sssd.conf)

В файле `/etc/sss/sss.conf` должны быть заданы следующие параметры:

```
user = root
ad_maximum_machine_account_password_age = 0
```

Значения остальных параметров в файле должны соответствовать аналогичному файлу на обычных клиентах домена.

Пример файла `/etc/sss/sss.conf`:

```
[sss]
config_file_version = 2
services = nss, pam

# Managed by system facility command:
## control sss-drop-privileges unprivileged|privileged|default
user = root

# SSSD will not start if you do not configure any domains.
domains = TEST.ALT
[nss]

[pam]
[domain/TEST.ALT]
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad
default_shell = /bin/bash
fallback_homedir = /home/%d/%u
debug_level = 0
; cache_credentials = false
ad_gpo_ignore_unreadable = true
ad_gpo_access_control = permissive
ad_update_samba_machine_account_password = true
ad_maximum_machine_account_password_age = 0
```

10.3.7.2.3. Настройка Samba (smb.conf)

В файле `/etc/samba/smb.conf` должны быть заданы следующие параметры:

```
idmap config * : range = 200000-2000200000
idmap config * : backend = sss
```

Значения остальных параметров в файле должны соответствовать аналогичному файлу на обычных клиентах домена.

Пример файла `/etc/samba/smb.conf`:

```
[global]
    dns forwarder = 8.8.8.8
    netbios name = DC1
```

```

realm = TEST.ALT
server role = active directory domain controller
workgroup = TEST
idmap_ldb:use rfc2307 = yes

```

```

template shell = /bin/bash
template homedir = /home/TEST.ALT/%U

```

```

kerberos method = system keytab
wins support = no
winbind use default domain = yes
winbind enum users = no
winbind enum groups = no
winbind refresh tickets = yes
winbind offline logon = yes

```

```

idmap config * : range = 200000-2000200000
idmap config * : backend = sss

```

[sysvol]

```

path = /var/lib/samba/sysvol
read only = No

```

[netlogon]

```

path = /var/lib/samba/sysvol/test.alt/scripts
read only = No

```

10.3.7.2.2.4. Настройка NSS (nsswitch.conf)

В файле /etc/nsswitch.conf должны быть заданы следующие параметры:

```

passwd: files sss systemd
shadow: tcb files sss
group: files [SUCCESS=merge] sss role system

```

Пример файла /etc/nsswitch.conf:

```

passwd:      files sss systemd
shadow:      tcb files sss
group:       files [SUCCESS=merge] sss role systemd
gshadow:     files

```

```

hosts:       files myhostname dns

```

```

ethers:      files
netmasks:   files
networks:    files
protocols:   files
rpc:         files
services:    files

```

```

automount:   files
aliases:     files

```


10.3.7.2.3. Настройка аутентификации

Необходимо переключить РАМ-стек на использование для аутентификации sss-модулей:

```
# control system-auth sss
```

10.3.7.3. Генерация keytab-файла

Необходимо сгенерировать системный keytab-файл для машинного аккаунта контроллера домена. Для этого следует выполнить следующую команду:

```
# net ads keytab create
```

10.3.7.4. Службы

Необходимо отключить сервис nscd:

```
# systemctl disable --now nscd
```

Если используется схема с SSSD клиентом, необходимо запустить и включить автоматический запуск для службы sssd:

```
# systemctl enable --now sssd
```

10.3.7.5. Настройка ролей

Необходимо указать, какие локальные роли, каким группам домена соответствуют:

- обычные пользователи домена («Domain Users») соответствуют локальной роли users:

```
# roleadd 'domain users' users
```

- администраторы домена («Domain Admins») соответствуют локальной роли localadmins:

```
# roleadd 'domain admins' localadmins
```

ВАЖНО

В русскоязычных версиях MS Windows Server встроенные группы «Domain Users» и «Domain Admins» имеют русифицированные названия «Пользователи домена» и «Администраторы домена».

10.3.7.6. Групповые политики

Для включения поддержки групповых политик необходимо выполнить команду:

```
# gpupdate-setup enable --local-policy ad-domain-controller
```

ВАЖНО

Работа групповых политик на контроллере домена с SSSD клиентом может быть не стабильной.

10.3.7.7. Настройка SSH

Разрешить удаленный доступ по SSH только Администраторам домена:

```
# control sshd-allow-groups enabled
# control sshd-allow-groups-list remote
```

При необходимости можно разрешить аутентификацию по Kerberos билетам:

```
# control sshd-gssapi-auth enabled
```

Для применения настроек необходимо перезапустить сервис sshd:

```
# systemctl restart sshd
```

Примечание. Данные настройки можно применить с помощью механизма групповых политик control. Подробнее см. п. 10.4.6.4.2.

10.3.8. Настройка обновления паролей аккаунтов машин

После завершения процедуры ввода в домен каждая машина получает специальный аккаунт вида MACHINE01\$. Такой аккаунт, ассоциированный с машиной, а не с конкретным пользователем, позволяет машине выполнять в домене действия от своего имени. Например, запрашивать информацию о пользователях, получать машинные групповые политики и т. д.

Как и у любого другого пользователя, у машинного пользователя есть свой пароль, генерируемый автоматически в процессе ввода машины в домен. В отличие от обычных пользователей, у машинных аккаунтов нет ограничения на время жизни пароля, но машина имеет возможность поменять его самостоятельно. По умолчанию машины с MS Windows 2000 и старше меняют пароль раз в 30 дней. Информация о последней смене пароля хранится в атрибуте машинного аккаунта `pwdlastset`.

10.3.8.1. Локальная политика смены пароля

Сменой пароля учетной записи компьютера можно управлять с помощью групповых политик. Для этого нужно отредактировать параметр политики домена по умолчанию (Default domain policy) «Член домена: максимальный срок действия пароля учетной записи компьютера», который располагается в подразделе

«Конфигурация компьютера» → «Политики» → «Конфигурация Windows» → «Параметры безопасности» → «Локальные политики» → «Параметры безопасности» (Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options) (рис. 235).

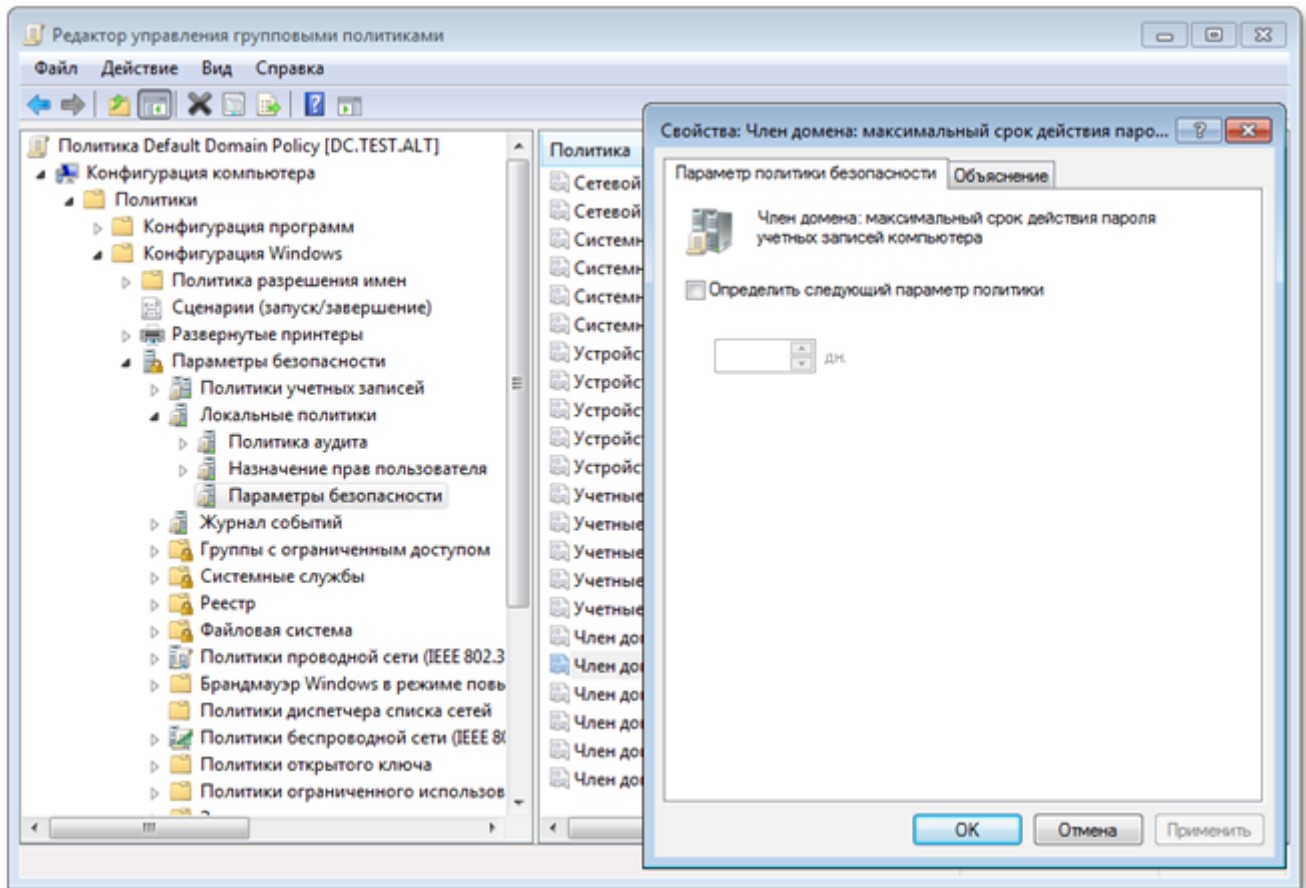


Рис. 235 – Окно параметра «Член домена»

Примечание. На данный момент в ADMS (adms 0.16.4) нет возможности настроить данные параметры групповой политики. Необходимо использовать оснастку RSAT «Управление групповыми политиками» (см. п. 10.4.2.3).

Этот параметр безопасности определяет, как часто член домена будет пытаться изменить пароль учетной записи компьютера. Значение по умолчанию: 30 дней.

С помощью параметра «Член домена: отключить изменение пароля учетных записей компьютера» можно отключить обновления пароля машинного аккаунта совсем, но делать этого не рекомендуется.

ВАЖНО

Указанные выше параметры корректно работают на машинах с ОС MS Windows 2000 и старше.

ВАЖНО

На машинах с ОС Альт СП (sssd 2.9.4) данные параметры игнорируются.

10.3.8.2. Включение обновления пароля**10.3.8.2.1. ОС Windows**

Для включения периодического обновления пароля учетной записи компьютера на машинах под управлением ОС Windows 2000 и старше дополнительных действий не требуется. Периодичность обновления настраивается с помощью соответствующей групповой политики.

10.3.8.2.2. ОС Альт СП

За обновление пароля машинного аккаунта на машинах под управлением ОС Альт СП отвечают сервисы `sssd` и `winbind`.

10.3.8.2.2.1. Winbind

`Winbind`, на текущий момент (`samba-winbind 4.19.7`), не умеет после смены пароля учетной записи компьютера обновлять системный `keytab`-файл (`/etc/krb5.keytab`). Поэтому, во избежание конфликтов с `sssd`, следует отключить этот функционал.

Для отключения периодического обновления пароля учетной записи компьютера необходимо в файл `smb.conf` в секцию `[global]` добавить параметр `machine password timeout = 0`:

```
[global]
machine password timeout = 0
```

10.3.8.2.2.2. SSSD

`SSSD` для обновления пароля учетной записи компьютера использует утилиту `adcli`. Необходимо убедиться, что пакет `adcli` установлен в системе:

```
# apt-get install adcli
```

Периодичностью обновления пароля учетной записи компьютера можно управлять с помощью параметра `ad_maximum_machine_account_password_age` (секция `[domain/<Домен>]`) в `/etc/sss/sss.conf`. Значение по умолчанию: 30 дней.

Для корректного функционирования обновления пароля учетной записи компьютера `sss` необходим доступ на запись в файл `/etc/krb5.keytab`. Для этого недостаточно привилегий пользователя `_sss`, от которого обычно и запускается `sss`. Необходимо запускать `sss` с правами суперпользователя. Для этого следует в файле `/etc/sss/sss.conf` в секции `[sss]` изменить значение параметра `user` на `root`:

```
[sss]
user = root

[domain/<Домен>]
ad_update_samba_machine_account_password = true
```

ВАЖНО

При вводе компьютера в домен с помощью ЦУС следующие параметры прописываются в конфигурационные файлы по умолчанию:

```
- /etc/samba/smb.conf:
  machine password timeout = 0
- /etc/sss/sss.conf:
  ad_update_samba_machine_account_password = true
```

10.3.8.3. Отключение обновления пароля

10.3.8.3.1. ОС Windows

Для отключения периодического обновления пароля учетной записи компьютера на машинах под управлением ОС Windows 2000 и старше достаточно включить параметр групповой политики «Default domain policy» «Член домена: отключить изменение пароля учетных записей компьютера».

10.3.8.3.2. ОС Альт СП

Для отключения периодического обновления пароля учетной записи компьютера на машинах под управлением ОС Альт СП необходимо:

- в файле `/etc/sss/sss.conf` (секция `[domain/<Домен>]`) значение параметра `ad_maximum_machine_account_password_age` установить равным 0:

```
[domain/<Домен>]
ad_maximum_machine_account_password_age = 0
- в файле /etc/samba/smb.conf (секция [global]) значение параметра
machine password timeout установить равным 0:
[global]
machine password timeout = 0
```

10.3.8.4. Диагностика

10.3.8.4.1. Дата последней смены пароля

Дата последней смены пароля учетной записи компьютера хранится в базе данных «Альт Домен». Запросить ее можно одним из способов:

- на введенной в домен машине выполнить команду:

```
# net ads info
...
Last machine account password change: Ср, 20 мар 2024 12:36:35
EET
```

- если машина уже потеряла доверие в домене, то выполнить эту же команду от доменного пользователя:

```
# net ads info -U <user>
```

Дата последней смены пароля учетной записи компьютера будет показана в параметре:

```
Last machine account password change.
```

10.3.8.4.2. Потеря доверия между машиной и доменом

Для проверки того, имеет ли машина возможность аутентифицироваться в домене, можно выполнить следующие действия:

- убедиться, что keytab-файла (/etc/krb5.keytab) содержит корректную информацию:

```
# klist -ke
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
-----
-----
1 host/work.test.alt@TEST.ALT (aes256-cts-hmac-sha1-96)
1 host/WORK@TEST.ALT (aes256-cts-hmac-sha1-96)
1 host/work.test.alt@TEST.ALT (aes128-cts-hmac-sha1-96)
1 host/WORK@TEST.ALT (aes128-cts-hmac-sha1-96)
1 host/work.test.alt@TEST.ALT (DEPRECATED:arcfour-hmac)
1 host/WORK@TEST.ALT (DEPRECATED:arcfour-hmac)
1 restrictedkrbhost/work.test.alt@TEST.ALT (aes256-cts-hmac-sha1-
96)
```

ЛКНВ.11100-01 90 03

```

1 restrictedkrbhost/WORK@TEST.ALT (aes256-cts-hmac-sha1-96)
1 restrictedkrbhost/work.test.alt@TEST.ALT (aes128-cts-hmac-sha1-96)
1 restrictedkrbhost/WORK@TEST.ALT (aes128-cts-hmac-sha1-96)
1 restrictedkrbhost/work.test.alt@TEST.ALT (DEPRECATED:arcfour-hmac)
1 restrictedkrbhost/WORK@TEST.ALT (DEPRECATED:arcfour-hmac)
1 WORK$@TEST.ALT (aes256-cts-hmac-sha1-96)
1 WORK$@TEST.ALT (aes128-cts-hmac-sha1-96)
1 WORK$@TEST.ALT (DEPRECATED:arcfour-hmac)

```

- попытаться получить билет Kerberos для учетной записи компьютера (в примере WORK\$), используя файл /etc/krb5.keytab:

```
# kinit -k WORK\@$@TEST.ALT
```

- убедиться, что билет успешно получен и удалить его:

```

# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: WORK$@TEST.ALT

Valid starting Expires Service principal
21.04.2023 12:25:37 21.04.2023 22:25:37 krbtgt/TEST.ALT@TEST.ALT

renew until 28.04.2023 12:25:37

# kdestroy -p WORK\@$@TEST.ALT

```

ВАЖНО

Следует убедиться, что имя машины в keytab-файле (/etc/krb5.keytab) соответствует реальному имени машины (см. вывод команды hostnamectl).

10.3.8.5. Восстановление работоспособности

Если диагностика показала, что машина потеряла доверие с доменом, то для восстановления работоспособности, необходимо выполнить следующие действия:

- обновить систему:

```
# apt-get update && apt-get dist-upgrade
```

- удалить файл /etc/krb5.keytab;

- повторно ввести машину в домен;

- убедиться, что конфигурационные файлы соответствуют одному из сценариев: «Включение обновления пароля» или «Отключение обновления пароля»;

- перезагрузить машину.

10.4. Инструменты управления объектами домена и групповыми политиками

10.4.1. Групповые политики

Групповые политики – это набор правил и настроек для серверов и рабочих станций, реализуемых в корпоративных решениях. В соответствии с групповыми политиками производится настройка рабочей среды относительно локальных политик, действующих по умолчанию.

Групповые политики, как механизм, отличаются от стандартных инструментов управления конфигурациями (таких как, например, Puppet и Ansible) тремя ключевыми особенностями:

- интеграцией в инфраструктуру AD;
- соответствием декларативной части настроек конфигураций конкретным дистрибутивным решениям;
- наличием не только управления конфигурациями компьютеров, но и конфигурациями пользователей.

В ОС Альт СП для применения групповых политик используется инструмент `grupdate` (см. п. 10.4.4). Инструмент рассчитан на работу на машине, введенной в «Альт Домен».

Интеграция в инфраструктуру LDAP-объектов «Альт Домен» позволяет осуществлять привязку настроек управляемых конфигураций объектам в дереве каталогов. Кроме глобальных настроек в рамках домена, возможна привязка к следующим группам объектов:

- подразделения (OU) – пользователи и компьютеры, хранящиеся в соответствующей части дерева объектов;
- сайты – группы компьютеров в заданной подсети в рамках одного и того же домена;
- конкретные пользователи и компьютеры.

Кроме того, в самих объектах групповых политик могут быть заданы дополнительные условия, фильтры и ограничения, на основании которых принимается решение о том, как применять данную групповую политику.

Политики подразделяются на политики для компьютеров (Machine) и политики для пользователей (User).

Примечание. Групповая политика для компьютеров должна быть привязана к OU с компьютерами. Групповая политика для пользователей должна быть привязана к OU с пользователями. Объект, к которому должна применяться политика, должен находиться в нужном OU с компьютерами или пользователями.

Политики для компьютеров применяются на узле в момент загрузки, а также в момент явного или регулярного запроса планировщиком (раз в час). Пользовательские политики применяются в момент входа в систему. Некоторые задачи управления конфигурациями можно решить как через пользовательские, так и через машинные параметры.

Система управления групповых политик в «Альт Домен» представлена широким набором конфигурационных настроек. В общем виде эти настройки делятся на две категории – политики и предпочтения. Основное отличие политик от предпочтений состоит в том, что политики можно отменить, поскольку они «накладываются» через реестр поверх настроек приложений так, что приложения не могут их изменить. Исключение составляют настройки, перегружаемые через такой механизм, как GConf или dconf, а также определенные правила для PolicyKit.

Основным отличием предпочтений от политик состоит в том, что эти настройки пользователь или приложение может изменить или отменить после их применения. Регулярная перезапись таких настроек частично сглаживает эту особенность, доставляя конечному пользователю неудобство, но не ограничивая его возможности повлиять на заданную для него или его компьютера политику, точнее предпочтение.

Одним из ключевых ограничений, не позволяющих использовать политики вместо предпочтений, является то, что значения конфигурационных настроек при их задании перезаписываются, теряя исходное состояние. В рамках дистрибутивных решений ОС Альт СП разработан механизм локальной политики (аналогичный Local Policy под Windows), позволяющий частично преодолеть эту проблему. На текущий момент этот механизм представлен профилями, определяющими шаблон локальной политики, определяемый при включении механизма применения групповых политик.

Далее, для терминологического упрощения, политики и предпочтения называются одним термином «Групповая политика» (ГП) с поправками на особенности их применения.

Список групповых политик, которые можно настроить и применять в «Альт Домен» представлен в таблице 17.

Примечание. Экспериментальными называются политики, реализация которых может в процессе разработки поменяться так, что ранее установленные политики после обновления перестанут быть установленными, поскольку настройки таких политик не утверждены технически.

Логическая структура инструментов управления (рис. 236) содержит следующие компоненты:

- сервер базы данных с информацией о клиентах и их конфигурации;
- клиентское ПО для репликации и применения конфигурации;
- графическая панель управления включением механизма применения конфигурации;
- графический редактор базы данных конфигурации (ADMC);
- графический редактор настроек клиентской конфигурации (GPUJ).

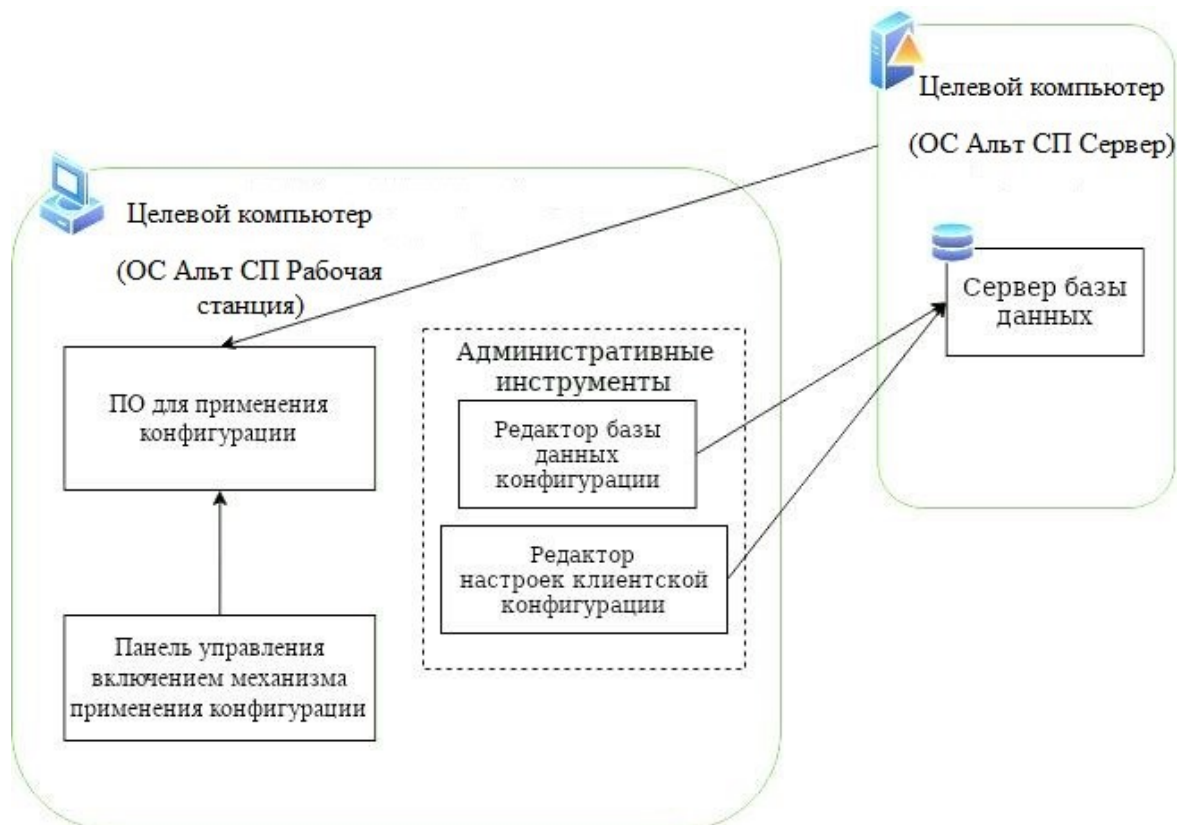


Рис. 236 – Логическая структура

Т а б л и ц а 17 – Список групповых политик

Политика	Статус	Комментарий
Управление политиками control	Стабильная	ADMX-файлы ALT (пакет admx-basealt)
Включение или выключение различных служб (сервисов systemd)	Стабильная	ADMX-файлы ALT (пакет admx-basealt)
Настройка браузера Firefox	Стабильная	ADMX-файлы Mozilla Firefox (пакет admx-firefox)
Настройка браузера Chromium	Стабильная	ADMX-файлы Google Chrome (пакет admx-chromium)
Настройка «Яндекс.Браузера»	Стабильная	ADMX-файлы Yandex (пакет admx-yandex-browser)
Управление Gsettings (настройки графической среды MATE и удаленного доступа к рабочему столу VNC)	Стабильная	ADMX-файлы ALT (пакет admx-basealt)
Настройки среды рабочего стола KDE	Экспериментальная	ADMX-файлы ALT (пакет admx-basealt)
Управление настройками службы Polkit	Стабильная	ADMX-файлы ALT (пакет admx-basealt)
Подключение сетевых дисков	Стабильная	
Управление общими каталогами	Экспериментальная	
Управление ярлыками для запуска программ	Стабильная	
Управление каталогами	Стабильная	
Управление файлами	Экспериментальная	
Управление INI-файлами	Экспериментальная	
Управление переменными среды	Экспериментальная	
Управление logon-скриптами	Экспериментальная	
Установка и удаление пакетов	Экспериментальная	

10.4.2. Установка административных шаблонов и административных инструментов

10.4.2.1. Установка административных шаблонов

Для задания конфигурации необходимо на контроллере домена установить административные шаблоны (ADMX-файлы). Для этого следует:

1) установить пакеты политик:

```
# apt-get install admx-basealt admx-yandex-browser admx-chromium
admx-firefox admx-msi-setup
```

доступны следующие пакеты политик:

- admx-basealt – ADMX-файлы, специфичные для BaseALT;
- admx-yandex-browser – ADMX-файлы для управления настройками Яндекс.Браузера;

- admx-firefox – ADMX-файлы для управления настройками браузера Mozilla Firefox;
- admx-chromium – ADMX-файлы для управления настройками браузера Google Chrome.

Примечание. Шаг установки пакетов политик можно пропустить, если при установке ОС на этапе «Установка системы» был выбран профиль «Альт Домен (контроллер домена)» (рис. 213).

- 2) запустить утилиту `admx-msi-setup`, которая загрузит и установит ADMX-файлы от Microsoft:

```
# admx-msi-setup
```

- 3) после установки, политики будут находиться в каталоге `/usr/share/PolicyDefinitions`. Скопировать локальные ADMX-файлы в сетевой каталог `sysvol (/var/lib/samba/sysvol/<DOMAIN>/Policies/)`:

```
# samba-tool gpo admxload -U Administrator
```

Примечание. По умолчанию, утилита `admx-msi-setup` устанавливает последнюю версию ADMX от Microsoft (сейчас это Microsoft Group Policy – Windows 10 October 2020 Update (20H2)). С помощью параметров, можно указать другой источник:

```
# admx-msi-setup -h
admx-msi-setup - download msi files and extract them in
<destination-directory> default value is
/usr/share/PolicyDefinitions/.
```

```
Usage: admx-msi-setup [-d <destination-directory>] [-s <admx-msi-
source>]
```

```
Removing admx-msi-setup temporary files...
```

10.4.2.2. Административные инструменты

Административные инструменты обычно устанавливаются на рабочей станции, введенной в домен.

Примечание. Шаг установки административных инструментов можно пропустить, если при установке рабочей станции на этапе «Установка системы» был выбран профиль «Альт Домен (инструмент управления ГПО)» (рис. 237).

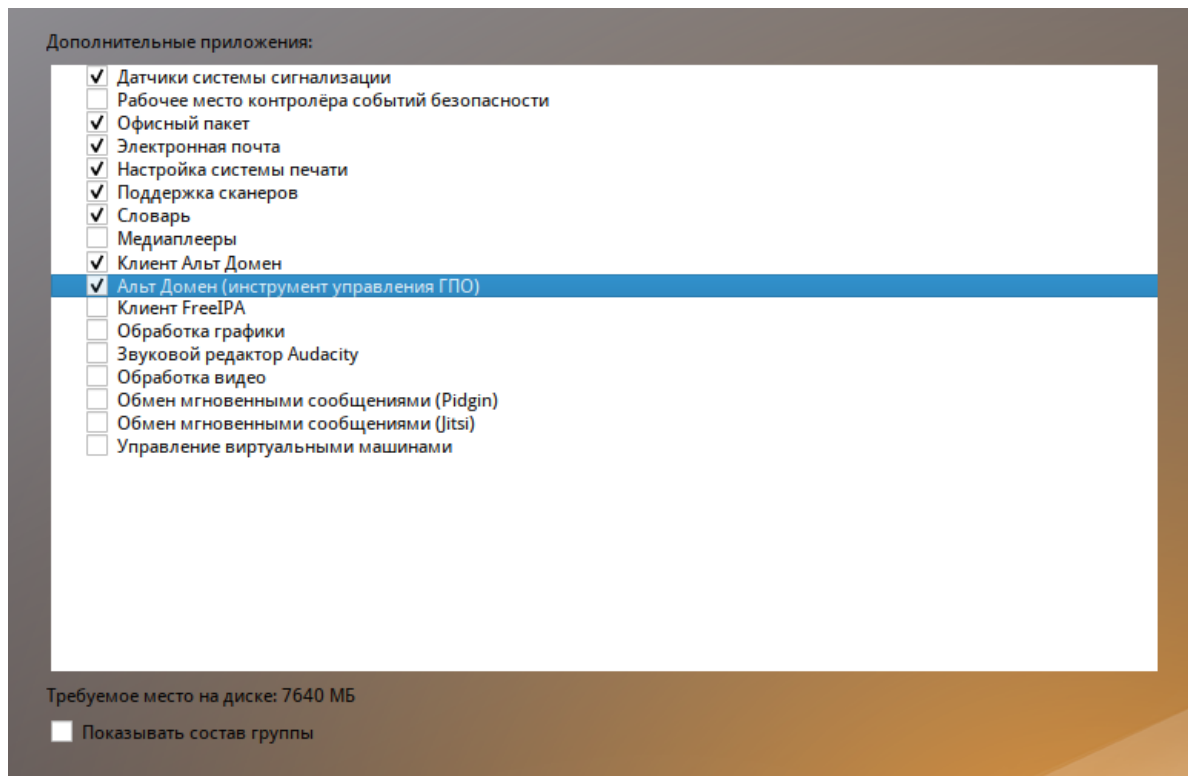


Рис. 237 – Выбор профиля «Клиент Альт Домен» при установке ОС

10.4.2.2.1. ADMC

Установить пакет `admc`:

```
# apt-get install admc
```

Запуск ADMC осуществляется из меню запуска приложений: пункт «Системные»→«ADMC» или из командной строки (команда `admc`).

Примечание. Для использования ADMC необходимо предварительно получить ключ Kerberos для администратора домена. Получить ключ Kerberos можно, например, выполнив следующую команду:

```
$ kinit administrator
```

Подробнее о работе с ADMC см. п. 10.4.5.

10.4.2.2.2. GPUI

Установить пакет `gpiui`:

```
# apt-get install gpiui
```

В настоящее время GPUИ не умеет читать файлы ADMX с контроллера домена. Поэтому для корректной работы необходимо также установить пакеты admx и файлы ADMX от Microsoft:

```
# apt-get install admx-basealt admx-samba admx-chromium
admx-firefox admx-msi-setup
# admx-msi-setup
```

Примечание. Для использования GPUИ необходимо предварительно получить ключ Kerberos для администратора домена.

Подробнее о работе с GPUИ см. п. 10.4.6

10.4.2.3. Установка RSAT

Для администрирования «Альт Домен» из Windows можно использовать средства удаленного администрирования сервера Microsoft (RSAT).

10.4.2.3.1. Windows Server

В ОС Windows Server средства удаленного администрирования сервера Microsoft (RSAT) включены по умолчанию.

Для установки необходимо выполнить следующие пункты:

- 1) запустить Диспетчер серверов;
- 2) на Windows Server 2012, 2012 R2, и 2016:

- выбрать «Управление» → «Добавить роли и компоненты» (рис. 238);

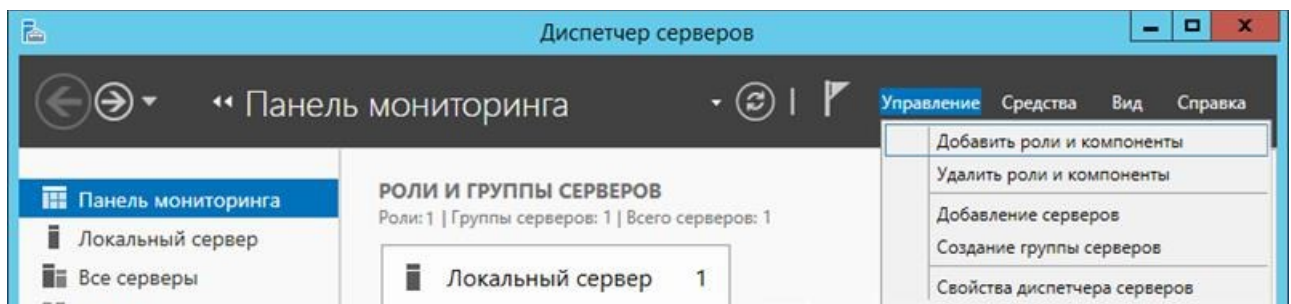


Рис. 238 – Диспетчер сервисов

- в открывшемся окне «Мастер добавления ролей и компонентов» выбрать пункт «Установка ролей или компонентов» (рис. 239);

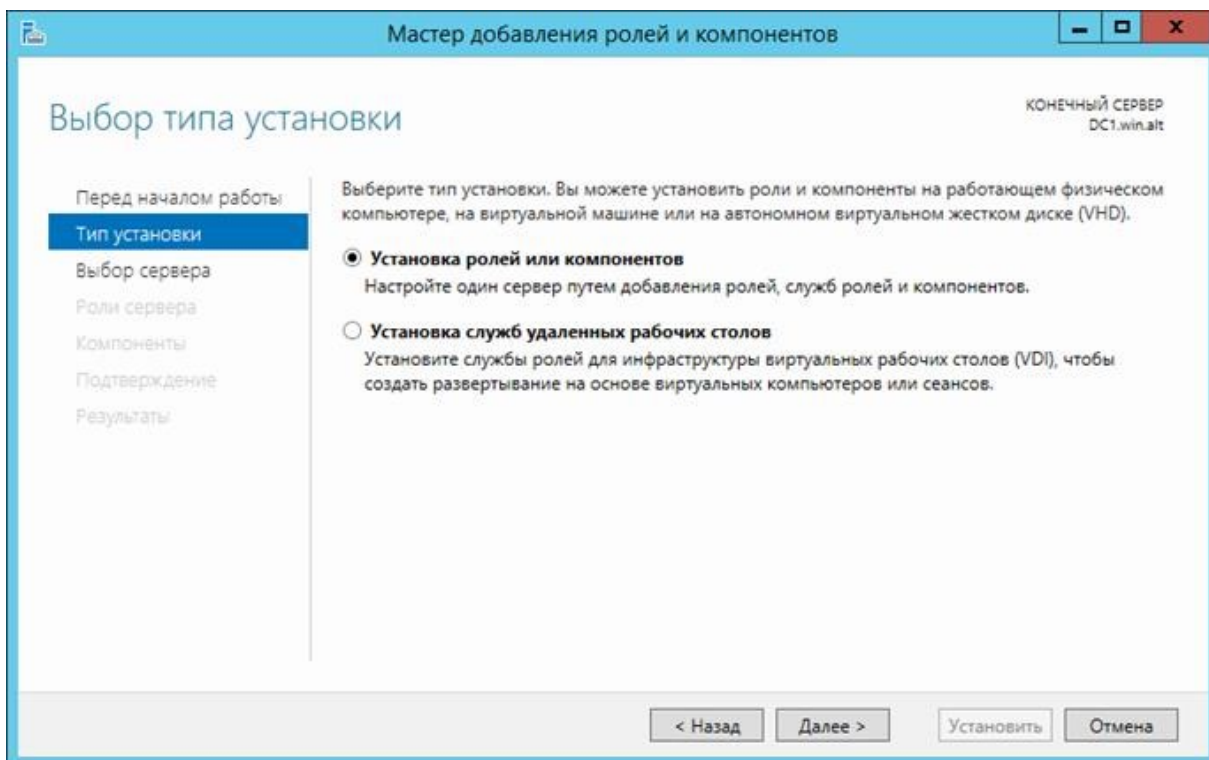


Рис. 239 – Выбор типа установки

- выбрать узел, на котором будут установлены компоненты (рис. 240);
- на шаге «Роли сервера» нажать кнопку «Далее»;

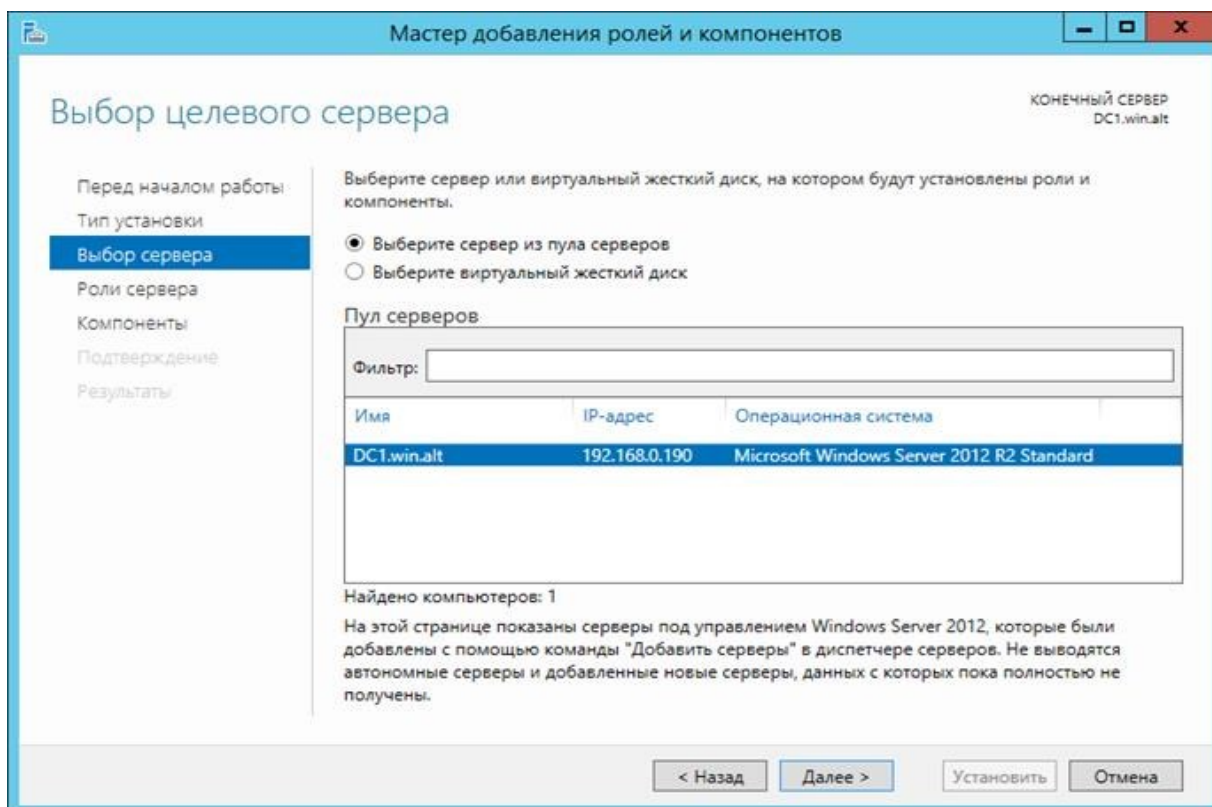


Рис. 240 – Выбор целевого сервера

- 3) на Windows Server 2008 и 2008 R2 в дереве навигации выбрать «Компоненты» и нажать «Добавить компоненты»;
- 4) выбрать компоненты для установки (рис. 241). Рекомендуемые компоненты см. в таблице 18.

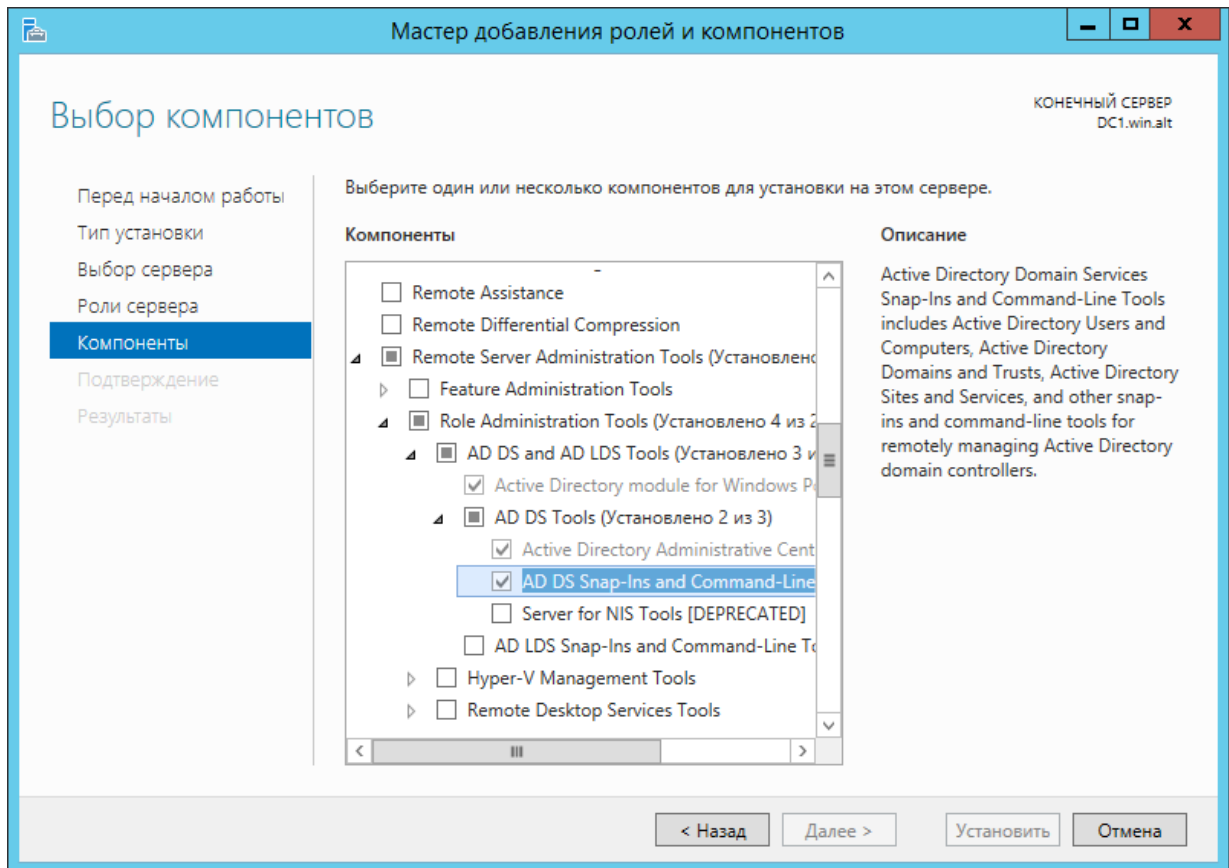


Рис. 241 – Выбор компонентов

Т а б л и ц а 18 – Компоненты Windows для администрирования домена

Компонент	Описание
Group Policy Management	Предоставляет оснастки для групповой политики: средство управления (GPMC), редактор управления (gpedit) и начальный редактор GPO
AD DS Snap-Ins and Command-Line Tools	Предоставляет оснастку «Пользователи и компьютеры Active Directory» (ADUC) и «Сайты и службы Active Directory» (ADSS)
Server for NIS	Добавляет вкладку Атрибуты UNIX в свойства объектов ADUC. Позволяет настраивать атрибуты RFC2307. Эта функция не поддерживается в Windows Server 2016
Active Directory Module for Windows PowerShell	Включает команды Active Directory (AD) PowerShell
DNS Server tools	Оснастка MMC DNS для удаленного управления DNS

10.4.2.4. Windows 10 (1809 и более поздние версии)

В Windows 10 1809 и более поздних версиях RSAT устанавливается в качестве дополнительной функции. Для установки компьютер должен иметь доступ в Интернет.

Для установки RSAT выполнить следующие действия:

- 1) перейти в раздел «Settings» → «Apps» → «Optional Features» → «View features» («Параметры Windows» → «Приложения» → «Дополнительные возможности» → «Добавить компонент») (рис. 242);

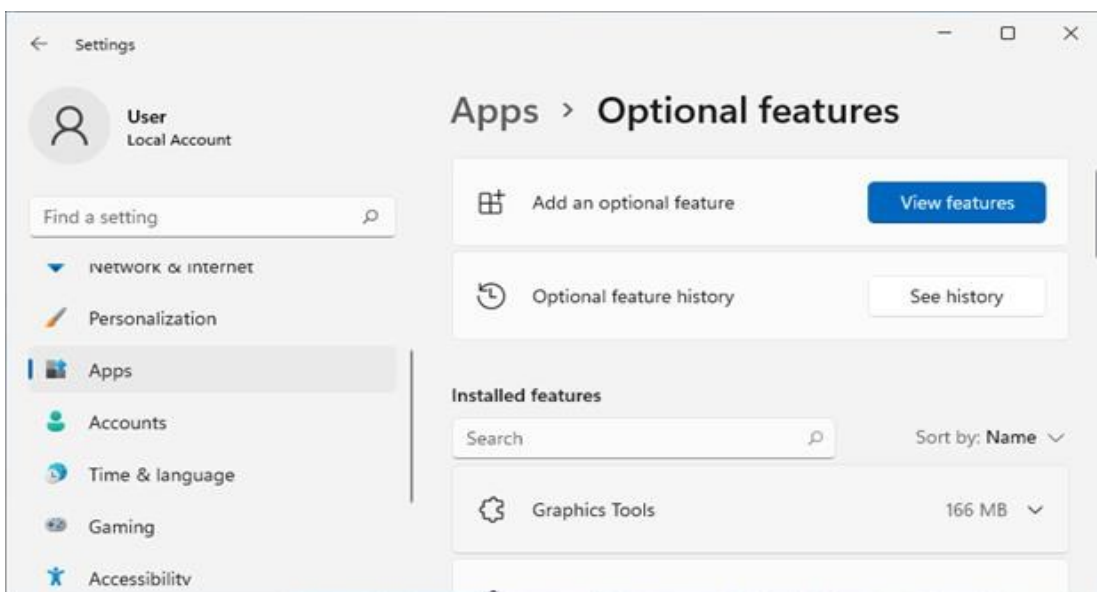


Рис. 242 – Дополнительные возможности

- 2) выбрать нужные компоненты RSAT (рекомендованные компоненты RSAT представлены в таблице 19) и нажать кнопку «Next» (рис. 243);

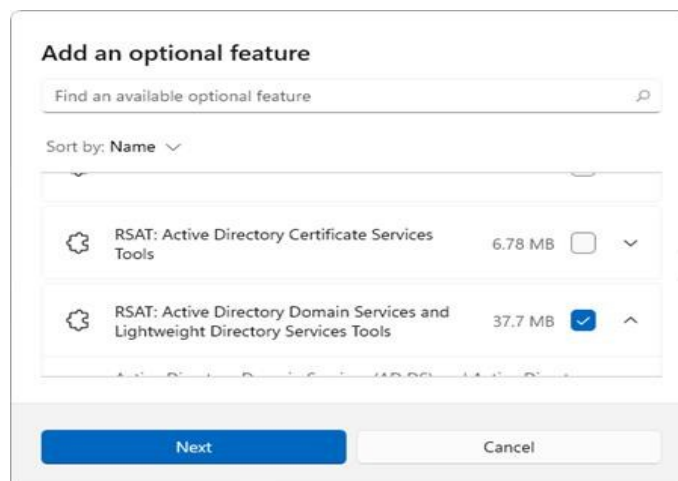


Рис. 243 – Добавление компонентов

3) нажать кнопку «Install».

Т а б л и ц а 19 – Рекомендуемые компоненты RSAT

Компонент	Описание
RSAT: Group Policy Management Tools	Включает консоль управления групповыми политиками (gpmmc.msc), редактор управления групповыми политиками (gpme.msc) и редактор GPO инициализирующей программы групповой политики (gpedit.msc)
RSAT: Active Directory Domain Services and Lightweight Directory Services Tools	Предоставляет оснастку «Пользователи и компьютеры Active Directory» (ADUC) и «Сайты и службы Active Directory» (ADSS)
RSAT: DNS Server Tools	Включает оснастку «Диспетчер DNS» для удаленного управления DNS и программу командной строки dnscmd.exe
RSAT: Remote Desktop Services Tool	Добавляет вкладку Профиль служб удаленных рабочих столов в свойства объекта пользователя ADUC и устанавливает оснастку MMC «Удаленные рабочие столы» для администрирования RDP-сервера (tsmmc.msc).

10.4.2.5. Windows Vista и 7

До версии Windows 10 1809 пакет удаленного администрирования серверов RSAT устанавливается в виде MSU обновления, которое нужно скачать с серверов Microsoft.

Для установки RSAT необходимо выполнить следующие действия:

- 1) перейти в «Панель управления» → «Программы» → «Включение или отключение компонентов Windows» (рис. 244);

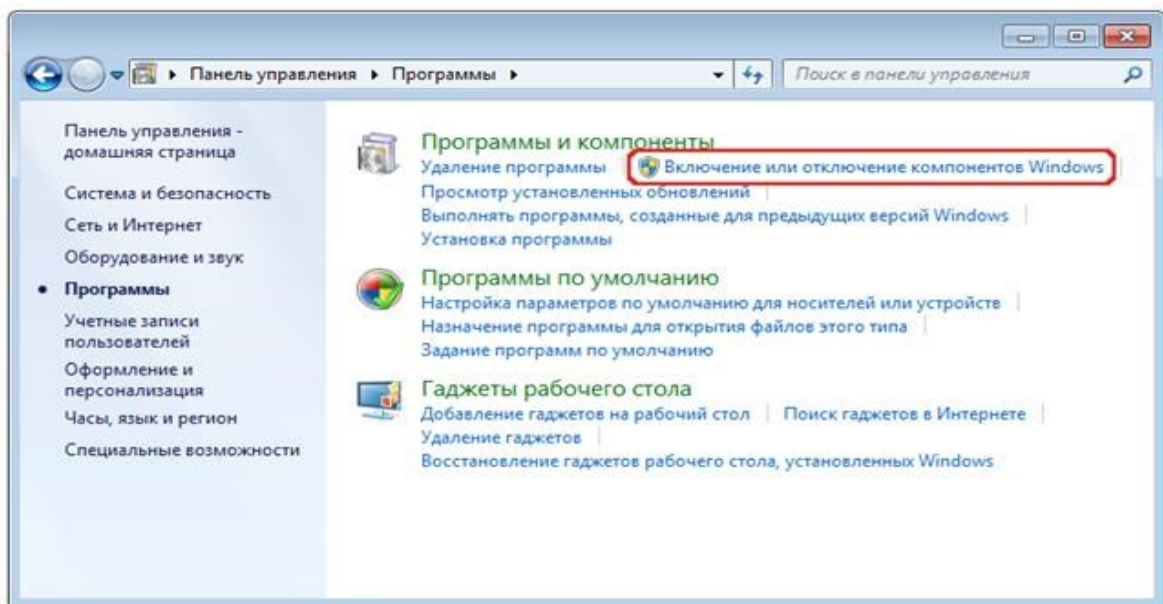


Рис. 244 – «Включение или отключение компонентов Windows»

2) включить компоненты, представленные на рис. 245 и описанные в таблице 20;

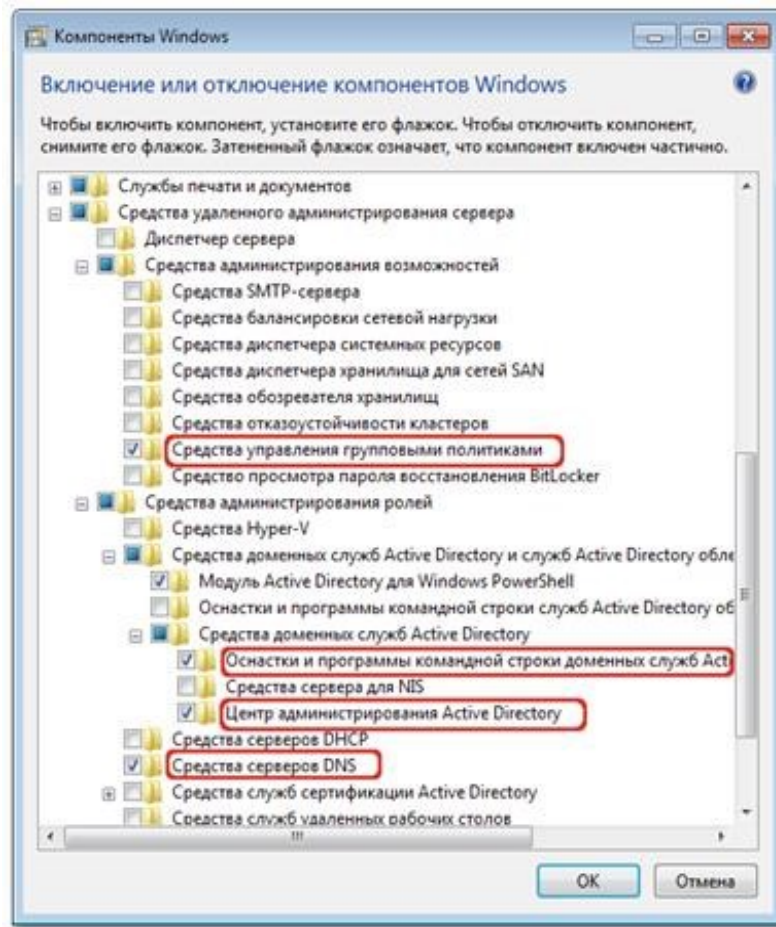


Рис. 245 – Компоненты для включения

Т а б л и ц а 20 – Рекомендуемые компоненты Windows

Компонент	Описание
Group Policy Management Tools (Средства управления групповыми политиками)	Включают консоль управления групповыми политиками (gpms.msc), редактор управления групповыми политиками (gpmc.msc) и редактор GPO инициализирующей программы групповой политики (gpedit.msc)
AD DS Tools (Оснастки и программы командной строки доменных служб Active Directory)	Предоставляет оснастку «Пользователи и компьютеры Active Directory» (ADUC) и «Сайты и службы Active Directory» (ADSS)
Server for NIS Tools (Средства сервера для NIS)	Средства сервера для сетевых информационных служб добавляет вкладку Атрибуты UNIX (UNIX Attributes) в свойства объектов ADUC. Позволяет настраивать атрибуты RFC2307. Включает программу командной строки upclear.exe

Окончание таблицы 20

Компонент	Описание
Active Directory Module for Windows PowerShell (Модуль Active Directory для Windows PowerShell)	Обеспечивает централизованную среду для управления службами каталогов
DNS Server tools (Средства серверов DNS)	Включает оснастку «Диспетчер DNS» для удаленного управления DNS и программу командной строки dnscmd.exe
Remote Desktop Services Tool(Средства служб удаленных рабочих столов)	Добавляет вкладку Профиль служб удаленных рабочих столов в свойства объекта пользователя ADUC и устанавливает оснастку MMC «Удаленные рабочие столы» для администрирования RDP-сервера (tsmmc.msc).

3) нажать кнопку «ОК».

10.4.3. Включение механизма применения конфигурации на клиентских машинах

Модуль панели управления операционной системы для включения механизма применения конфигурации на клиентских машинах предназначен для управления включением работы групповых политик и выбором политики по умолчанию.

Модуль панели управления операционной системы для включения механизма применения конфигурации на клиентских машинах представляет собой следующие модули ЦУС:

- «Аутентификация» (пакет alterator-auth);
- «Групповые политики» (пакет alterator-grupdate).

Включить групповые политики можно как при вводе машины в «Альт Домен», так и на уже включенной в домен рабочей станции.

Для включения групповых политик при вводе машины в домен следует в модуле ЦУС «Аутентификация» (пакет alterator-auth) выбрать пункт «Домен Active Directory», заполнить поля «Домен», «Рабочая группа» и «Имя компьютера», и нажать кнопку «Применить» (рис. 246).

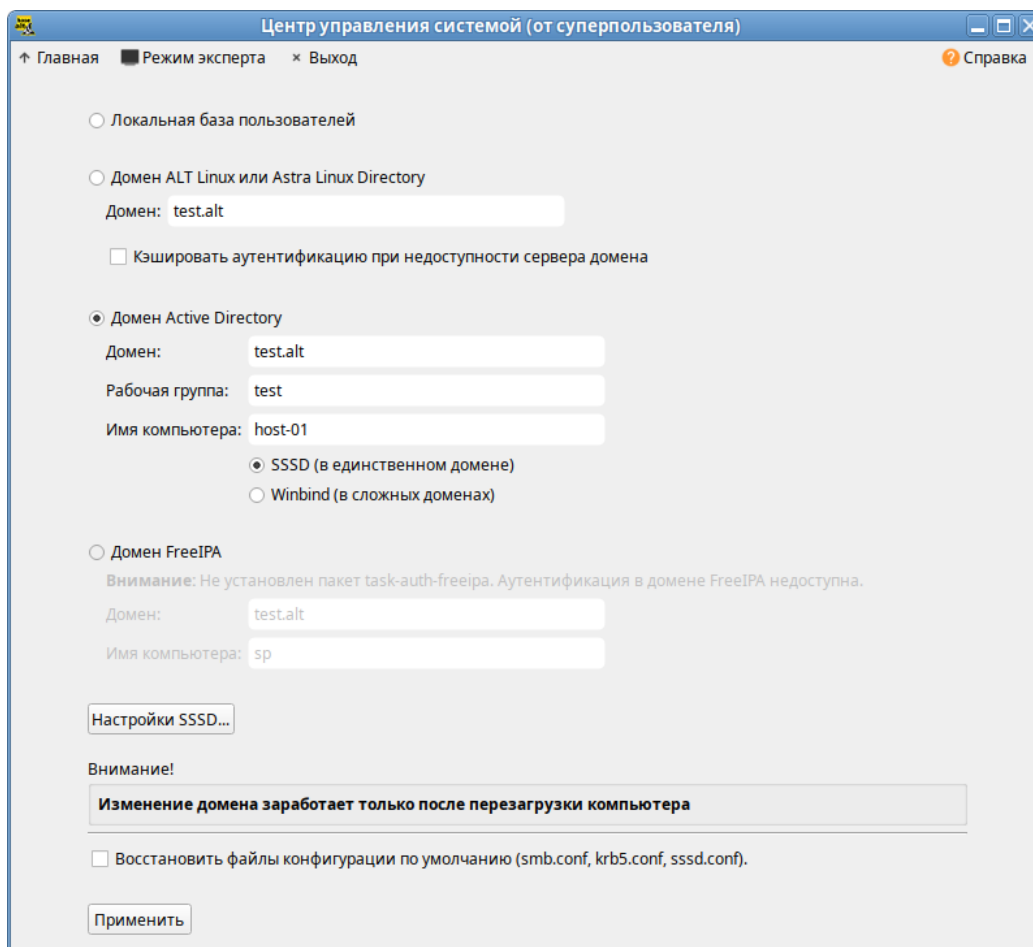


Рис. 246 – Ввод в домен в ЦУС

В открывшемся окне ввести имя пользователя, имеющего право вводить машины в домен, и его пароль, отметить пункт «Включить групповые политики» и нажать кнопку «ОК» (рис. 247).

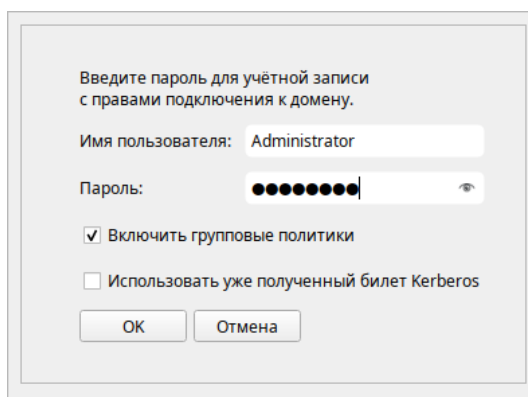


Рис. 247 – Включение групповых политик при вводе в домен

Включить поддержку управления групповыми политиками на машине, уже введенной в домен, можно в модуле ЦУС «Групповые политики» (рис. 248).

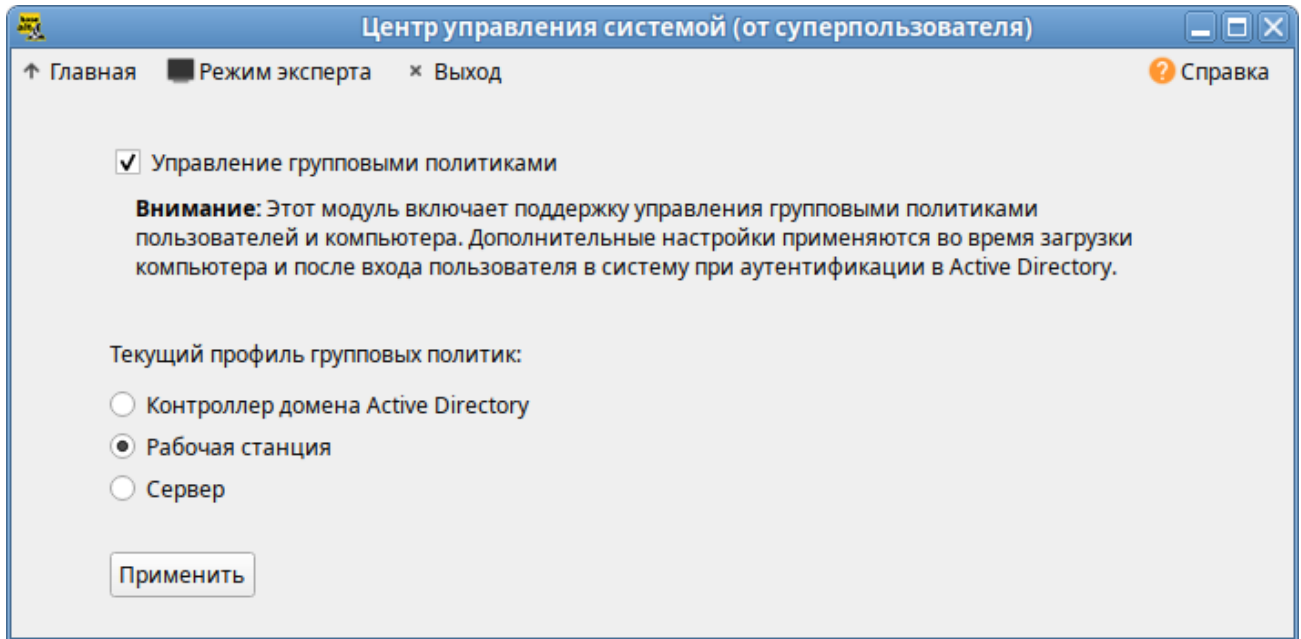


Рис. 248 – Включение поддержки управления групповыми политиками

Модуль «Групповые политики» позволяет управлять включением/выключением поддержки групповых политик на машинах, введенных в домен, а также выбирать профиль политики по умолчанию:

- «Сервер»;
- «Контроллер домена Active Directory»;
- «Рабочая станция».

Для возможности включения групповых политик на машинах под управлением ОС Альт СП, на которых не установлена графическая оболочка, модуль «Групповые политики» доступен также в веб-интерфейсе ЦУС (рис. 249).

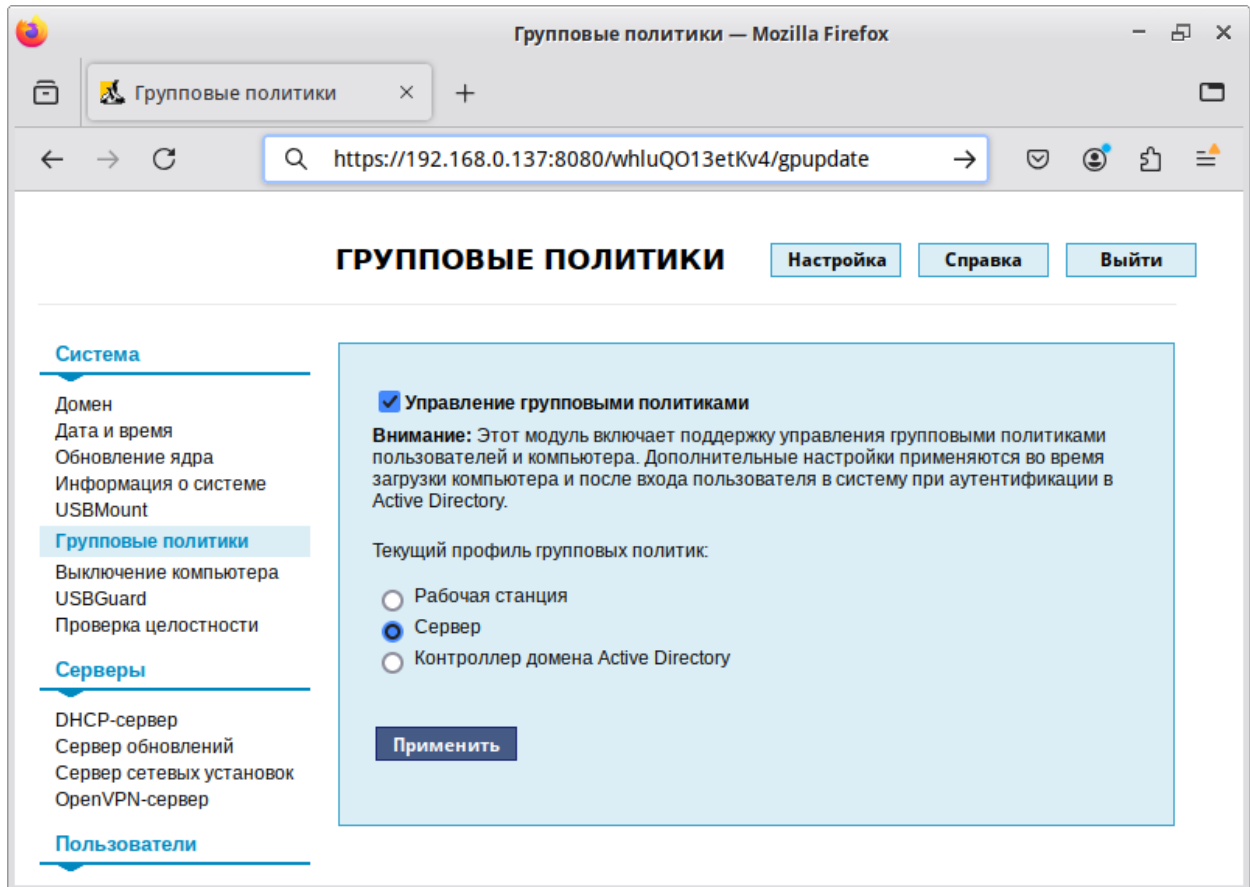


Рис. 249 – Веб-интерфейс модуля «Групповые политики»

10.4.4. Модуль клиентской машины для применения конфигурации

Модуль клиентской машины для применения конфигурации (далее – gpupdate) отвечает за применение заданных администратором системы настроек конфигурации к клиентской машине и/или пользователю машины.

ПО состоит из компонента, который авторизуется в домене и выполняет скачивание файлов настроек на клиентскую машину. Далее происходит разбор файлов настроек и складывание полученных данных в хранилище, именуемое также «реестр». Это позволяет развязать методы доставки и применения настроек.

При успешной репликации настроек запускается часть системы, называемая «фронтенд». Она отвечает за запуск различных модулей (appliers), каждый из которых отвечает за свою логическую функцию. Например, модуль firefox отвечает за вычитывание настроек для веб-браузера Mozilla Firefox и создание файла политик для него, а модуль ntp отвечает за чтение настроек, касающихся NTP-сервера, и создание подходящей конфигурации.

Количество и функционал модулей может меняться по мере развития и актуализации продукта и компонентов системы, с которыми они работают.

Групповые политики обрабатываются в следующем порядке:

- объект локальной групповой политики;
- объекты групповой политики, связанные с доменом (в рамках возможностей и ограничений поддержки леса доменов в Samba, как набора клиентских компонентов);
- объекты групповой политики, связанные с OU, обрабатываются в определенном порядке. Сначала обрабатываются объекты групповой политики, находящиеся на самом высоком уровне в иерархии службы каталогов, затем объекты групповой политики, связанные с дочерним подразделением и т. д. Последними обрабатываются объекты групповой политики, связанные с OU, в которой находится пользователь или компьютер.

Процесс применения настроек:

- настройки для машины реплицируются при запуске компьютера и далее обновляются раз в час;
- настройки для пользователя реплицируются при входе пользователя в систему и далее обновляются раз в час.

Для работы механизмов применения пользовательских настроек задействовано множество компонентов ОС, таких как systemd, D-Bus, PAM (рис. 250).

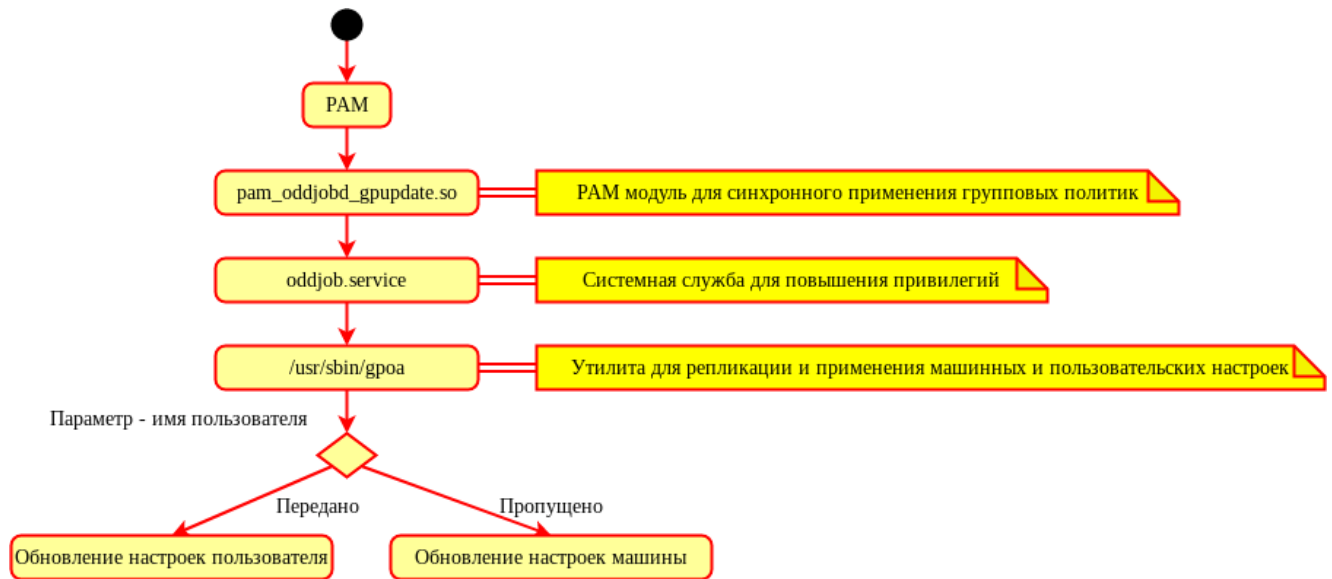


Рис. 250 – Механизм применения групповых политик

Часть проекта, отвечающая за получение и применение групповых политик, внутри использует базу данных («реестр»), для хранения настроек, полученных из различных источников.

10.4.4.1. Утилиты модуля

Модуль состоит из трех утилит:

- gpoa – системная утилита, осуществляющая применение групповых политик для компьютера или пользователя (gpoa без параметра обрабатывает только для машины, для пользователя нужно указывать username);
- gpupdate – утилита, осуществляющая запрос на применение групповых политик. При запуске с привилегиями администратора может непосредственно выполнить применение групповых политик, минуя необходимость повышения привилегий;
- gpupdate-setup – инструмент администрирования механизмов применения групповых политик. Позволяет включать и отключать применение групповых политик, а также задавать шаблон политики по умолчанию («Рабочая станция», «Сервер», «Контроллер домена»).

Синтаксис команды gpoa:

```
gpoa [-h] [--dc DC] [--nodomain] [--nouupdate] [--nopugins] [--list-backends] [--loglevel LOGLEVEL] [пользователь]
```

Опции команды `gpoa` указаны в таблице 21.

Т а б л и ц а 21 – Опции команды `gpoa`

Ключ	Описание
<code>-h, --help</code>	Вывести справку о команде
<code>--dc DC</code>	Указать полное имя (FQDN) контроллера домена для реплицирования SYSVOL
<code>--nodomain</code>	Работать без домена (применить политику по умолчанию)
<code>--nouupdate</code>	Не пытаться обновить хранилище, только запустить <code>appliers</code>
<code>--nopugins</code>	Не запускать плагины
<code>--list-backends</code>	Показать список доступных бэкэндов
<code>--loglevel LOGLEVEL</code>	Установить уровень журналирования
пользователь	Имя пользователя домена

Примеры работы с командой `gpoa`:

- получить и применить настройки для текущей машины:

```
# gpoa --loglevel 0
```

- применить кэшированные настройки для текущей машины:

```
# gpoa --nouupdate
```

- получить и применить настройки с контроллера домена `dc1.test.alt` для пользователя `ivanov`:

```
# gpoa --dc dc1.test.alt --loglevel 3 ivanov
```

- применить политику по умолчанию:

```
# gpoa --nodomain --loglevel 0
```

Синтаксис команды `gpupdate`:

```
gpupdate [-h] [-u USER] [-t {ALL,USER,COMPUTER}] [-l LOGLEVEL] [-s]
```

Опции команды `gpupdate` указаны в таблице 22.

Т а б л и ц а 22 – Опции команды `gpupdate`

Ключ	Описание
<code>-h, --help</code>	Вывести справку о команде
<code>-u USER,</code> <code>--user USER</code>	Имя пользователя для обновления GPO
<code>--target TARGET</code>	Указать политики, которые нужно обновить (пользователя или компьютера). Возможные значения: All (по умолчанию), Computer, User
<code>--loglevel LOGLEVEL</code>	Установить уровень журналирования
<code>-s, --system</code>	Запустить <code>gpupdate</code> в системном режиме

Только root может указать любое имя пользователя для обновления.

Пользователь может выполнять groupdate только для машины или самого себя.

Примеры работы с командой groupdate:

- получить и применить настройки для текущей машины:

```
$ groupdate --target Computer
Apply group policies for computer.
```

- получить и применить настройки для текущего пользователя:

```
$ groupdate --target User
Apply group policies for kudrin.
```

- получить и применить настройки для текущего пользователя и машины:

```
$ groupdate
Apply group policies for kudrin.
```

- попытаться получить настройки для пользователя ivanov (с правами пользователя kim):

```
$ groupdate -u ivanov --target User --loglevel 0
2024-06-10 17:17:18.113|[D00010]| Групповые политики будут обновлены
для указанной цели|{'target': 'USER'}
2024-06-10 17:17:18.113|[W00002]| Текущий уровень привилегий не
позволяет выполнить groupdate для указанного пользователя. Будут
обновлены настройки текущего пользователя.|{'username': 'kim'}
2024-06-10 17:17:18.118|[D00013]| Запускается GPOA обращением к
oddjobd через D-Bus|{}
2024-06-10 17:17:18.119|[D00900]| Неизвестный отладочный
код|{'bus_name': 'ru.basealt.oddjob_groupdate'}
2024-06-10 17:17:18.119|[D00006]| Запускается GPOA для пользователя
обращением к oddjobd через D-Bus|{'username': 'kim'}
2024-06-10 17:17:37.972|[D00012]| Получен код возврата из
утилиты|{'retcode': dbus.Int32(0)}
Apply group policies for kim.
```

- попытаться получить настройки для пользователя ivanov (с правами суперпользователя):

```
# groupdate -u ivanov --target User --loglevel 0
2024-06-10 17:19:53.960|[D00010]| Групповые политики будут обновлены
для указанной цели|{'target': 'USER'}
2024-06-10 17:19:53.978|[D00013]| Запускается GPOA обращением к
oddjobd через D-Bus|{}
2024-06-10 17:19:53.979|[D00900]| Неизвестный отладочный
код|{'bus_name': 'ru.basealt.oddjob_groupdate'}
2024-06-10 17:19:53.979|[D00006]| Запускается GPOA для пользователя
обращением к oddjobd через D-Bus|{'username': 'ivanov'}
2024-06-10 17:20:13.852|[D00012]| Получен код возврата из
утилиты|{'retcode': dbus.Int32(0)}
Apply group policies for ivanov.
```

Синтаксис команды `gpupdate-setup`:

`gpupdate-setup [-h]` действие

Опции команды `gpupdate-setup` указаны в таблице 23.

Т а б л и ц а 23 – Опции команды `gpupdate-setup`

Ключ	Описание
<code>list</code>	Показать список доступных типов локальной политики
<code>list-backends</code>	Показать список доступных бэкэндов
<code>status</code>	Показать текущий статус групповой политики (действие по умолчанию)
<code>enable</code>	Включить подсистему групповой политики
<code>disable</code>	Отключить подсистему групповой политики
<code>update</code>	Обновить состояние. Проверяет, в каком состоянии находилась служба <code>gpupdate</code> . В случае, если служба <code>gpupdate</code> запущена, <code>gpupdate-setup</code> также запустит весь перечень служб (например, <code>gpupdate-run-scripts</code>)
<code>write</code>	Операции с групповыми политиками (включить, отключить, указать тип политики по умолчанию)
<code>set-backend</code>	Установить или изменить активную в данный момент серверную часть (бэкэнд)
<code>default-policy</code>	Показать название политики по умолчанию
<code>active-policy</code>	Показать название текущего профиля политики
<code>active-backend</code>	Показать текущий настроенный бэкэнд

Примеры работы с командой `gpupdate-setup`:

- просмотр текущего состояния подсистемы групповых политик:

```
# gpupdate-setup
disabled
```

- включение групповых политик (для включения через ЦУС доступен соответствующий графический модуль управления, а также отметка во время введения машины в домен см. п. 10.3.3.2.2):

```
# gpupdate-setup enable
workstation

Created symlink /etc/systemd/user/default.target.wants/gpupdate-
user.service → /usr/lib/systemd/user/gpupdate-user.service.
Created symlink /etc/systemd/system/multi-
user.target.wants/gpupdate-scripts-run.service →
/lib/systemd/system/gpupdate-scripts-run.service.
Created symlink /etc/systemd/user/default.target.wants/gpupdate-
scripts-run-user.service → /usr/lib/systemd/user/gpupdate-
scripts-run-user.service.
Created symlink
/etc/systemd/system/timers.target.wants/gpupdate.timer →
/lib/systemd/system/gpupdate.timer.
Created symlink /etc/systemd/user/timers.target.wants/gpupdate-
user.timer → /usr/lib/systemd/user/gpupdate-user.timer.
```

```
# control system-policy
gpupdate
```

- выключение групповых политик:

```
# gpupdate-setup disable

Removed /etc/systemd/system/multi-
user.target.wants/gpupdate.service.
Removed /etc/systemd/user/default.target.wants/gpupdate-
user.service.
Removed /etc/systemd/system/timers.target.wants/gpupdate.timer.
Removed /etc/systemd/user/timers.target.wants/gpupdate-
user.timer.
Removed /etc/systemd/system/multi-user.target.wants/gpupdate-
scripts-run.service.
Removed /etc/systemd/user/default.target.wants/gpupdate-scripts-
run-user.service.
```

- вывод списка доступных бэкендов:

```
# gpupdate-setup list-backends
local
samba
```

- включение групповых политик и установка профиля политики по умолчанию server:

```
# gpupdate-setup write enable server
```

По умолчанию, нет необходимости конфигурирования gpupdate. Однако в файле `/etc/gpupdate/gpupdate.ini` можно указать в явном виде следующие опции:

1) раздел `[gpoa]`:

- `backend` – способ получения настроек;
- `local-policy` – профиль политики по умолчанию, который будет применен сразу после загрузки ОС (`ad-domain-controller`, `workstation`, `server`, `default`);

2) раздел `[samba]`:

- `dc` – контроллер домена, с которого нужно обновлять групповые политики.

Пример файла `/etc/gpupdate/gpupdate.ini` на контроллере домена:

```
[gpoa]
backend = samba
local-policy = ad-domain-controller
```

Пример файла `/etc/gpupdate/gpupdate.ini` на рабочей станции:

```
[gpoa]
backend = samba
local-policy = workstation
```

В следующем примере указан пустой профиль локальной политики. Указать пустой профиль бывает нужно для тестирования групповых политик, чтобы они не наслаивались на локальные политики:

```
[gpoa]
backend = samba
local-policy = /usr/share/local-policy/default

[samba]
dc = dcl.test.alt
```

10.4.4.2. Локальная политика

Настройки локальной политики находятся в каталоге `/usr/share/local-policy/`. Данные настройки по умолчанию поставляются пакетом `local-policy`. Администраторы инфраструктур имеют возможность поставлять собственный пакет с локальной политикой и разворачивать ее единообразно на всех клиентах. Формат шаблонов политик, по умолчанию, представляет собой архивный формат политик Samba с дополнительными модификациями. Состав локальной политики может меняться или адаптироваться системным администратором (таблица 24).

Т а б л и ц а 24 – Состав локальной политики

Параметры	Описание	Комментарий
<code>oddjobd.service</code>	Включение <code>oddjobd.service</code> (механизм <code>Systemd</code>)	Нужно для обеспечения возможности запуска <code>gpupdate</code> для пользователя с правами администратора
<code>gpupdate.service</code>	Включение <code>gpupdate.service</code> (механизм <code>Systemd</code>)	Нужно для регулярного обновления настроек машины
<code>sshd.service</code>	Включение <code>sshd.service</code> (механизм <code>Systemd</code>)	Нужно для обеспечения возможности удаленного администрирования
<code>sshd-gssapi-auth, ssh-gssapi-auth</code>	Включение аутентификации с помощью GSSAPI на сервере OpenSSH (механизм <code>Control</code>)	Отвечает за возможность аутентификации в домене при доступе через SSH
<code>sshd-allow-groups, sshd-allow-groups-list</code>	Ограничение аутентификации на сервере OpenSSH по группам <code>wheel</code> и <code>remote</code> (механизм <code>Control</code>)	Нужно для ограничения доступа при доступе через SSH для всех пользователей домена (только при наличии соответствующей привилегии)

Окончание таблицы 24

Параметры	Описание	Комментарий
system-policy	Применяет групповые политики при логине (механизм Control)	
OpenSSH	Открытие порта 22	Нужно для обеспечения возможности подключения по SSH на машинах при старте Firewall applier

Пример локальной политики (файл

/usr/share/local-policy/workstation/Machine/Registry.pol.xml):

```
<?xml version="1.0" encoding="utf-8"?>
<PolFile num_entries="9" signature="PReg" version="1">
  <Entry type="1" type_name="REG_SZ">
    <Key>Software\BaseALT\Policies\Control</Key>
    <ValueName>sshd-gssapi-auth</ValueName>
    <Value>enabled</Value>
  </Entry>
  <Entry type="1" type_name="REG_SZ">
    <Key>Software\BaseALT\Policies\Control</Key>
    <ValueName>ssh-gssapi-auth</ValueName>
    <Value>enabled</Value>
  </Entry>
  <Entry type="1" type_name="REG_SZ">
    <Key>Software\BaseALT\Policies\Control</Key>
    <ValueName>sshd-allow-groups</ValueName>
    <Value>enabled</Value>
  </Entry>
  <Entry type="1" type_name="REG_SZ">
    <Key>Software\BaseALT\Policies\Control</Key>
    <ValueName>sshd-allow-groups-list</ValueName>
    <Value>remote</Value>
  </Entry>
  <Entry type="1" type_name="REG_SZ">
    <Key>Software\BaseALT\Policies\Control</Key>
    <ValueName>system-policy</ValueName>
    <Value>gpupdate</Value>
  </Entry>
  <Entry type="4" type_name="REG_DWORD">
    <Key>Software\BaseALT\Policies\SystemdUnits</Key>
    <ValueName>odddjobd.service</ValueName>
    <Value>1</Value>
  </Entry>
  <Entry type="4" type_name="REG_DWORD">
    <Key>Software\BaseALT\Policies\SystemdUnits</Key>
    <ValueName>sshd.service</ValueName>
    <Value>1</Value>
  </Entry>
  <Entry type="4" type_name="REG_DWORD">
    <Key>Software\BaseALT\Policies\SystemdUnits</Key>
    <ValueName>gpupdate.service</ValueName>
```

```

    <Value>1</Value>
  </Entry>
  <Entry type="1" type_name="REG_SZ">

  <Key>SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules</Key>
    <ValueName>OpenSSH</ValueName>

  <Value>v2.20|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=22|
  Name=Open SSH port|Desc=Open SSH port|</Value>
  </Entry>
</PolFile>

```

Локальную политику рекомендуется править только опытным администраторам.

10.4.4.3. Ключи реестра

Ключи реестра, полученные из объектов групповой политики (GPO), хранятся в Dconf.

Машинные политики хранятся в файле `/etc/dconf/db/policy.d/policy.ini`, политики пользователя – в файле `/etc/dconf/db/policy<UID>.d/policy<UID>.ini` (где UID – идентификатор пользователя в системе).

Отследить какие политики «прилетели» на машину клиента можно, выполнив команду:

```
dconf dump /
```

При выполнении этой команды с правами доменного пользователя будут выведены машинные политики и политики данного пользователя, при выполнении с правами пользователя root будут выведены только машинные политики.

Пример результата выполнения команды `dconf` с правами доменного пользователя:

```

$ dconf dump /
[SOFTWARE/Policies/Microsoft/WindowsFirewall/FirewallRules]
OpenSSH='v2.20|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=22|Name=Open SSH port|Desc=Open SSH port|'

[Software/BaseALT/Policies/Control]
ssh-gssapi-auth='enabled'
sshd-allow-groups='enabled'
sshd-allow-groups-list='remote'

```


JKHB.11100-01 90 03

```
sshd-gssapi-auth='enabled'  
system-policy='gpupdate'
```

```
[Software/BaseALT/Policies/ReadQueue/Machine]  
0="('Local Policy', '/var/cache/gpupdate/local-policy', None)"  
1="('Firefox',  
'/var/cache/samba/gpo_cache/TEST.ALT/POLICIES/{0CCFA74C-57F5-  
42B5-98E2-007D4A59C4C4}', 262148) "
```

```
[Software/BaseALT/Policies/ReadQueue/User]  
0="('nm',  
'/var/cache/samba/gpo_cache/TEST.ALT/POLICIES/{6F65CD4D-9209-  
4A81-9801-17A35CEE5CFD}', 131074) "
```

```
[Software/BaseALT/Policies/SystemdUnits]  
gpupdate.service=1  
oddjobd.service=1  
sshd.service=1
```

```
[Software/Policies/Mozilla/Firefox]  
DisableMasterPasswordCreation=1  
PasswordManagerEnabled=1  
ShowHomeButton=1
```

```
[Software/Policies/Mozilla/Firefox/Authentication]  
SPNEGO="['.test.alt']"
```

```
[Software/Policies/Mozilla/Firefox/Homepage]  
Locked=1  
URL='https://basealt.ru'
```

```
[org/gnome/evolution-data-server]  
migrated=true  
network-monitor-gio-name=''
```

```
[org/mate/caja/window-state]  
geometry='800x550+310+75'  
maximized=false  
start-with-sidebar=true  
start-with-status-bar=true  
start-with-toolbar=true
```

```
[org/mate/desktop/accessibility/keyboard]  
bouncekeys-beep-reject=true  
bouncekeys-delay=300  
bouncekeys-enable=false
```

```
enable=false
feature-state-change-beep=false
mousekeys-accel-time=1200
mousekeys-enable=false
mousekeys-init-delay=160
mousekeys-max-speed=750
slowkeys-beep-accept=true
slowkeys-beep-press=true
slowkeys-beep-reject=false
slowkeys-delay=300
slowkeys-enable=false
stickykeys-enable=false
stickykeys-latch-to-lock=true
stickykeys-modifier-beep=true
stickykeys-two-key-off=true
timeout=120
timeout-enable=false
togglekeys-enable=false

[org/mate/desktop/session]
session-start=1718111448

[org/mate/mate-menu/plugins/applications]
last-active-tab=0

[org/mate/panel/general]
object-id-list=['menu-bar', 'show-desktop', 'workspace-switcher',
'window-list', 'notification-area', 'clock']
toplevel-id-list=['bottom']

[org/mate/panel/objects/clock]
applet-iid='ClockAppletFactory::ClockApplet'
locked=true
object-type='applet'
panel-right-stick=true
position=0
toplevel-id='bottom'

[org/mate/panel/objects/clock/prefs]
custom-format=''
format='24-hour'

[org/mate/panel/objects/menu-bar]
applet-iid='MateMenuAppletFactory::MateMenuApplet'
has-arrow=false
locked=true
```

```
object-type='applet'  
position=0  
toplevel-id='bottom'
```

```
[org/mate/panel/objects/notification-area]  
applet-iiid='NotificationAreaAppletFactory::NotificationArea'  
locked=true  
object-type='applet'  
panel-right-stick=true  
position=10  
toplevel-id='bottom'
```

```
[org/mate/panel/objects/show-desktop]  
applet-iiid='WnckletFactory::ShowDesktopApplet'  
locked=true  
object-type='applet'  
position=1  
toplevel-id='bottom'
```

```
[org/mate/panel/objects/window-list]  
applet-iiid='WnckletFactory::WindowListApplet'  
locked=true  
object-type='applet'  
position=20  
toplevel-id='bottom'
```

```
[org/mate/panel/objects/workspace-switcher]  
applet-iiid='WnckletFactory::WorkspaceSwitcherApplet'  
locked=true  
object-type='applet'  
position=10  
toplevel-id='bottom'
```

```
[org/mate/panel/toplevels/bottom]  
expand=true  
orientation='bottom'  
screen=0  
size=28  
y=836  
y-bottom=0
```

```
[org/mate/terminal/profiles/default]  
background-color='#2C2C2C2C2C2C'  
background-darkness=0.94999999999999996  
background-type='transparent'  
bold-color='#000000000000'
```

```

foreground-color='#F5F5F5F5E4E4'
palette='#2E2E34343636:#CCCC00000000:#4E4E9A9A0606:#C4C4A0A00000:
#34346565A4A4:#757550507B7B:#060698209A9A:#D3D3D7D7CFCF:#5555757
5353:#EFEF29292929:#8A8AE2E23434:#FCFCE9E94F4F:#72729F9FCFCF:#ADA
D7F7FA8A8:#3434E2E2E2E2:#EEEEEEEEEECEC'
use-theme-colors=false
visible-name='По умолчанию'

```

10.4.4.4. Модули клиентской стороны (Applier)

На клиентский компьютер должны распространяться параметры политики, указанные в соответствующем объекте ГП.

Каждая группа параметров групповой политики обслуживается определенным модулем (Applier) клиентской стороны (таблица 25).

Т а б л и ц а 25 – Список модулей

Расширение клиентской стороны	Модуль	Описание
Управление control framework	control	Управляет фреймворком control. Может быть вызван только машинной политикой. Принцип работы – вызвать утилиту control с нужным параметром
Управление настройками PolKit	polkit	Управляет генерацией настроек PolicyKit. Работа с правилами PolicyKit ведется методом генерации файлов .rules
Управление настройками PolKit	polkit_user	Управляет генерацией настроек PolicyKit в контексте пользователя
Включение или выключение различных служб	systemd	Управление включением или выключением сервисов systemd. Данный applier реализован только для машин. Его функция – включение или выключение systemd units (при их наличии). Applier способен обрабатывать параметры, полученные из PReg файлов (через ADMX) в виде ветвей реестра
Настройка веб-браузера Chromium	chromium	Генерирует файл политики для Chromium (policies.json). Данные настройки устанавливаются из ADMX-файлов для Chromium. Может быть вызван только машинной политикой.
Настройка веб-браузера Firefox	firefox	Генерирует файл политики для Firefox (policies.json). Данные настройки устанавливаются из ADMX-файлов для Firefox. Может быть вызван только машинной политикой.
Настройка Яндекс.Браузер	yandex_browser	Генерирует файл политики для Яндекс.Браузера (policies.json). Данные настройки устанавливаются из ADMX-файлов для Яндекс.Браузера. Может быть вызван только машинной политикой.
Управление ярлыками запуска программ	shortcuts	Управляет .desktop файлами (создание/удаление/замена)

Продолжение таблицы 25

Расширение клиентской стороны	Модуль	Описание
Управление ярлыками запуска программ	shortcuts_user	Управляет .desktop файлами в контексте пользователя. Способен реагировать на опцию выполнения операций в контексте администратора или пользователя
Управление подключением сетевых дисков	cifs	Управляет подключением сетевых дисков
Управление подключением сетевых дисков	cifs_user	Управляет подключением сетевых дисков в контексте пользователя
Управление каталогами файловой системы	folder	Управляет каталогами файловой системы (создание/удаление/пересоздание)
Управление каталогами файловой системы	folder_user	Управляет каталогами файловой системы в контексте пользователя
Управление файлами	files	Управляет файлами (создание/удаление/пересоздание)
Управление файлами	files_user	Управляет файлами в контексте пользователя
Управление INI-файлами	inifiles	Управляет INI-файлами (создание/удаление/пересоздание)
Управление INI-файлами	inifiles_user	Управляет INI-файлами в контексте пользователя
Управление переменными среды	envar	Управляет переменными среды
Управление переменными среды	envar_user	Управляет переменными среды в контексте пользователя
Управление общими каталогами	networkshares	Управляет общими каталогами
Управление общими каталогами	networkshares_user	Управляет общими каталогами в контексте пользователя
Управление общими каталогами	networkshares	Управляет общими каталогами
Управление общими каталогами	networkshares_user	Управляет общими каталогами в контексте пользователя

Окончание таблицы 25

Расширение клиентской стороны	Модуль	Описание
Управление gsettings (настройки графической среды MATE)	gsettings_user	Устанавливает настройки gsettings для пользователя
Управление настройками графической среды KDE	kde	Средство управления настройками среды рабочего стола KDE
Управление настройками графической среды KDE	kde_user	Устанавливает настройки KDE в контексте пользователя
Управление пакетами	package	Средство работы с пакетным менеджером для установки и удаления пакетов программ
Управление пакетами	package_user	Управление пакетами в контексте пользователя
Управление logon-скриптами	scripts	Управление скриптами
Управление logon-скриптами	scripts_user	Управление скриптами в контексте пользователя

Модель групповых политик вызывает Applier отвечающие за внесение изменений, согласно параметрам политики. Для выполнения настроек, указанных в параметрах групповой политики, расширения клиентской стороны изменяют конкретные параметры операционной системы. Изменения, внесенные в операционную систему при помощи модуля групповых политик, записываются в журналы событий.

10.4.4.5. Периодичность запуска групповых политик

Каждый фронтенд срабатывает на определенные ветки настроек. Запуск фронтенда для машины по умолчанию производится раз в час средством Systemd – gupdate.timer. Запуск фронтенда для пользователя в административном контексте производится с помощью модуля pam_oddjob при входе в систему и далее раз в час (по умолчанию) также средством Systemd – gupdate-user.timer.

Для мониторинга и контроля времени выполнения службы gupdate.service используются системный таймер gupdate.timer и пользовательский таймер

`gpubdate-user.timer`. Для управления периодом запуска групповых политик достаточно изменить параметр соответствующего таймера `systemd` (по умолчанию период запуска составляет 1 час).

Изменить периодичность запуска системного таймера можно, изменив значение параметра `OnUnitActiveSec` в файле

`/lib/systemd/system/gpubdate.timer`:

```
[Unit]
Description=Run gpubdate every hour
[Timer]
OnStartupSec=1
OnUnitActiveSec=60min

[Install]
WantedBy=timers.target
```

По умолчанию таймер `gpubdate.timer` запустится после загрузки ОС, а затем будет запускаться каждый час во время работы системы. Просмотреть статус системного таймера можно, выполнив команду:

```
# systemctl status gpubdate.timer
● gpubdate.timer - Run gpubdate every hour
Loaded: loaded (/lib/systemd/system/gpubdate.timer; enabled;
vendor preset: disabled)
Active: active (waiting) since Mon 2024-06-10 16:39:44 EET; 5min
ago
Trigger: Mon 2024-06-10 17:29:17 EET; 43min left
Triggers: ● gpubdate.service

июн 10 16:39:44 w2.test.alt systemd[1]: Started Run gpubdate
every hour.
```

Изменить периодичность запуска пользовательского таймера можно, изменив в файле `/usr/lib/systemd/user/gpubdate-user.timer` значение параметра `OnUnitActiveSec`:

```
[Unit]
Description=Run gpubdate-user every hour

[Timer]
OnStartupSec=1
OnUnitActiveSec=60min

[Install]
WantedBy=timers.target
```

По умолчанию таймер `gpupdate-user.timer` запустится после входа пользователя в систему, а затем будет запускаться каждый час, пока активен сеанс соответствующего пользователя. Просмотреть статус пользовательского таймера можно, выполнив команду от имени пользователя:

```
$ systemctl --user status gpupdate-user.timer
● gpupdate-user.timer - Run gpupdate-user every hour
Loaded: loaded (/usr/lib/systemd/user/gpupdate-user.timer;
enabled; vendor preset: enabled)
Active: active (waiting) since Mon 2024-06-10 16:29:32 EET; 10min
ago
Trigger: Mon 2024-06-10 17:29:32 EET; 49min left
Triggers: ● gpupdate-user.service

июн 10 16:29:32 w2.test.alt systemd[3469]: Started Run gpupdate-
user every hour.
```

Чтобы изменения, внесенные в файл `/usr/lib/systemd/user/gpupdate-user.timer`, вступили в силу, следует выполнить команду:

```
$ systemctl --user daemon-reload
```

Примечание. Управлять периодичностью запуска `gpupdate` можно также через групповые политики (см. п. 10.4.6.5.10).

Просмотреть список запущенных системных таймеров можно, выполнив команду:

```
$ systemctl list-timers
```

Просмотреть список запущенных пользовательских таймеров можно, выполнив команду:

```
$ systemctl --user list-timers
```

10.4.5. Модуль удаленного управления базой данных конфигурации (ADMC)

Компонент удаленного управления базой данных конфигурации (далее – ADCM) предназначен для управления:

- объектами в домене (пользователями, группами, компьютерами, подразделениями);
- групповыми политиками.

ADMC позволяет:

- создавать и администрировать учетные записи пользователей, компьютеров и групп;
- менять пароли пользователя;
- создавать организационные подразделения, для структурирования и выстраивания иерархической системы распределения учетных записей в домене;
- просматривать и редактировать атрибуты объектов;
- создавать и просматривать объекты групповых политик;
- выполнять поиск объектов по разным критериям;
- сохранять поисковые запросы;
- переносить поисковые запросы между компьютерами (выполнять экспорт и импорт поисковых запросов).

В ADMC реализована функция поиска объектов групповых политик.

10.4.5.1. Запуск ADMC

Запуск ADMC осуществляется из меню запуска приложений: пункт «Системные» → «ADMC» или из командной строки (команда `admc`).

Примечание. Для использования ADMC нужно предварительно получить ключ Kerberos для администратора домена. Получить ключ Kerberos можно, например, выполнив следующую команду:

```
$ kinit administrator
```

10.4.5.2. Интерфейс ADMC

Интерфейс ADMC приведен на рис. 251.

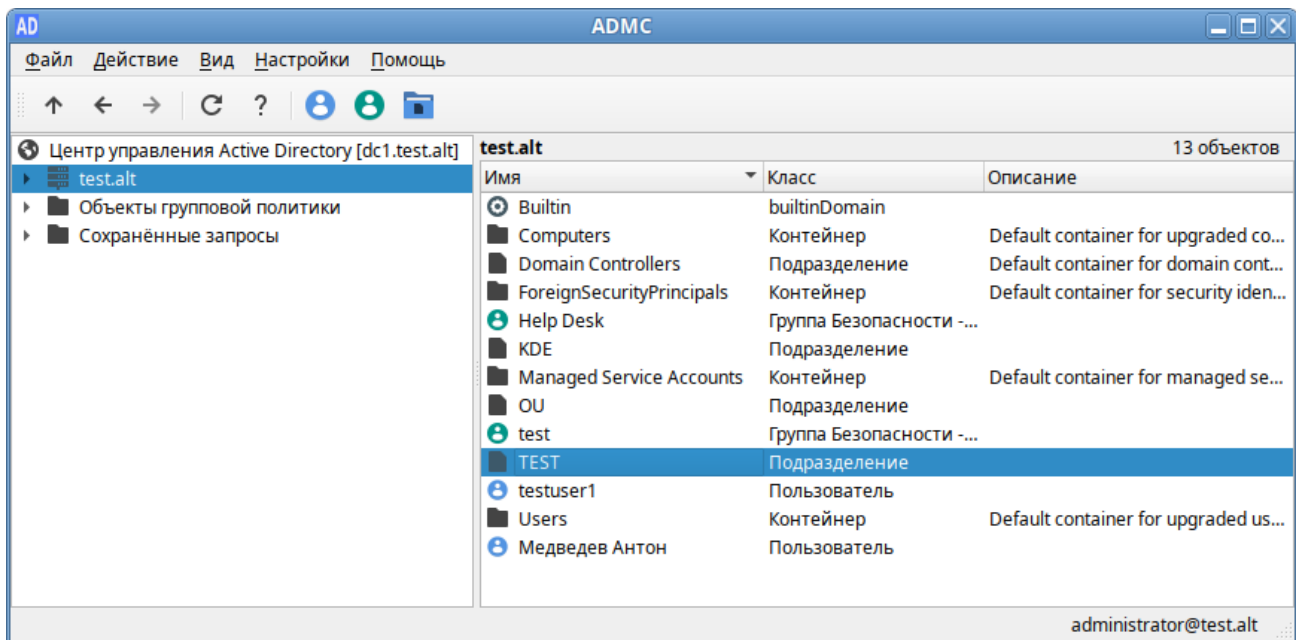


Рис. 251 – Интерфейс ADMC

Включить/выключить отображение панелей можно, отметив соответствующий пункт в меню «Вид» (рис. 252).

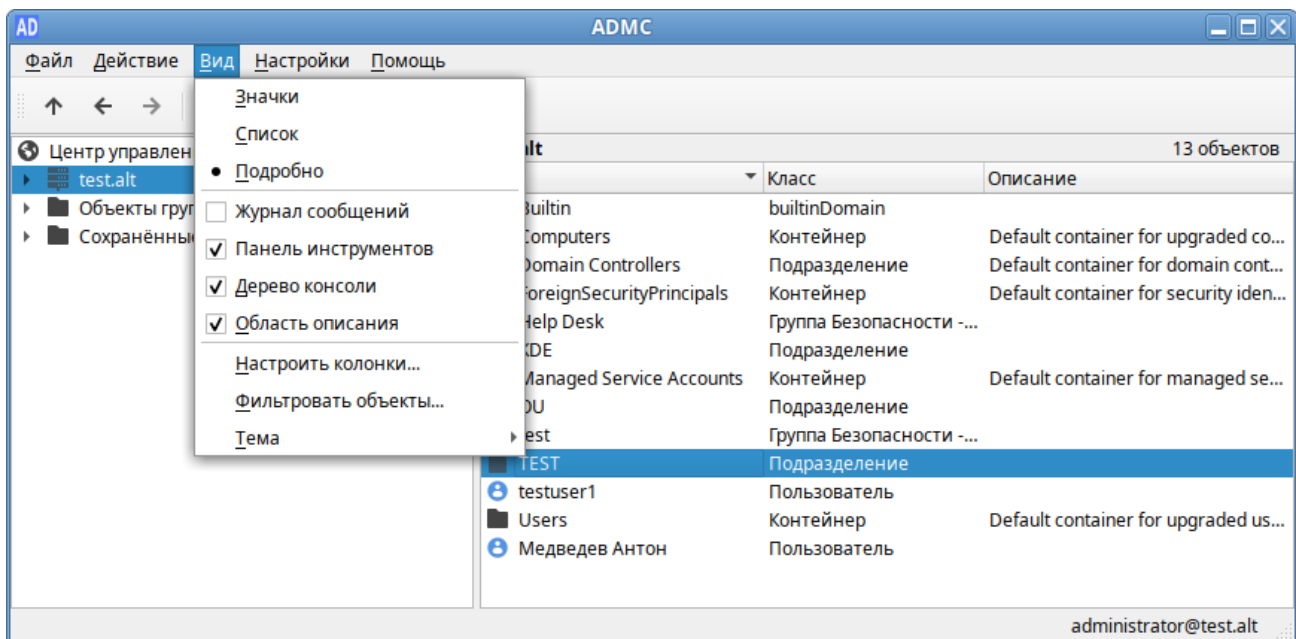


Рис. 252 – Включение/выключение отображения панелей

В панели «Журнала сообщений» отображаются сообщения о статусе приложения. Эти сообщения содержат отчеты обо всех выполненных действиях над объектами (рис. 253).

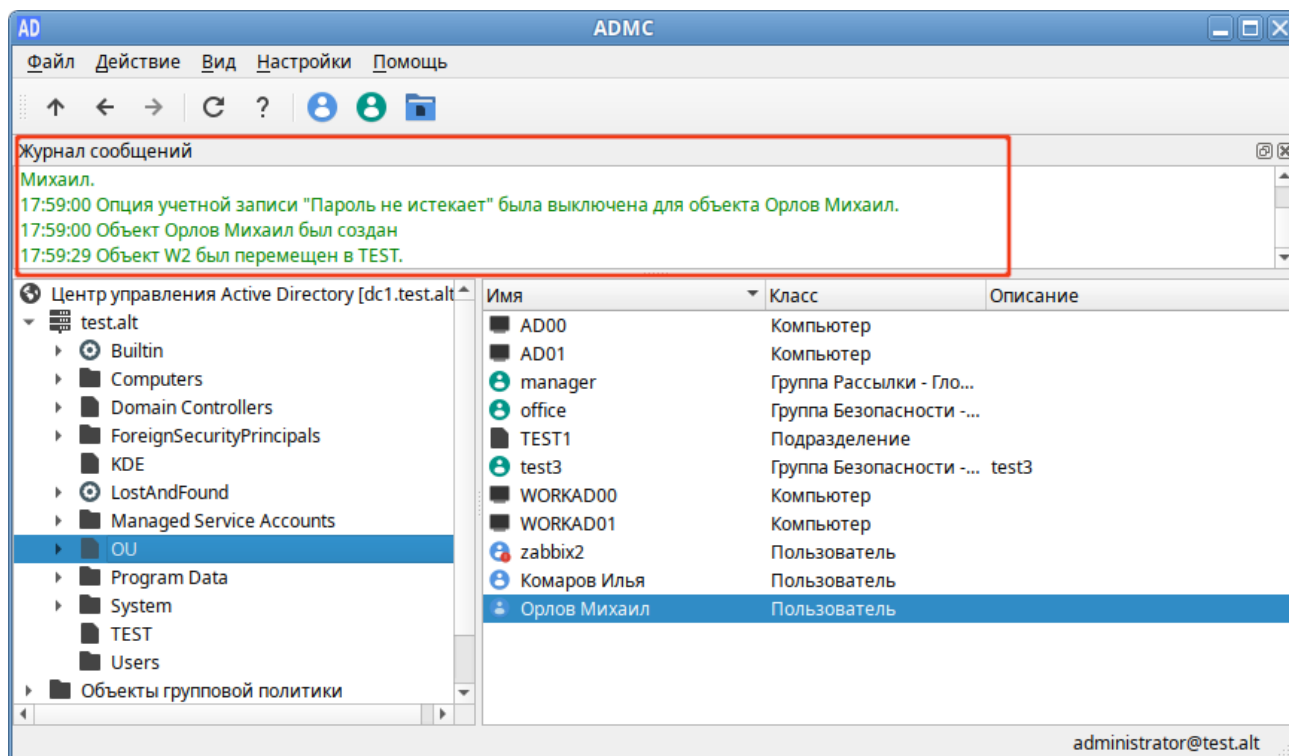


Рис. 253 – Панель «Журнал сообщений»

«Панель инструментов» содержит кнопки для быстрого запуска некоторых действий (рис. 254).

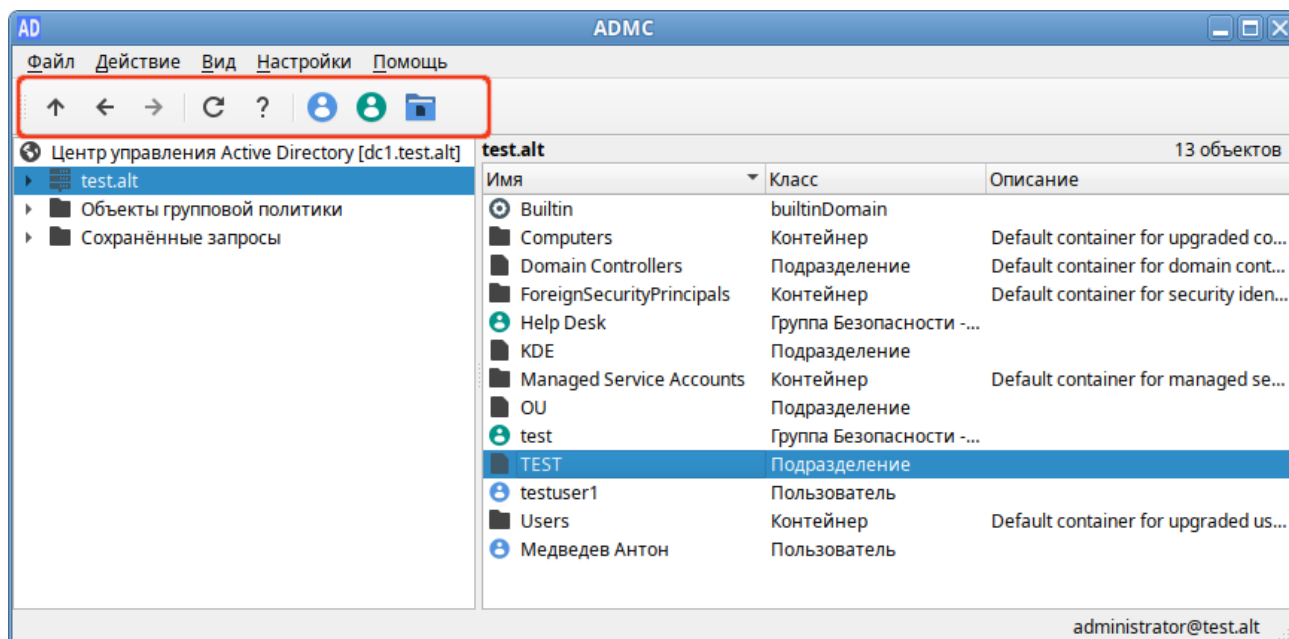


Рис. 254 – «Панель инструментов»

Панель дерева объектов домена («Дерево консоли») отображается слева, в правой панели будут отображаться сведения о выбранном объекте. По умолчанию в дереве отображаются объекты типа «контейнер» (рис. 255).

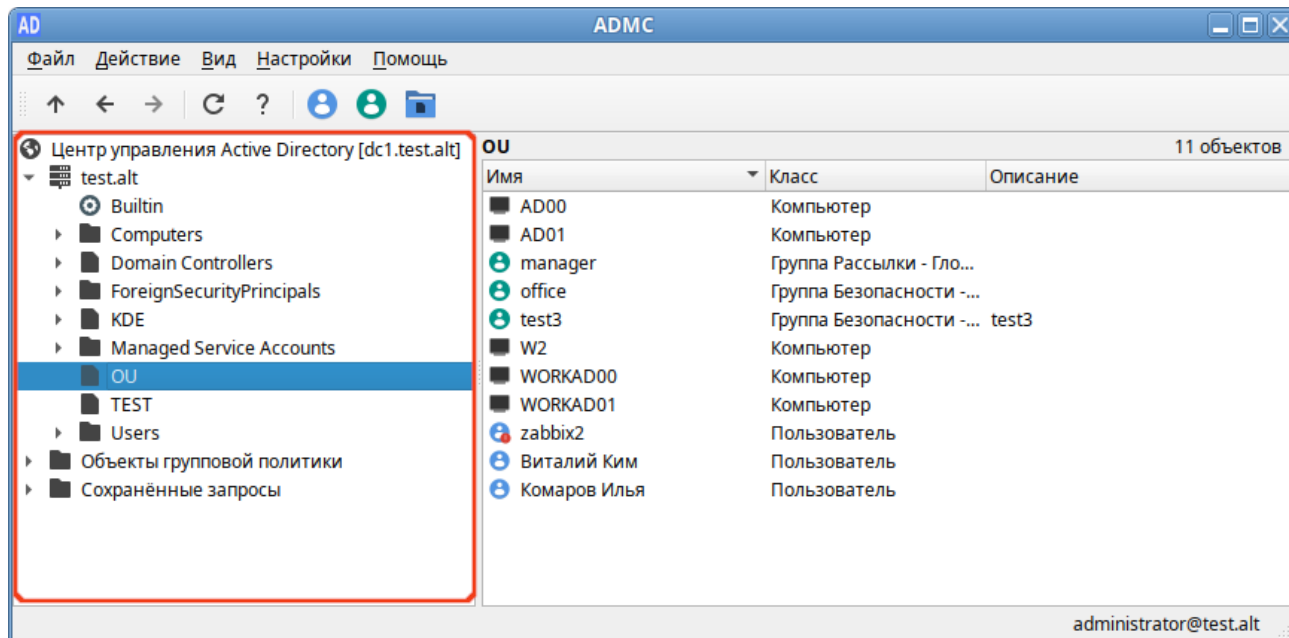


Рис. 255 – Панель «Дерево консоли»

В области описания отображается название контейнера и количество объектов в контейнере (рис. 256).

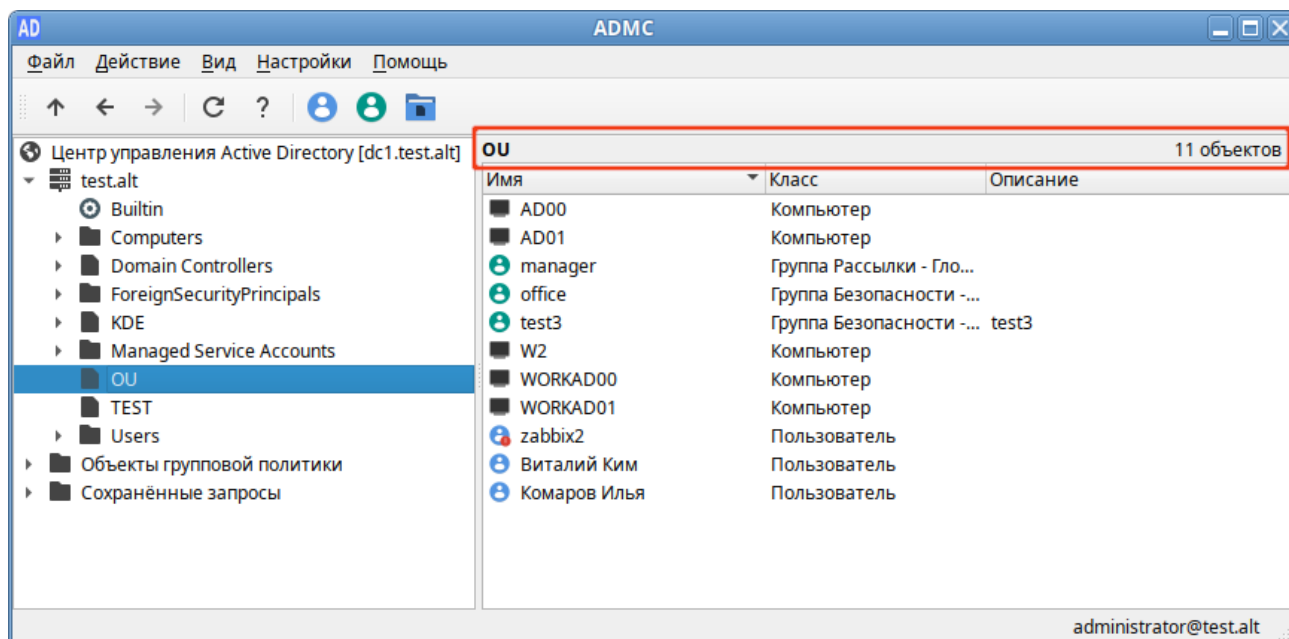


Рис. 256 – Панель «Область описания»

В меню «Вид» → «Тема» можно выбрать тему значков (рис. 257).

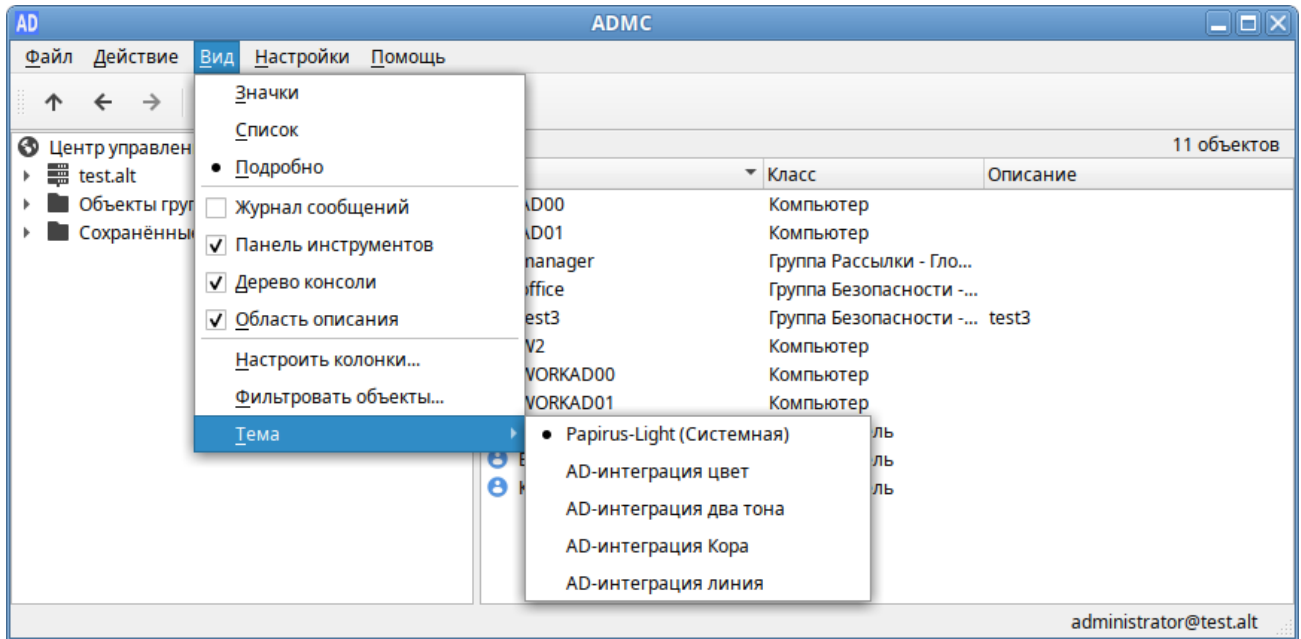


Рис. 257 – Выбор темы

Системная тема берется из каталога `/usr/share/icons`, пользовательские темы берутся по умолчанию из каталога `/usr/share/ad-integration`. Каталоги с темами определяются по наличию в них файла `index.theme` и могут быть символическими ссылками.

В меню «Настройки» можно изменить параметры ADMC (рис. 258).

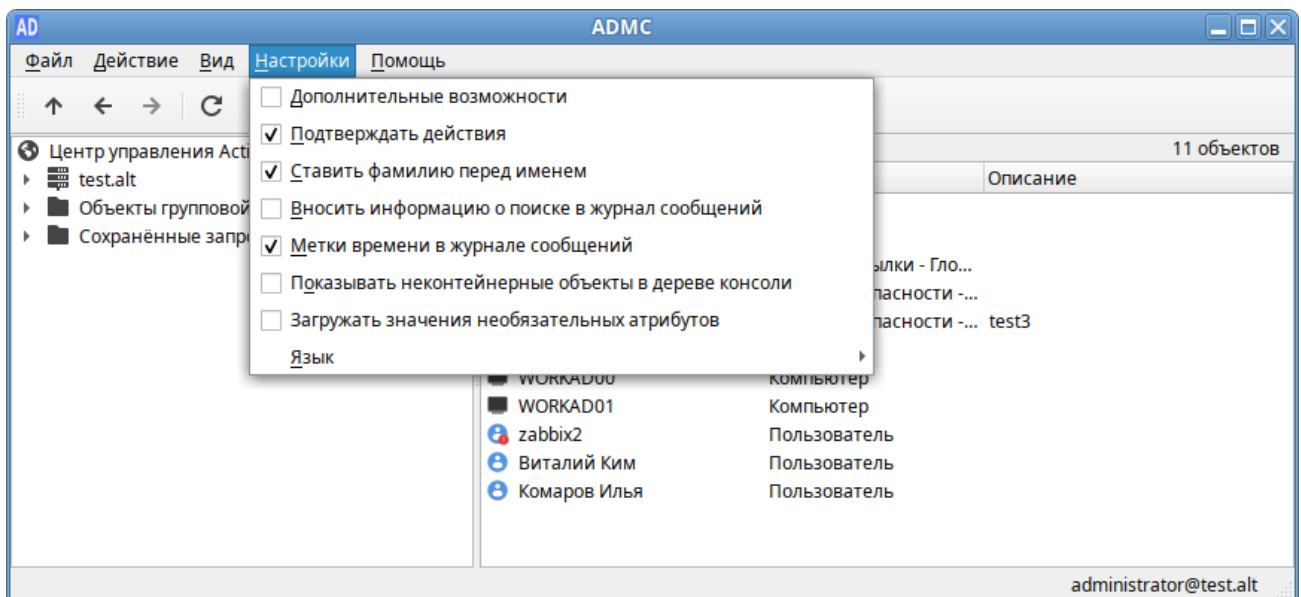


Рис. 258 – Меню «Настройки»

Если отмечен пункт «Дополнительные возможности», будут показаны расширенные объекты и элементы приложения.

Если отмечен пункт «Подтверждать действия», при выполнении потенциально опасных действий будет выводиться окно «Подтвердить действие», например, при удалении объекта (рис. 259).

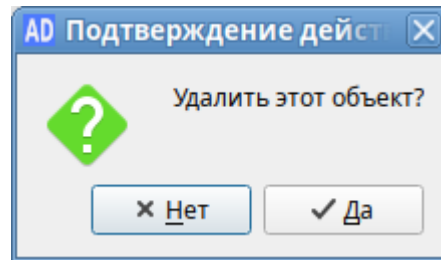


Рис. 259 – Окно «Подтвердить действие»

Другие параметры программы:

- «Ставить фамилию перед именем» – изменить формат полного имени (поле «сн») по умолчанию на «Фамилия Имя»;
- «Вносить информацию о поиске в журнал сообщений» – вносить в журнал поисковые запросы;
- «Метки времени в журнале сообщений» – показывать в журнале время события;
- «Показывать неконтэйнерные объекты в дереве консоли» – показывать неконтэйнерные объекты (например, учетные записи пользователей и компьютерные учетные записи) в панели дерева объектов домена;
- «Язык» – выбрать язык интерфейса (русский или английский).

Выбранные параметры сохраняются и восстанавливаются при каждом запуске программы.

При выборе корневого элемента в дереве консоли будет отображена информация о домене (рис. 260): дерево с сайтами, контроллерами домена и ролями FSMO (рис. 261). Данный виджет также содержит версию контроллера домена, количество сайтов и контроллеров домена, режимы работы домена и леса, версию схемы домена.

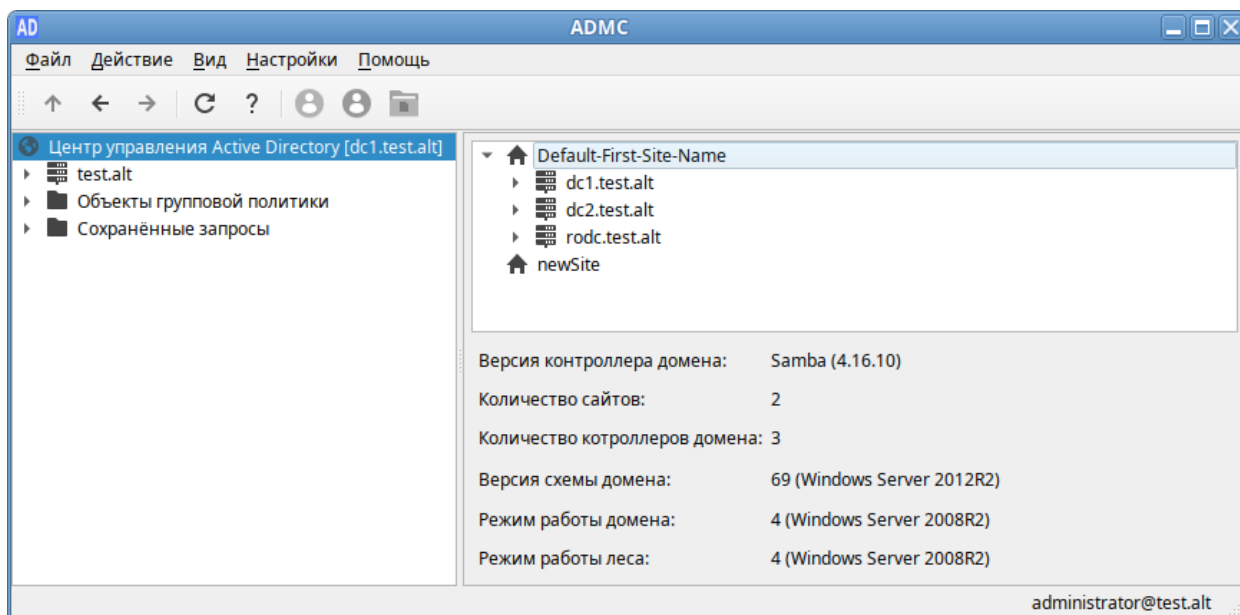


Рис. 260 – Информация о домене

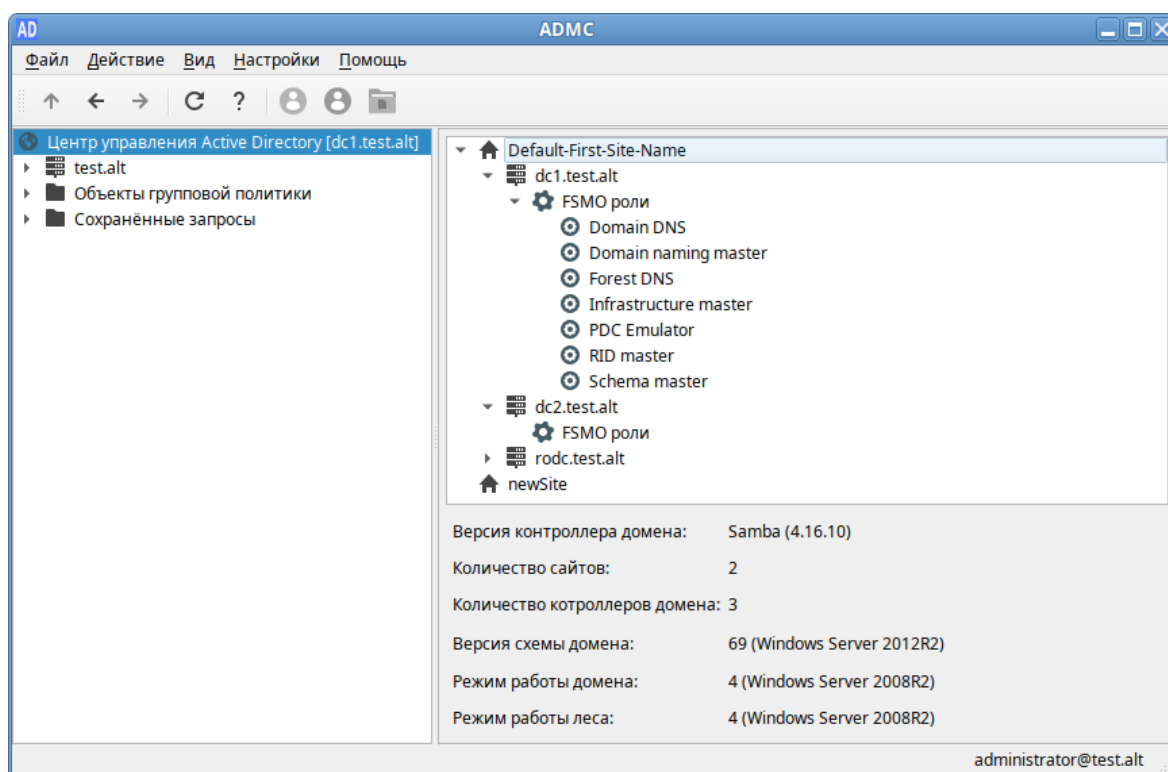


Рис. 261 – Роли FSMO

Меню операций с объектом открывается из строки меню (пункт «Действие») после выбора объекта (рис. 262) или в контекстном меню объекта (рис. 263).

Меню операций содержит действия применимые к выделенному объекту.

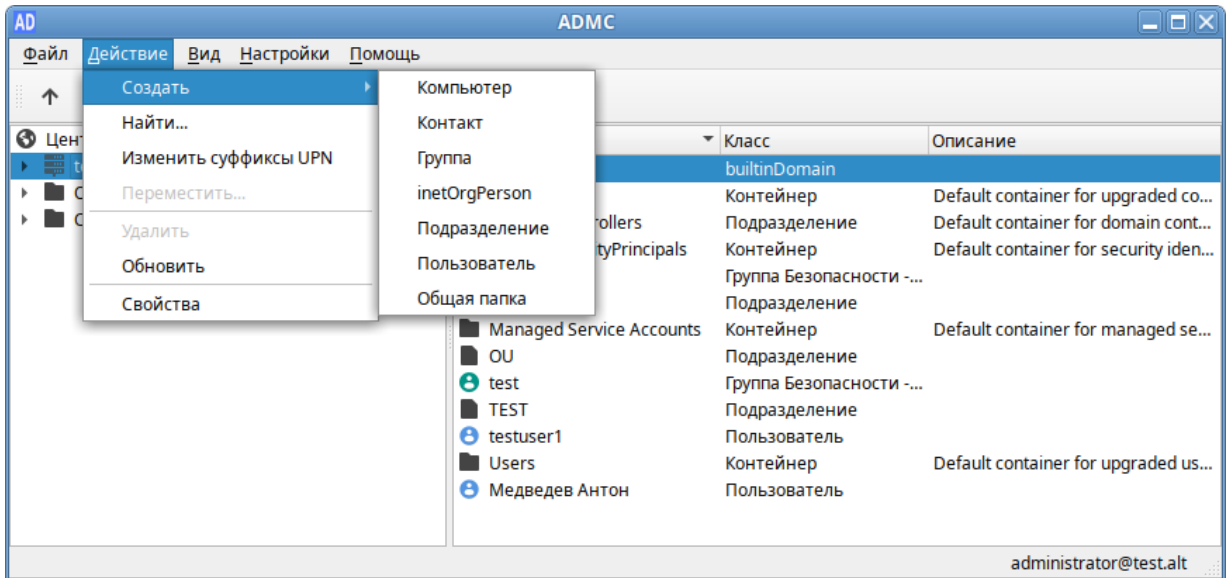


Рис. 262 – Пункт «Действие»

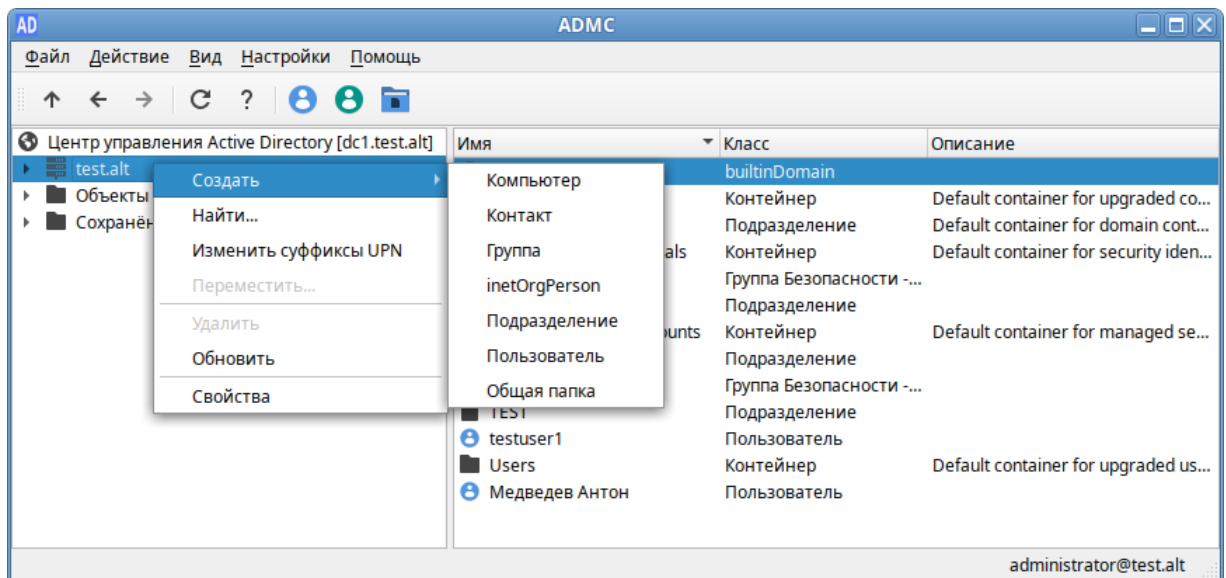


Рис. 263 – Контекстное меню объекта

10.4.5.3. Свойства объектов

Существует два режима работы ADMC: обычный и расширенный режим.

При включении расширенного режима («Настройки» → «Дополнительные возможности») в свойствах всех объектов появляются дополнительно две вкладки: «Атрибуты» и «Объект». Для объекта пользователь также появляется вкладка «Безопасность».

Окно «Учетная запись пользователя – Свойства» в расширенном режиме (рис. 264).

По умолчанию отображается вкладка «Общее». Назначение каждой группы параметров приведено в таблице 26.

Во вкладке «Общее» задаются личные данные сотрудника и его контактная информация: телефоны, размещение, адрес электронной почты и др. Вкладка «Общее» отображается по умолчанию при вызове свойств учетной записи любого объекта домена. В качестве значений параметров указаны названия соответствующих им полей в домене (таблица 27).

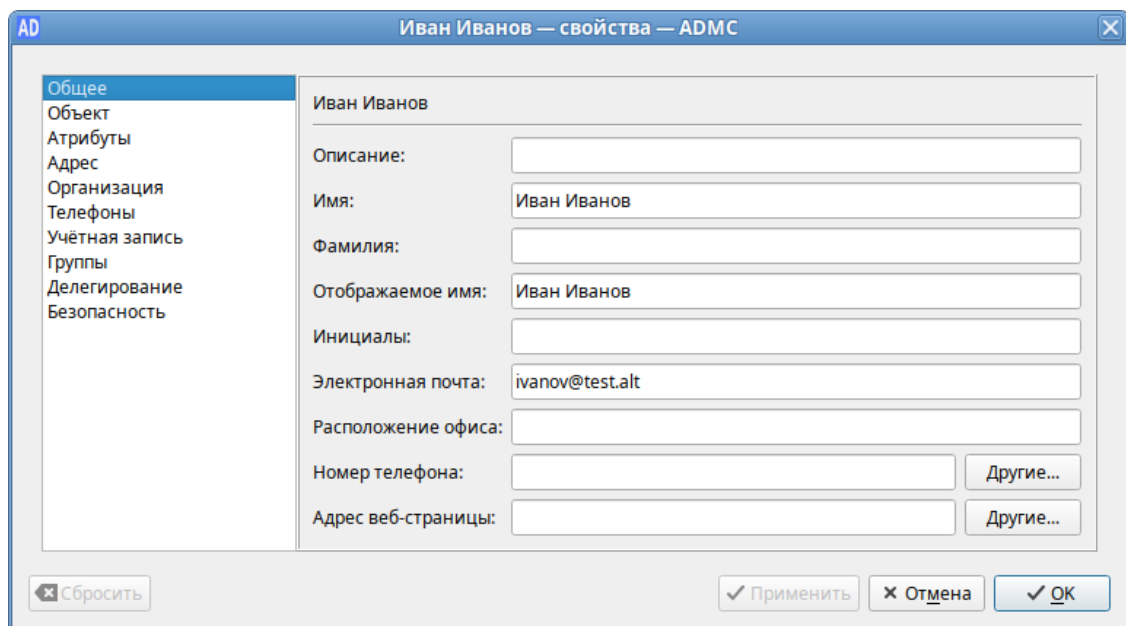


Рис. 264 – Окно «Учетная запись пользователя – Свойства»

Т а б л и ц а 26 – Назначение вкладок окна «Свойства учетной записи пользователя»

Вкладка	Описание	Расширенный режим
Общее	Основная вкладка, содержащая информацию, идентифицирующую личность пользователя, которой соответствует данная учетная запись	-
Учетная запись	Характеристики учетной записи пользователя, настройка правил регистрации в сети	-
Адрес	Почтовый адрес пользователя	-
Организация	Данные о сотруднике согласно штатному расписанию	-
Телефоны	Настройка телефонии	-
Группы	Управление членством в группах безопасности	-
Атрибуты	Список атрибутов объекта	+
Объект	Информация об объекте	+
Делегирование		-
Безопасность	Права доступа к объекту	+

Т а б л и ц а 27 – Соответствие параметров на вкладке «Общее» полям в AD

Поле на вкладке «Общее»	Примечание	Поле в Active Directory	Тип
Полное имя	Во вкладке «Общее» значение этого поля изменить нельзя	cn, name	Юникод
Описание		description	Юникод
Имя		givenName	Юникод
Фамилия		sn	Юникод
Отображаемое имя	Значение этого параметра складывается из суммы значений трех параметров: First Name, Initials и Last Name	diplayName	Юникод
Инициалы	Длина не более 6 символов	initials	Юникод
Электронная почта	Автоматически заполняемое поле в соответствии с форматом UPN (RFC 822) при создании почтового ящика для учетной записи пользователя. По умолчанию поле пустое	mail	Юникод
Расположение офиса	Указывается физическое месторасположение пользователя: комната, офис и т. д.	physicalDeliveryOfficeName	Юникод
Номер телефона		telephoneNumber	Юникод
Другие телефоны	Можно задать, нажав кнопку «Другие...»	otherTelephone	Юникод
Адрес веб-страницы		wwwHomePage	Юникод
Другие адреса веб-страниц	Можно задать, нажав кнопку «Другие...»	url	Юникод

Во вкладке «Учетная запись» сосредоточены настройки, характеризующие правила доступа пользователя к сети, включая имя входа в сеть (рис. 265).

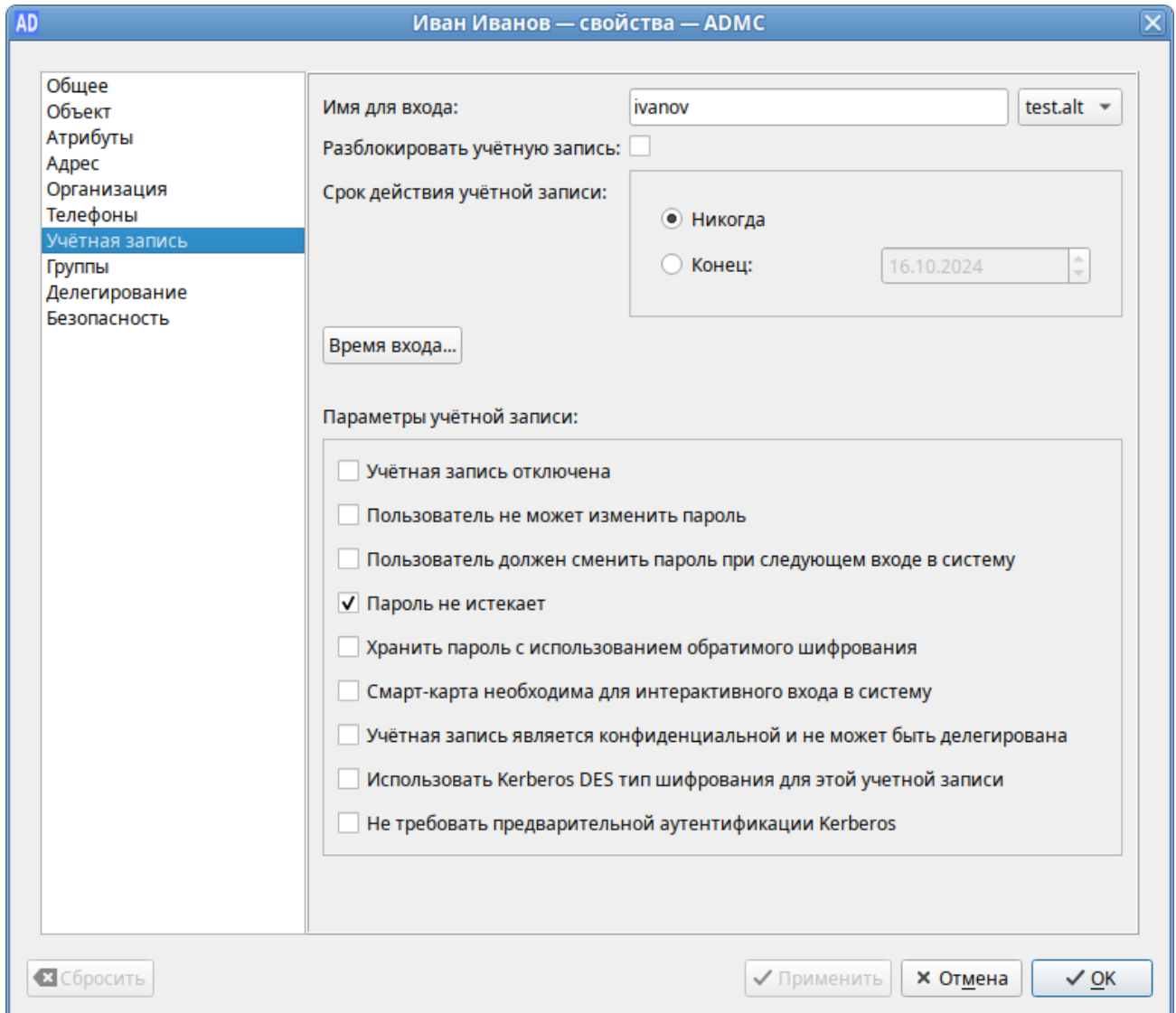


Рис. 265 – Вкладка «Учетная запись»

Соответствие параметров на вкладке «Учетная запись» полям в AD приведено в таблице 28.

Т а б л и ц а 28 – Соответствие параметров на вкладке «Учетная запись» полям в AD

Поле на вкладке «Учетная запись»	Примечание	Поле в Active Directory	Тип
Имя для входа	Имя пользователя для входа (логин пользователя)	userPrincipalName	Юникод
Разблокировать учетную запись	Позволяет разблокировать учетную запись пользователя, если она была заблокирована, например, из-за слишком большого количества неудачных попыток входа	userAccountControl = 16	Целое число
Срок действия учетной записи	Дата отключения учетной записи (по умолчанию «Никогда» – неограниченный срок действия). Если нужно задать дату окончания срока действия учетной записи пользователя, следует выбрать «Конец» и затем выбрать дату	accountExpires	Большое целое число
Время входа...	Часы, в которые пользователю разрешено выполнять вход в домен	logonHours	Октет
Учетная запись отключена (ACCOUNTDISABLE)	Если эта опция включена, пользователь не сможет войти в систему	userAccountControl = 0x0002 (2)	Целое число
Пользователь не может изменить пароль (PASSWORD_CANT_CHANGE)		userAccountControl = 0x0040 (64)	Целое число
Пользователь должен сменить пароль при следующем входе в систему		pwdLastSet	Большое целое число
Пароль не истекает (DONT_EXPIRE_PASSWORD)	Срок действия пароля для этой учетной записи никогда не истечет	userAccountControl = 0x10000 (65536)	Целое число
Хранить пароль с использованием обратимого шифрования (ENCRYPTED_TEXT_PWD_ALLOWED)	Для шифрования ключей использовать DES-шифрование. Эта политика обеспечивает поддержку приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности	userAccountControl = 0x0080 (128)	Целое число

Окончание таблицы 28

Поле на вкладке «Учетная запись»	Примечание	Поле в Active Directory	Тип
Смарт-карта нужна для интерактивного входа в систему (SMARTCARD_REQUIRED)	Пользователь должен войти в систему с помощью смарт-карты	userAccountControl = 0x40000 (262144)	Целое число
Учетная запись является конфиденциальной и не может быть делегирована (NOT_DELEGATED)	Пользователю нельзя доверять делегирование полномочий	userAccountControl = 0x100000 (1048576)	Целое число
Использовать Kerberos DES тип шифрования для этой учетной записи (USE_DES_KEY_ONLY)	Ограничить этот субъект использованием только типов шифрования DES (стандарт шифрования данных) для ключей	userAccountControl = 0x200000 (2097152)	Целое число
Не требовать предварительной аутентификации Kerberos (DONT_REQ_PREAUTH)	Для доступа к ресурсам сети не нужно предварительно проверять подлинность с помощью протокола Kerberos	userAccountControl = 0x400000 (4194304)	Целое число

Примечание. userAccountControl – атрибут управления учетной записью пользователя. Значение атрибута userAccountControl, образуется путем суммирования всех установленных значений. В таблице приведены только те значения, которые можно изменить явным образом на вкладках «Учетная запись» и «Делегирование».

Значения UserAccountControl по умолчанию для определенных объектов:

- обычный пользователь (NORMAL_ACCOUNT): 0x200 (512);
- контроллер домена (SERVER_TRUST_ACCOUNT): 0x2000 (8192);
- рабочая станция или сервер (WORKSTATION_TRUST_ACCOUNT): 0x1000 (4096).

На вкладке «Группы» формируется список групп, членом которых является текущий пользователь. Здесь также можно назначить основную группу (Primary Group). Для управления членством пользователя в группах безопасности AD используются две кнопки, находящиеся под списком групп, членами которой является пользователь: «Добавить» и «Удалить». По умолчанию пользователь входит в группу Domain Users (рис. 266).

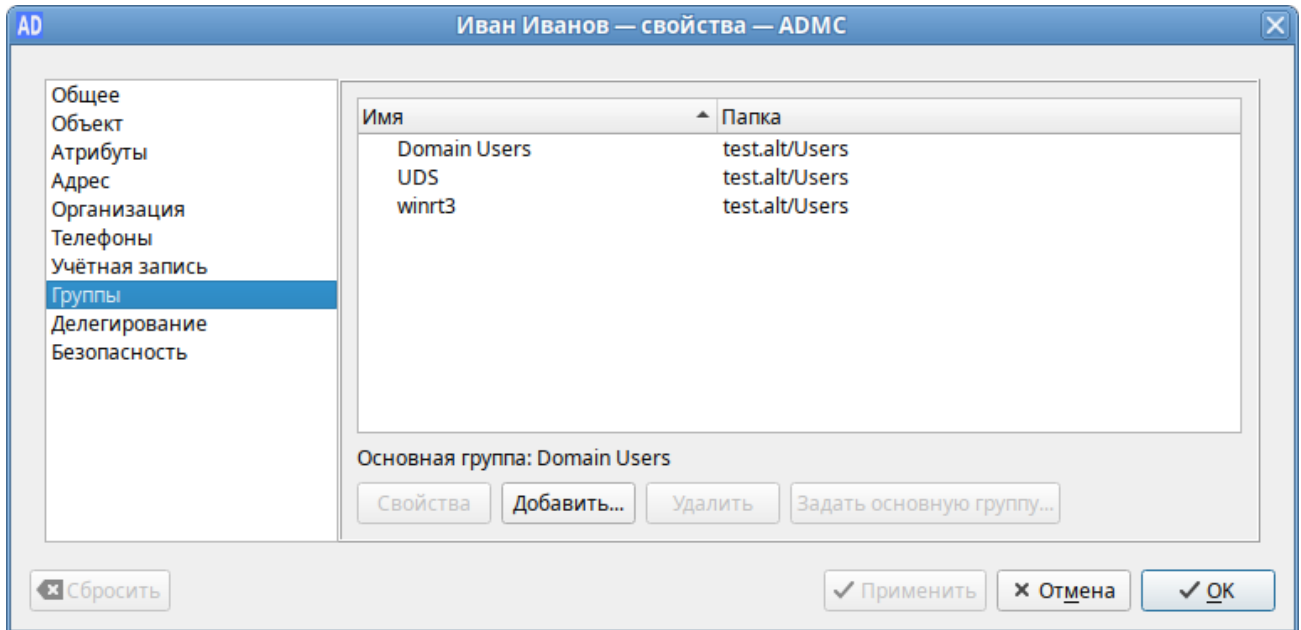


Рис. 266 – Вкладка «Группы»

На вкладке «Делегирование» доступно два параметра (рис. 267):

- «Не доверять делегирование» – запрещение делегирования услуг;
- «Доверять делегирование любых служб с использованием Kerberos» – задает возможность делегирования услуг только с помощью протокола Kerberos.

Примечание. Протокол проверки подлинности Kerberos – это основной протокол безопасности для проверки подлинности в домене. Он проверяет подлинность пользователя и системы.

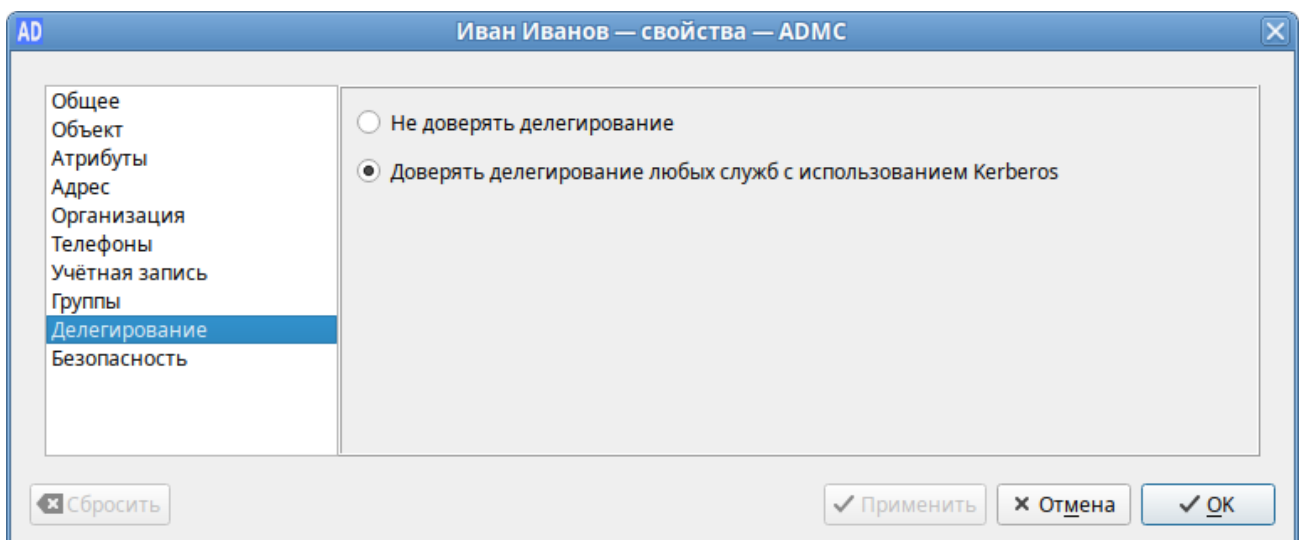


Рис. 267 – Вкладка «Делегирование»

Каждому объекту в сети назначается набор данных об управлении доступом. Этот набор данных определяет, какой тип доступа разрешается пользователям и группам. Управление разрешениями для выбранного объекта доступно на вкладке «Безопасность» (рис. 268).

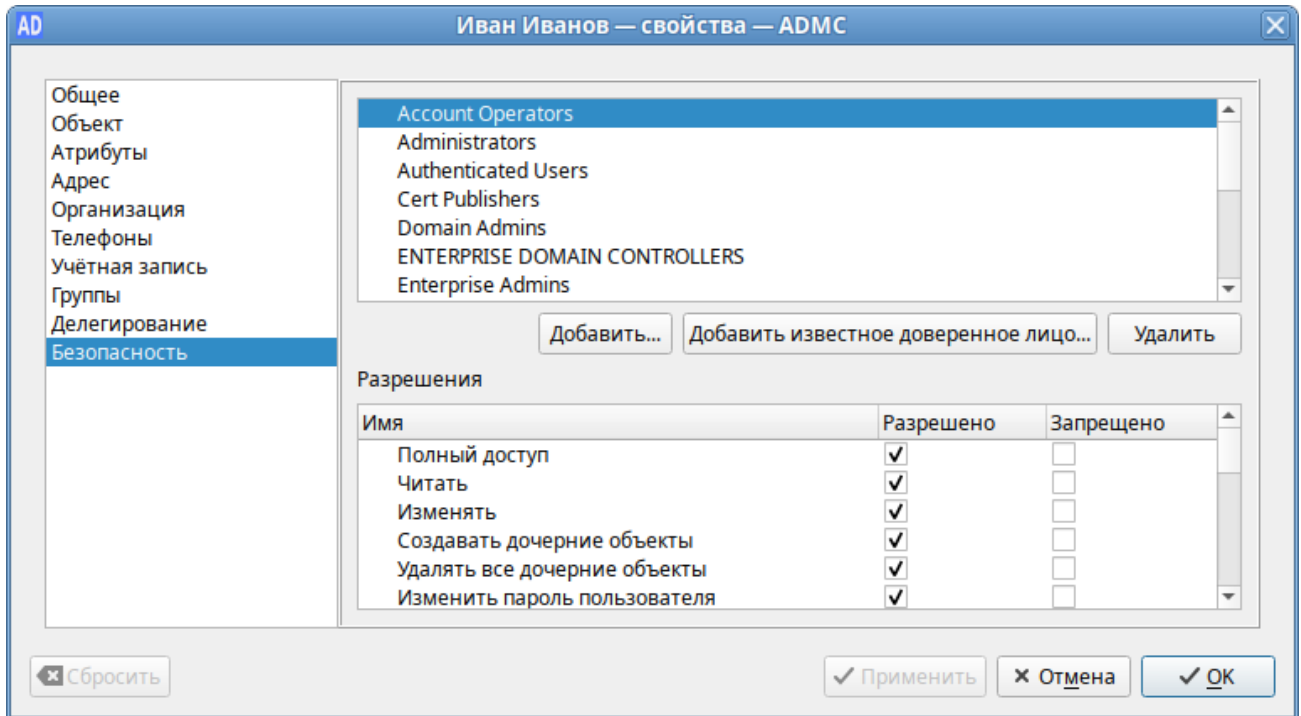


Рис. 268 – Вкладка «Безопасность»

В поле «Разрешения» отображается список действующих разрешений и запретов для каждой выбранной группы. Чтобы установить разрешения для группы, которая отсутствует в списке, можно воспользоваться кнопкой «Добавить...» или «Добавить известное доверенное лицо...».

Для тонкого редактирования свойств объектов домена (пользователей, компьютеров, групп) можно воспользоваться вкладкой «Атрибуты» (рис. 269).

Эту вкладку можно использовать для просмотра и редактирования атрибутов, недоступных через другие вкладки окна «Свойства объекта» (например, для просмотра значений неизменяемых атрибутов).

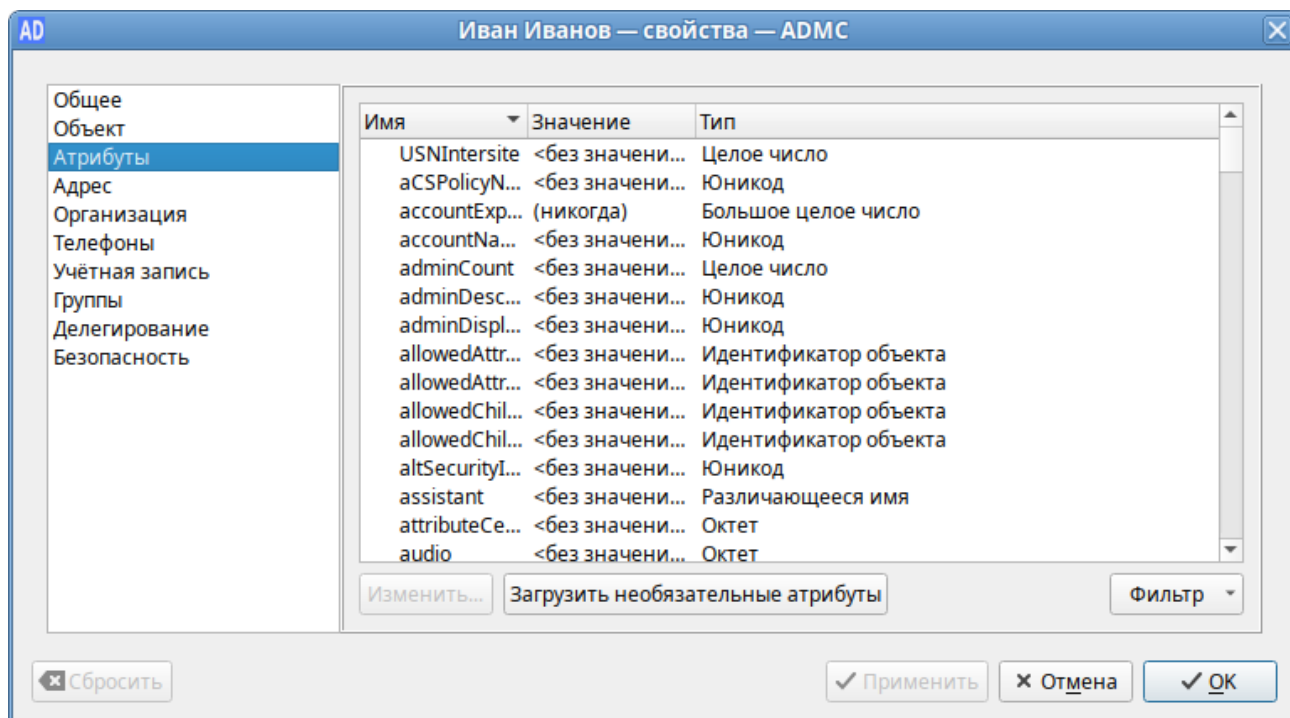


Рис. 269 – Вкладка «Атрибуты»

Содержимое окна редактирования атрибута зависит от типа атрибута (рис. 270, рис. 271).

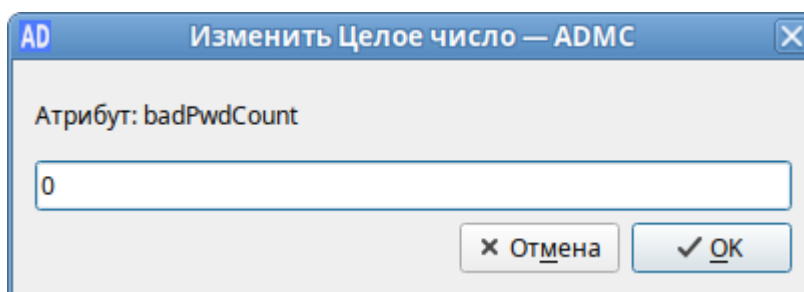


Рис. 270 – Окно редактирования атрибута целого типа

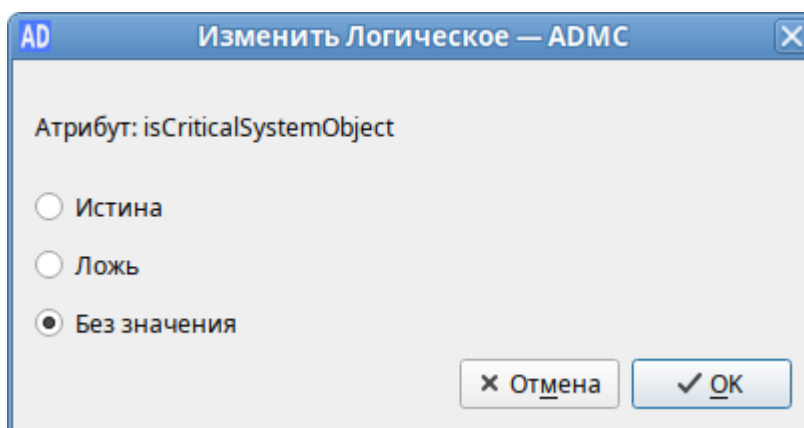


Рис. 271 – Окно редактирования атрибута логического типа

Для большинства атрибутов домена имеется встроенная функция декодирования значений. Например, значение атрибута `lastLogon` или `lastLogonTimestamp` (информация о времени последнего входа пользователя в домен) во вкладке «Атрибуты» и в окне редактирования атрибута отображается в формате «Дата Время», хотя время хранится в виде большого целого числа, представляющего число 100-наносекундных интервалов с 1 января 1601 (UTC) (рис. 272).

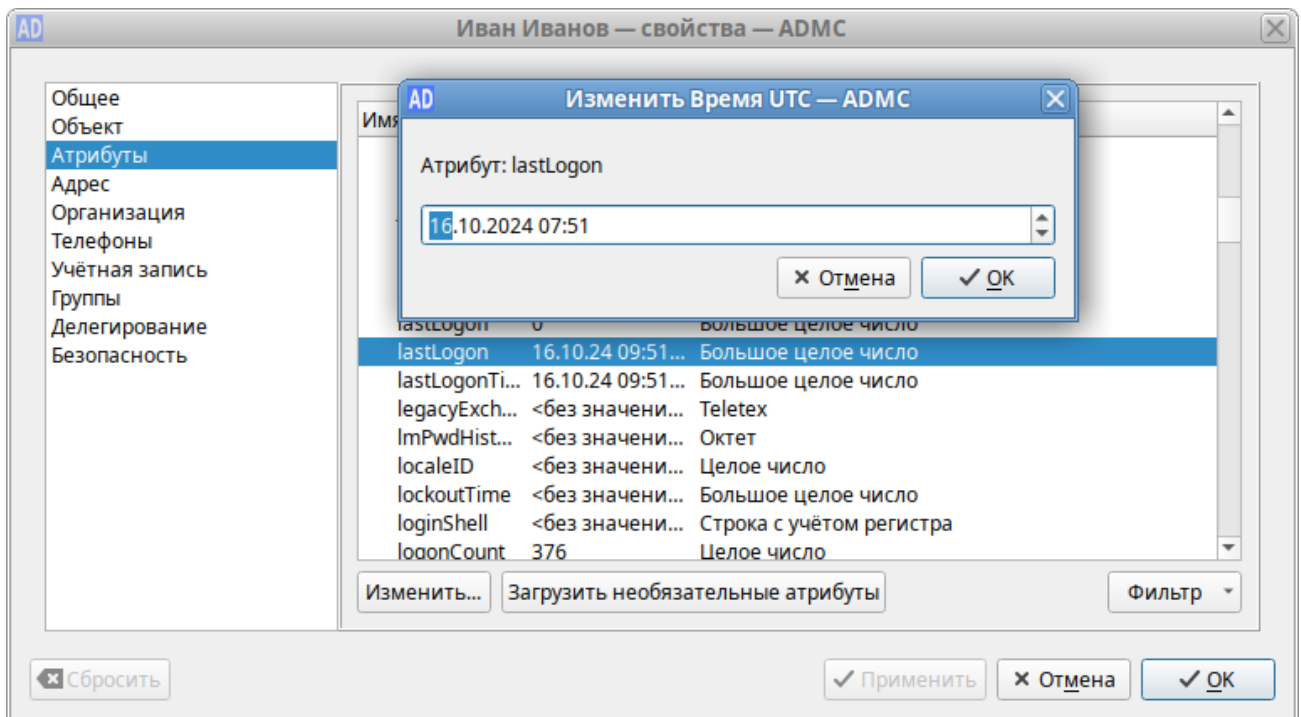


Рис. 272 – Атрибут `lastLogon`

Кнопка «Загрузить необязательные атрибуты» позволяет загрузить значения необязательных атрибутов.

Кнопка «Фильтр» позволяет управлять отображением списка атрибутов (рис. 273):

- «Без значения» – показывать пустые атрибуты;
- «Только для чтения» – показывать все атрибуты, в том числе на правку которых нет полномочий. Если снять отметку с этого пункта, будут показаны только те атрибуты, на правку которых делегированы полномочия

(например, если у пользователя нет полномочий на изменение атрибутов данного объекта, список атрибутов будет пуст);

- «Обязательные» – показывать обязательные атрибуты;
- «Необязательные» – показывать необязательные (дополнительные) атрибуты;
- «Системные» – показывать системные атрибуты, которые может изменять только сервер AD (например, `objectClass`);
- «Сконструированные» – показывать атрибуты, которые не хранятся в каталоге, но вычисляются контроллером домена (например, `canonicalName`);
- «Обратные ссылки» – показывать связанные атрибуты (например, `memberOf`).

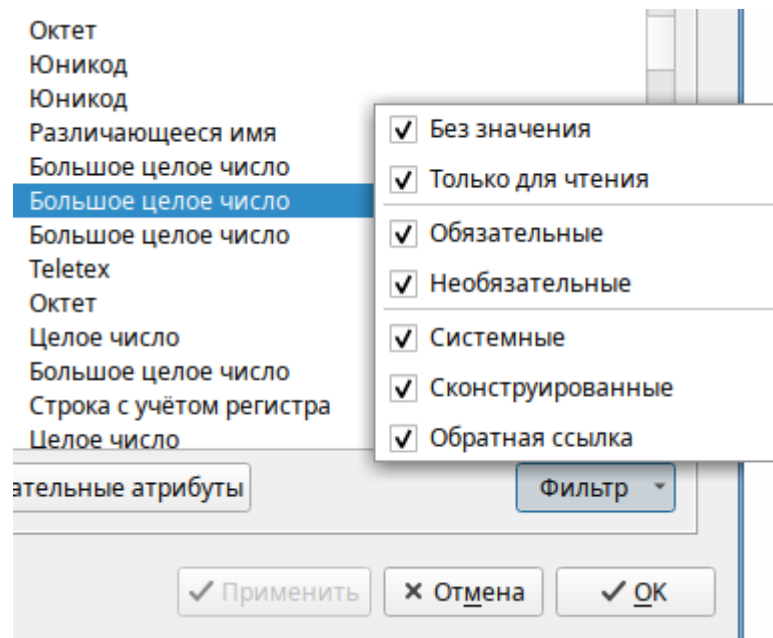


Рис. 273 – Кнопка «Фильтр»

10.4.5.4. Выбор контейнера

При перемещении объекта в новый контейнер (пункт «Переместить...» в контекстном меню объекта) открывается окно, в котором можно выбрать контейнер, в который следует переместить объект (рис. 274).

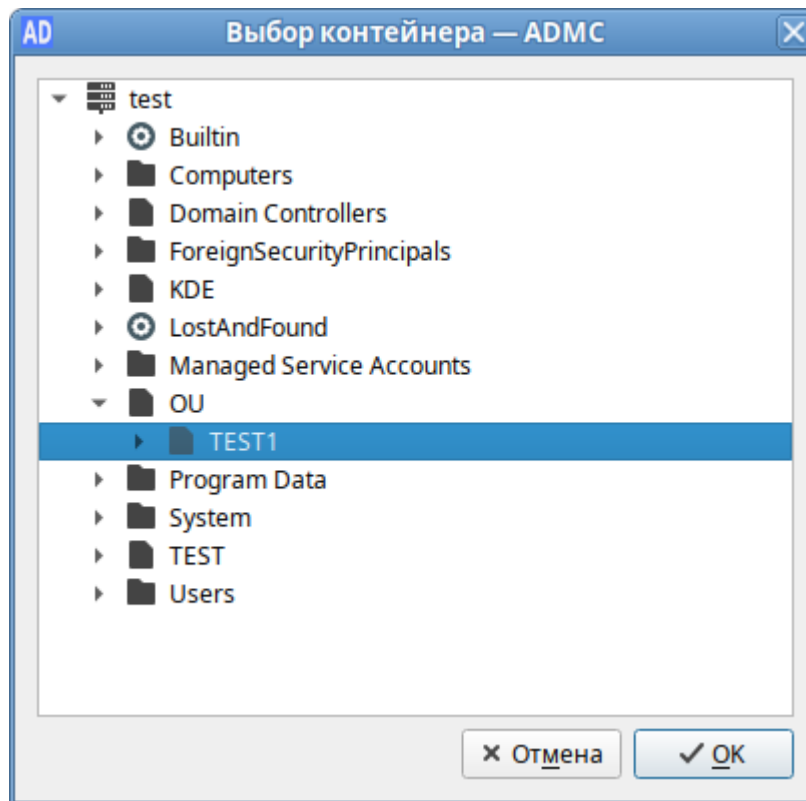


Рис. 274 – Выбор контейнера, в который следует переместить объект

10.4.5.5. Управление пользователями

Учетная запись пользователя «Альт Домен»:

- удостоверяет личность пользователя;
- разрешает или запрещает доступ к ресурсам домена.

В ADMS предусмотрена возможность создания новых учетных записей пользователей в доменных службах «Альт Домен» и управления существующими учетными записями пользователей.

Примечание. Для доступа к некоторым операциям нужно быть членом одной из этих групп: Account Operators, Domain Admins, Enterprise Admins.

Примечание. Объект InetOrgPerson является производным от класса пользователь (user). Он может работать в качестве субъекта безопасности так же, как и объект класса пользователь. Для создания учетной записи InetOrgPerson в контекстном меню контейнера следует выбрать пункт «Создать» → «inetOrgPerson».

10.4.5.5.1. Создание учетной записи пользователя

Для создания учетной записи пользователя в контекстном меню контейнера следует выбрать пункт «Создать» → «Пользователь». Окно мастера создания учетной записи пользователя (рис. 275).

AD Создать пользователя — ADMS

Имя: Михаил

Фамилия: Орлов

Полное имя: Орлов Михаил

Инициалы:

Имя для входа: orlov test.alt

Имя для входа (до Windows 2000): TEST\orlov

Пароль:

Подтвердите пароль:

Показывать пароль

Параметры учётной записи:

Пользователь должен сменить пароль при следующем входе в систему

Пользователь не может изменить пароль

Пароль не истекает

Учётная запись отключена

Отмена OK

Рис. 275 – Окно мастера создания учетной записи пользователя

При создании учетной записи пользователя можно указать следующие параметры (атрибуты):

- «Имя» – имя пользователя;
- «Фамилия» – фамилия пользователя;
- «Полное имя» – полное имя пользователя (в это поле можно добавить отчество или поменять имя и фамилию местами);

- «Инициалы» – инициалы пользователя;
- «Имя для входа» – имя пользователя для входа (логин пользователя). В раскрывающемся списке перечисляются доступные суффиксы основного имени пользователя (UPN), которые можно использовать для создания имени пользователя для входа (рис. 276). Список содержит полное имя системы доменных имен (DNS) текущего домена и все альтернативные суффиксы UPN;

The image shows a Windows login dialog box. The 'Имя для входа:' field contains the text 'orlov'. A dropdown menu is open to the right, showing a list of domain suffixes: 'test.new' (highlighted in blue), 'orlov', and 'test.alt'. Below this, the 'Имя для входа (до Windows 2000):' field contains 'TEST\'. The dialog box has a light gray background and rounded corners.

Рис. 276 – Ввод имени для входа

- «Имя для входа (до Windows 2000)» – имя пользователя для входа в старые системы (пред-Windows 2000);
- «Пароль/Подтвердите пароль» – пароль пользователя;
- «Пользователь должен сменить пароль при следующем входе в систему» – пользователь должен изменить пароль при следующем входе в систему. Если эта опция включена, только пользователь будет знать свой пароль;
- «Пользователь не может изменить пароль» – предотвращает изменение пароля пользователем;
- «Пароль не истекает» – установить бессрочный пароль. Если эта опция включена, срок действия учетной записи пользователя не ограничен (по умолчанию срок действия пароля задан атрибутом minPwdAge);
- «Учетная запись отключена» – отключить учетную запись пользователя. Если эта опция включена, пользователь не сможет войти в систему.

Примечание. Для совместимости с доменами пред-Windows 2000 (Windows NT) в AD задается два имени пользователя, значения которых имеют разный формат. Первое имя, используемое в доменах Window 2k, – UPN-имя, которому в AD соответствует поле userPrincipalName, имеющее формат user@domain, где:

- domain – DNS-имя домена, например, TEST.ALT;
- user – имя пользователя в сети.

Для удобства назначения имен UPN-имя разделено на две части (префикс UPN и суффикс UPN). Второе задаваемое имя пользователя – SAM-имя, которое используется для совместимости в доменах Windows NT. Структура SAM-имени следующая: domain\user, где:

- domain – сокращенное имя домена, например, TEST;
- user – имя пользователя.

В AD хранится только имя пользователя в поле samAccountName. Первая часть SAM-имени однозначно вычисляется из DNS-имени домена.

По умолчанию суффиксом основного имени (UPN) для учетной записи пользователя является DNS имя домена, которое содержит учетную запись пользователя. Для упрощения процессов администрирования и входа пользователя в систему, можно добавить альтернативные суффиксы UPN.

10.4.5.5.2. Изменение учетной записи пользователя

Для изменения учетной записи пользователя следует в контекстном меню пользователя выбрать соответствующее действие (рис. 277).

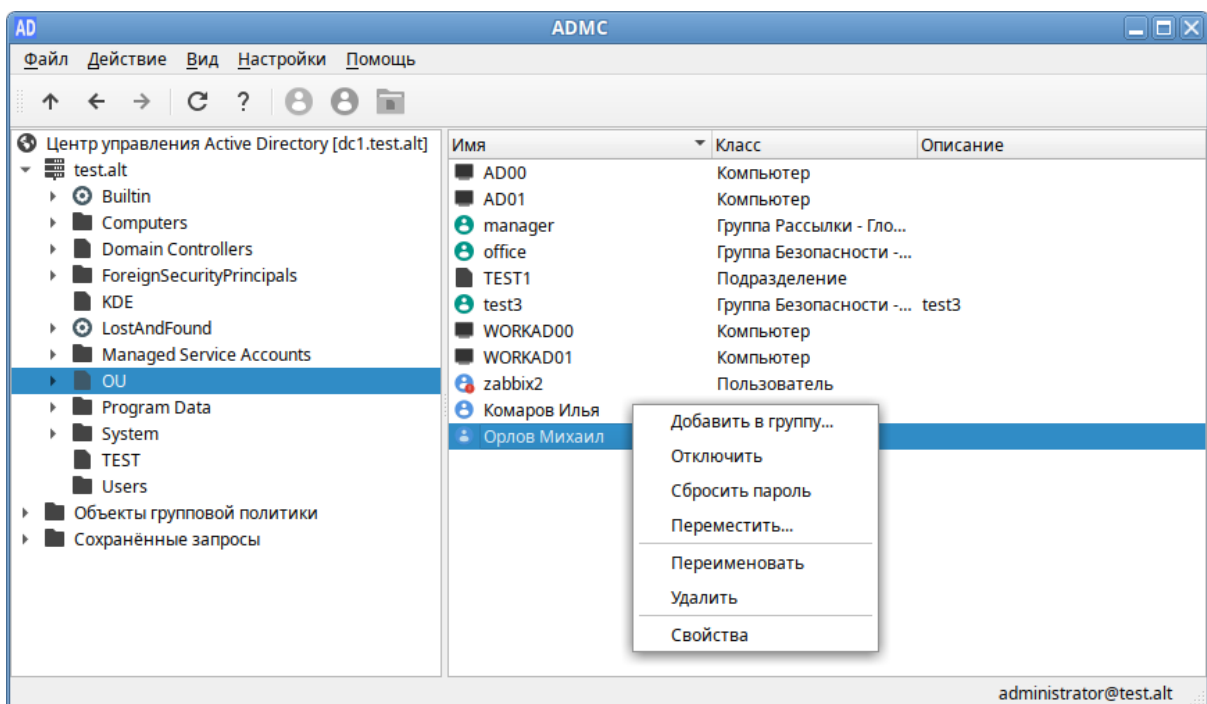


Рис. 277 – Контекстное меню учетной записи пользователя

Для добавления пользователя в группу:

- 1) в контекстном меню пользователя выбрать пункт «Добавить в группу...»;
- 2) в открывшемся окне выбрать группы, в которые следует добавить учетную запись пользователя в качестве участника (рис. 278);

3) нажать кнопку «ОК».

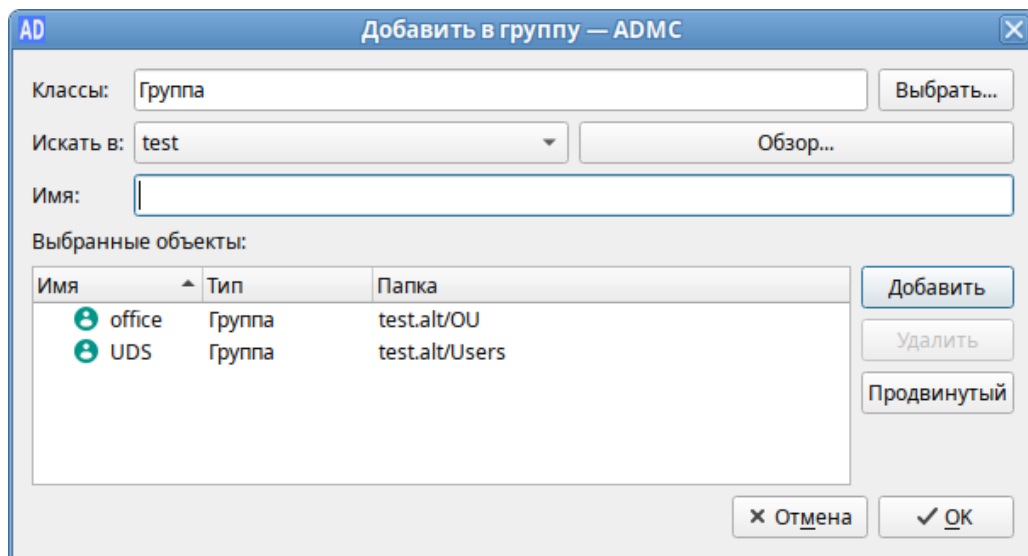


Рис. 278 – Добавление учетной записи пользователя

Для переименования пользователя:

- 1) в контекстном меню пользователя выбрать пункт «Переименовать»;
- 2) в открывшемся окне, если нужно, изменить соответствующие поля (рис. 279);
- 3) нажать кнопку «ОК» для сохранения изменений.

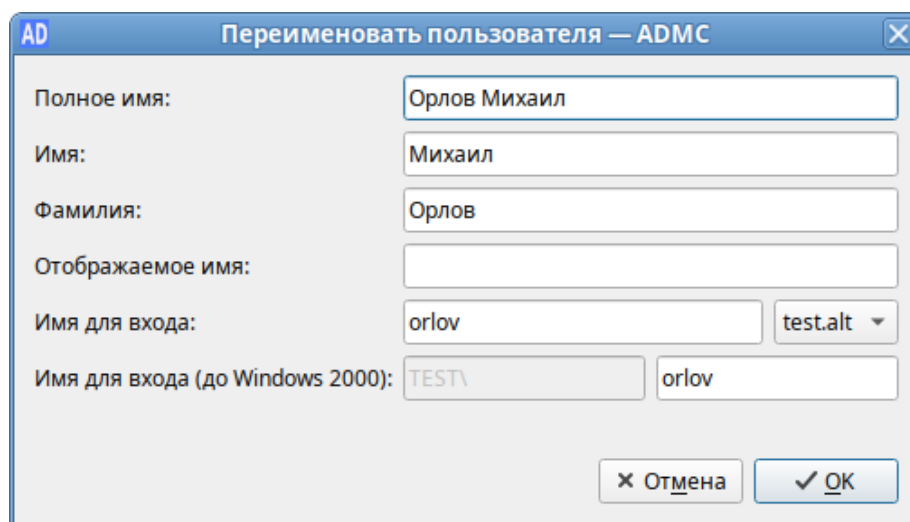


Рис. 279 – Переименование пользователя

Для изменения пароля пользователя:

- 1) в контекстном меню пользователя выбрать пункт «Сбросить пароль»;
- 2) в открывшемся окне ввести новый пароль и подтвердить его (рис. 280);

- 3) если нужно, чтобы пользователь изменил этот пароль при следующем входе в систему, установить отметку «Пользователь должен изменить пароль при следующем входе в систему»;
- 4) установить отметку «Разблокировать учетную запись», если нужно разблокировать учетную запись пользователя;
- 5) нажать кнопку «ОК» для сохранения изменений.

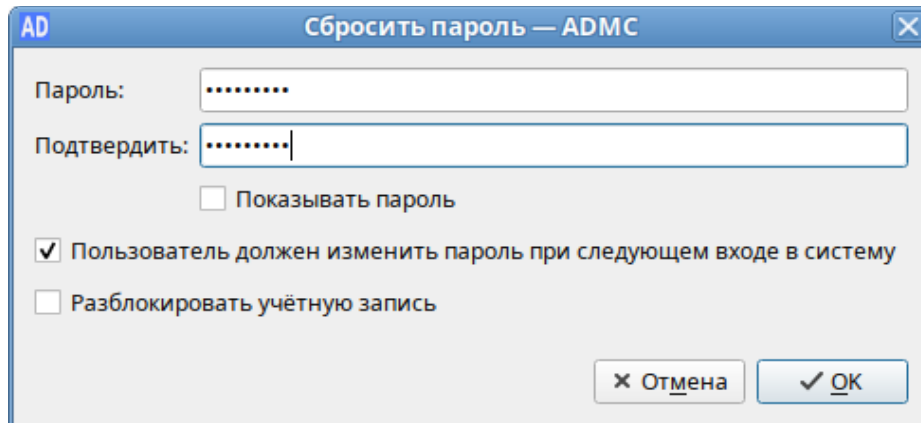


Рис. 280 – Подтверждение пароля

Для перемещения пользователя в другой контейнер:

- 1) в контекстном меню пользователя выбрать пункт «Переместить...»;
- 2) в открывшемся окне выбрать контейнер, в который следует переместить учетную запись пользователя (рис. 274);
- 3) нажать кнопку «ОК».

Для включения/отключения учетной записи пользователя нужно в контекстном меню пользователя выбрать пункт «Отключить» или «Включить» (в зависимости от состояния учетной записи будет доступно одно из этих действий).

Чтобы разблокировать учетную запись пользователя:

- 1) в контекстном меню пользователя выбрать пункт «Свойства»;
- 2) в открывшемся окне на вкладке «Учетная запись» отметить пункт «Разблокировать учетную запись» (рис. 281);
- 3) нажать кнопку «ОК» или «Применить».

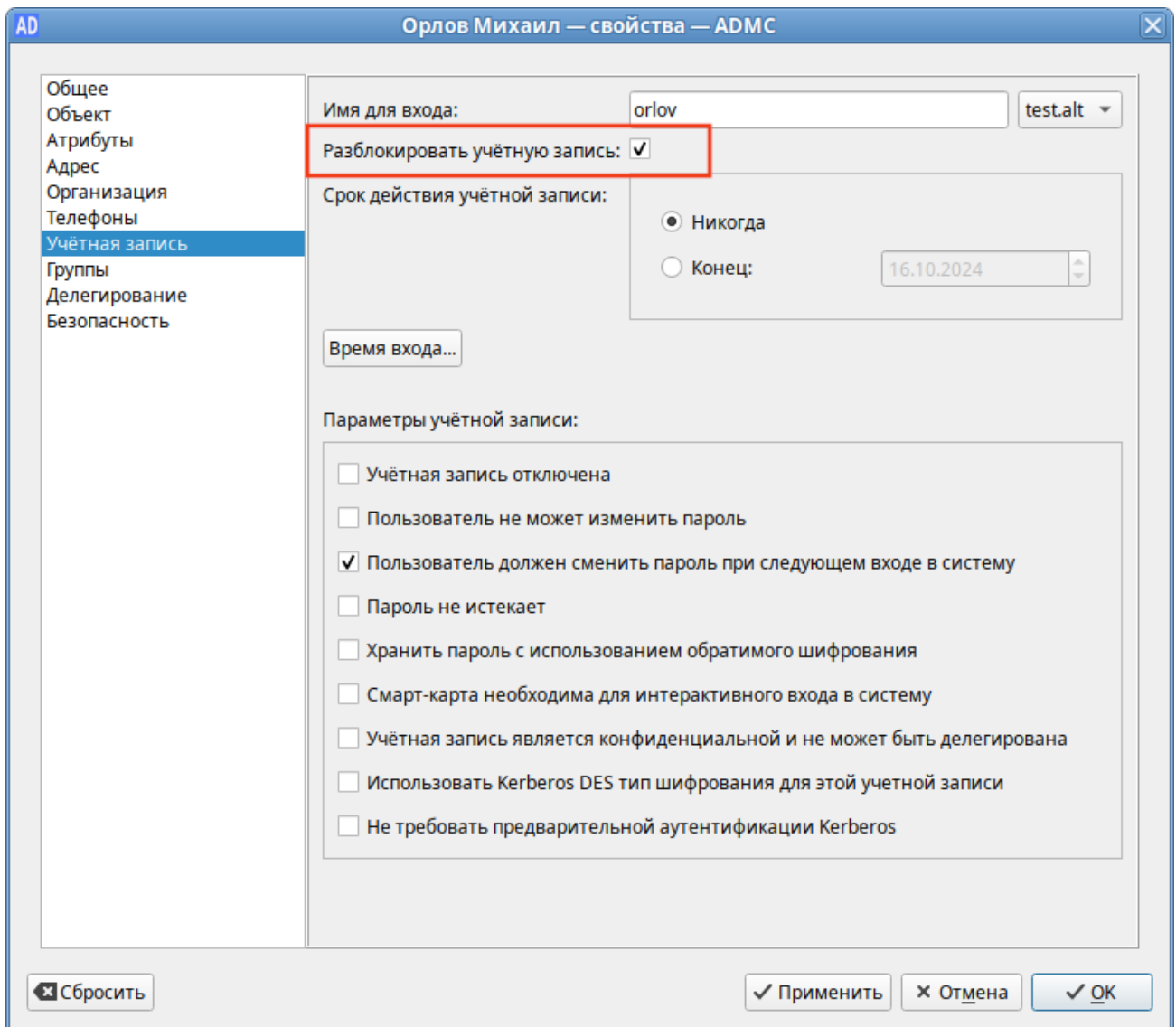


Рис. 281 – Пункт «Разблокировать учетную запись»

Для удаления учетной записи пользователя следует в контекстном меню пользователя выбрать пункт «Удалить».

⚠ Если в настройках ADMS не отмечен пункт «Подтверждать действия», пользователь будет удален сразу после выбора пункта меню «Удалить».

Для того чтобы найти группы, участником которых является пользователь:

- 1) в контекстном меню пользователя выбрать пункт «Свойства» (рис. 282);
- 2) в открывшемся окне на вкладке «Группы» будут отображаться группы, в которые входит данный пользователь.

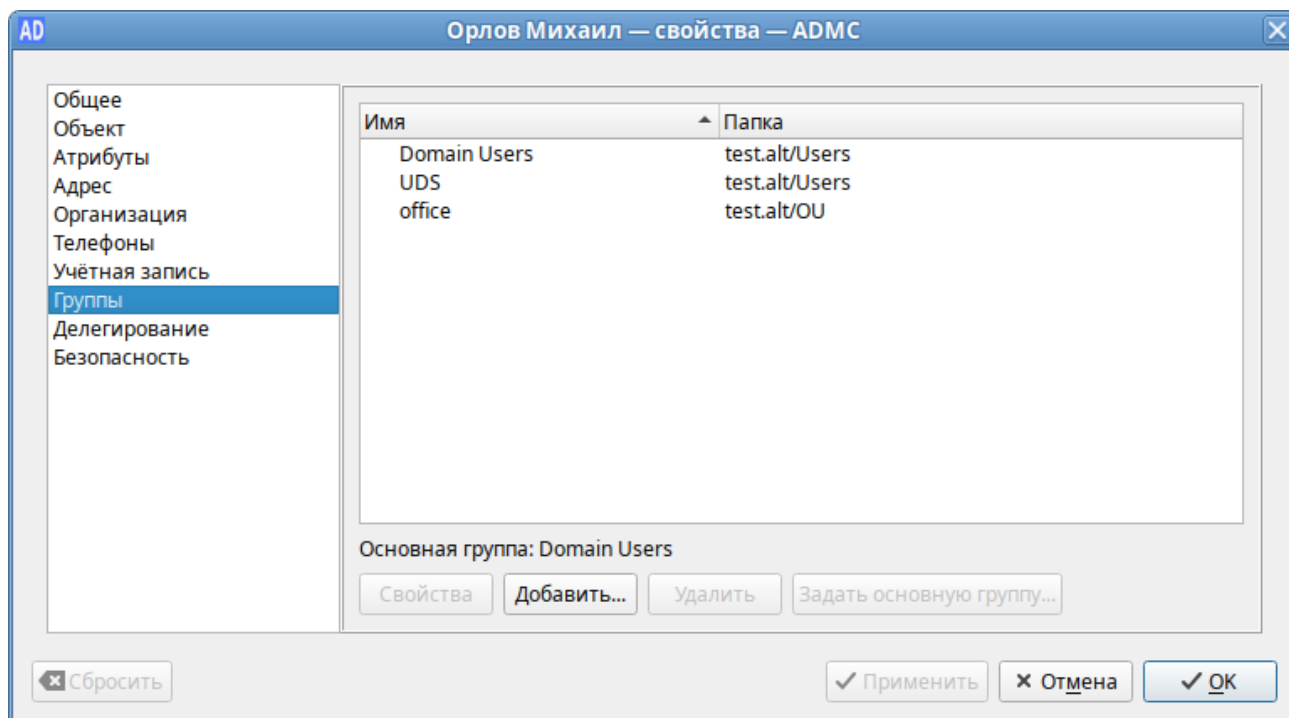


Рис. 282 – Вкладка «Группы»

10.4.5.6. Управление контактами

Контакт предназначен для хранения информации о пользователях, которым не требуется регистрация в домене.

10.4.5.6.1. Создание контакта

Для создания контакта в контекстном меню контейнера следует выбрать пункт «Создать» → «Контакт». Окно мастера создания контакта (рис. 283).

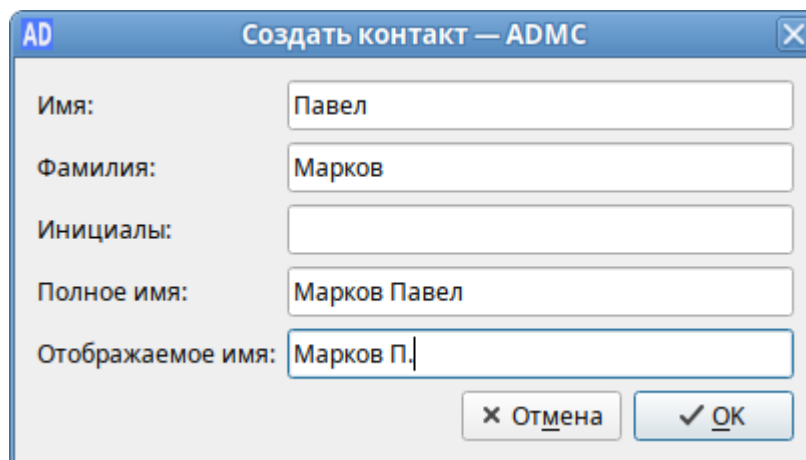


Рис. 283 – Окно мастера создания контакта

При создании контакта можно указать следующие параметры (атрибуты):

- «Имя» – имя пользователя;
- «Фамилия» – фамилия пользователя;
- «Инициалы» – инициалы пользователя;
- «Полное имя» – полное имя пользователя (в это поле можно добавить отчество или поменять имя и фамилию местами);
- «Отображаемое имя» – имя, отображаемое в адресной книге для определенной учетной записи.

10.4.5.6.2. Изменение свойств контакта

Для изменения учетной записи пользователя следует в контекстном меню контакта выбрать соответствующее действие (рис. 284).

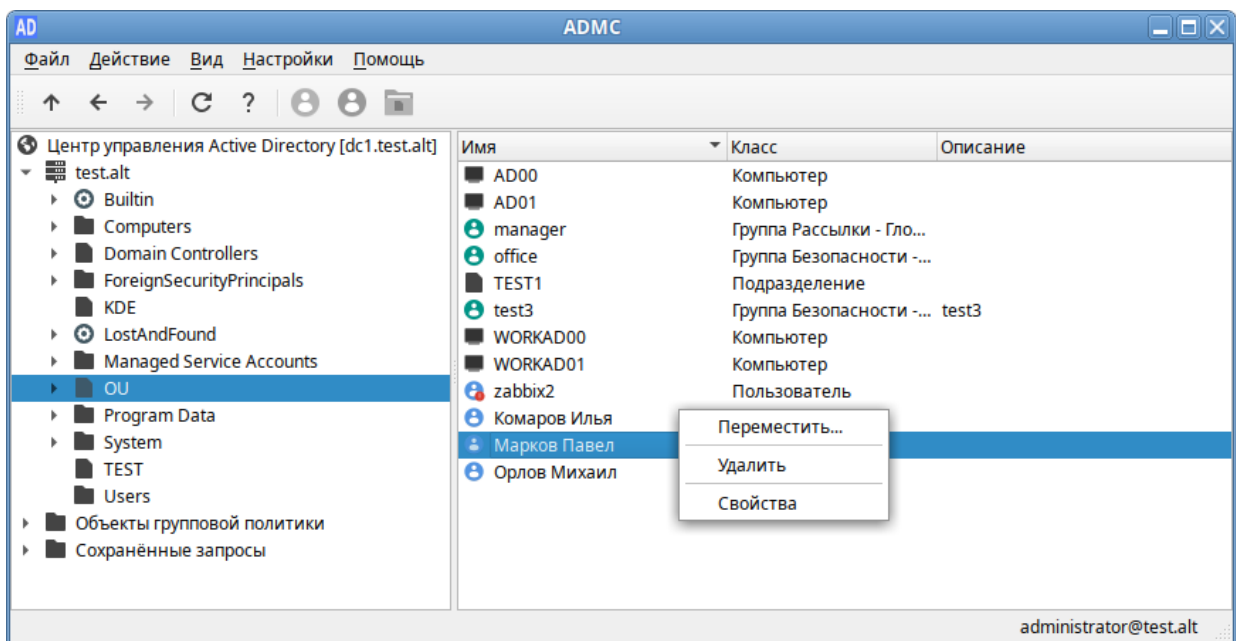


Рис. 284 – Контекстное меню учетной записи контакта

Вкладки «Общие», «Адрес», «Телефоны» и «Организация» в окне «Свойства» контакта идентичны соответствующим вкладкам окна «Свойства» учетной записи пользователя.

На вкладке «Группы» можно, по аналогии с учетными записями пользователей, указать, членом каких групп является контакт. Возможность членства в группах не дает контакту никаких прав в рамках домена и предназначена для организации групп рассылки.

Для контакта нельзя указать основную группу, так как это не требуется для функционирования групп рассылки.

10.4.5.7. Управление группами

Группа состоит из учетных записей пользователей и компьютеров, контактов и других групп и может управляться как единое целое. Пользователи и компьютеры, входящие в определенную группу, являются членами группы.

Группы характеризуются областью действия и типом. Область действия группы определяет пределы применения группы внутри домена или леса. Тип группы определяет возможность использования группы для назначения разрешений с ресурса общего доступа (для групп безопасности) или только для списков рассылки электронной почты (для групп рассылки).

10.4.5.7.1. Создание группы

Для создания группы следует в контекстном меню контейнера выбрать пункт «Создать» → «Группа». Окно мастера создания группы (рис. 285).

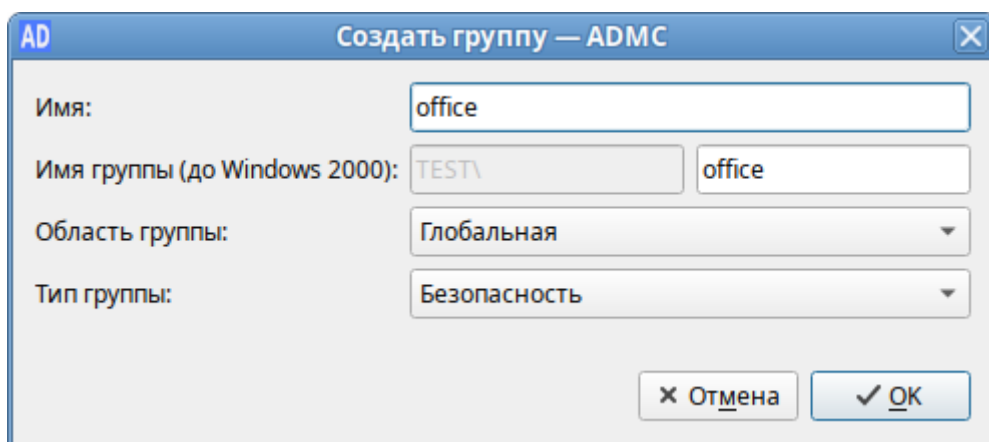


Рис. 285 – Окно мастера создания группы

При создании группы можно указать следующие параметры (атрибуты):

- 1) «Имя» – название группы;
- 2) «Имя группы (до Windows 2000)» – название группы для старых систем (пред-Windows 2000);
- 3) «Область группы» – область действия группы:
 - «Глобальная» – членами глобальной группы могут быть другие группы и учетные записи только из того домена, в котором определена группа.

Членам этой группы разрешения могут назначаться в любом домене леса;

- «Домен локальная» – членам такой группы разрешения могут назначаться только внутри домена (доступ к ресурсам одного домена);
- «Универсальная» – членами универсальных групп могут быть другие группы и учетные записи из любого домена дерева доменов или леса. Членам такой группы разрешения могут назначаться в любом домене дерева доменов или леса;

4) «Тип группы» – тип группы:

- «Безопасность» – используется для назначения разрешений доступа к общим ресурсам;
- «Рассылка» – используется для создания списков рассылки электронной почты.

10.4.5.7.2. Изменение группы

Для изменения группы следует в контекстном меню группы выбрать соответствующее действие (рис. 286).

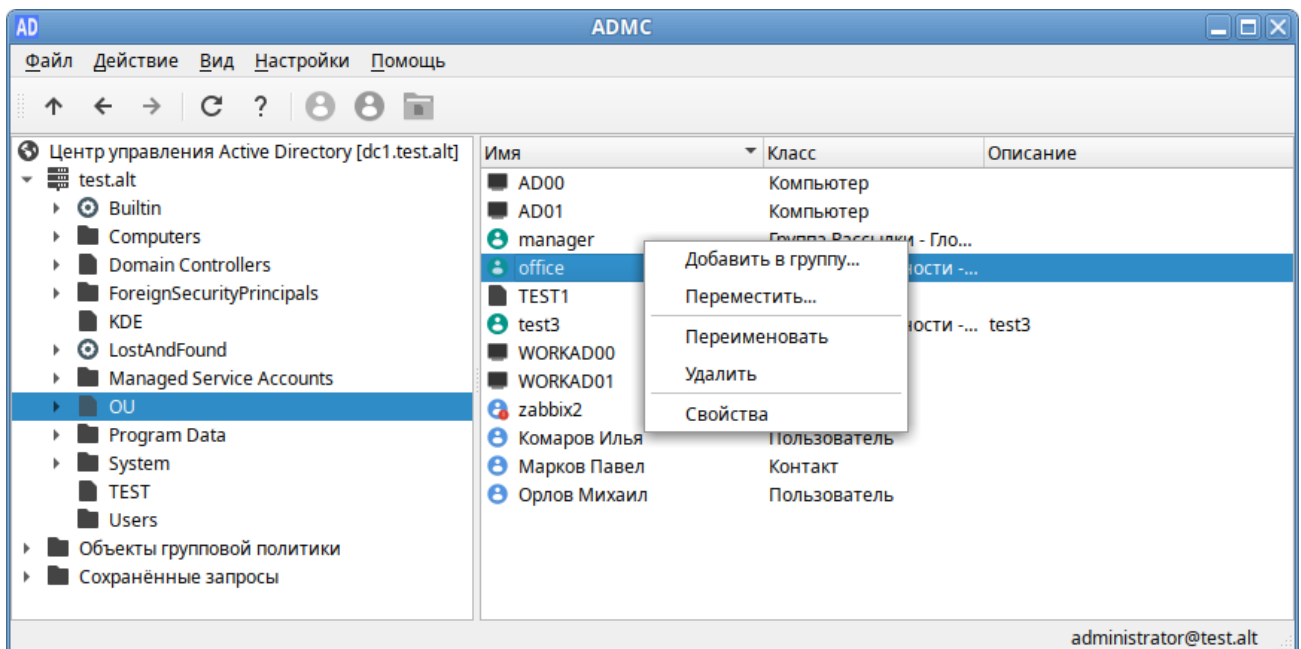


Рис. 286 – Контекстное меню группы

Для добавления группы в другую группу:

- 1) в контекстном меню группы выбрать пункт «Добавить в группу...»;

- 2) в открывшемся окне (рис. 287) выбрать группы, в которые следует добавить данную группу в качестве участника;
- 3) нажать кнопку «ОК».

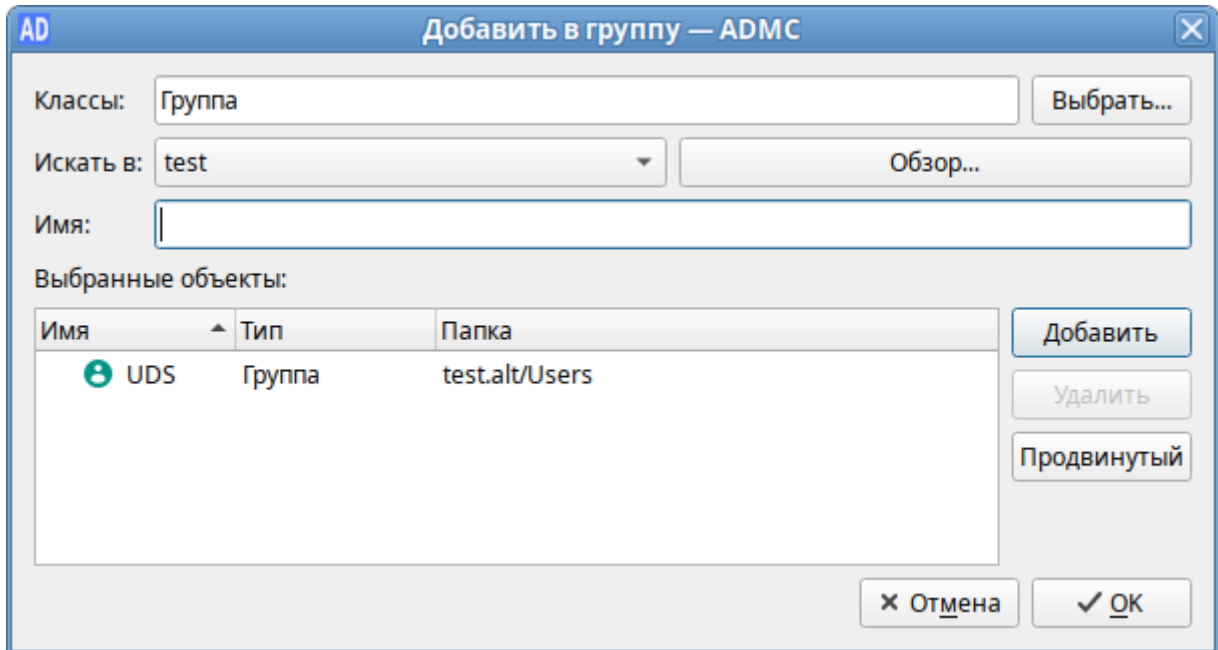


Рис. 287 – Добавление группы в другую группу

Для перемещения группы в другой контейнер:

- 1) в контекстном меню группы выбрать пункт «Переместить...»;
- 2) в открывшемся окне выбрать контейнер (рис. 274), в который следует переместить группу;
- 3) нажать кнопку «ОК».

Для переименования группы:

- 4) в контекстном меню группы выбрать пункт «Переименовать»;
- 5) в открывшемся окне (рис. 288), если нужно, изменить соответствующие поля;
- 6) нажать кнопку «ОК» для сохранения изменений.

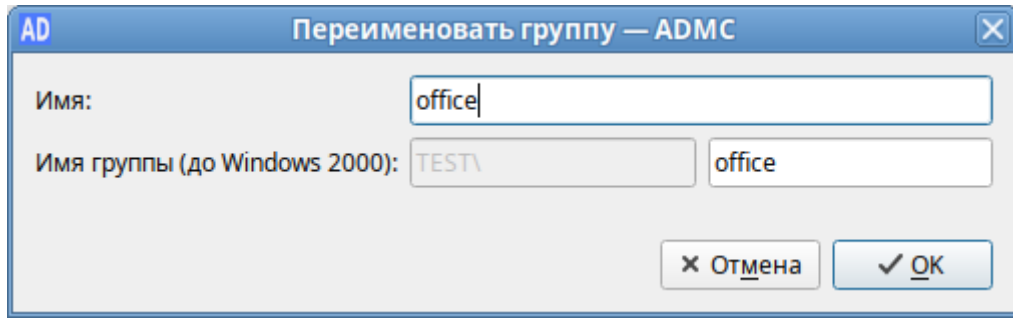


Рис. 288 – Переименование группы

Для удаления группы следует в контекстном меню группы выбрать пункт «Удалить».

⚠ Если в настройках ADMS не отмечен пункт «Подтверждать действия», группа будет удалена сразу после выбора пункта меню «Удалить».

Для того чтобы добавить участников в группу:

- 1) в контекстном меню группы выбрать пункт «Свойства»;
- 2) в открывшемся диалоговом окне на вкладке «Участники» нажать кнопку «Добавить...» (рис. 289);

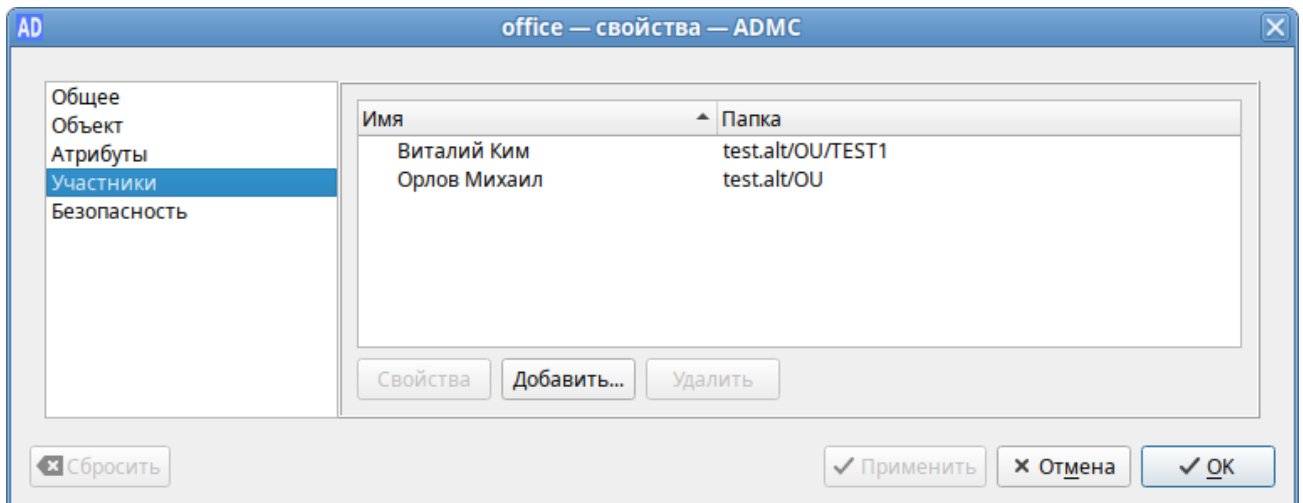


Рис. 289 – Добавление участников в группу

- 3) выбрать объекты, которые нужно добавить в группу (рис. 290);
- 4) нажать кнопку «ОК»;
- 5) нажать кнопку «ОК» или «Применить» для сохранения изменений.

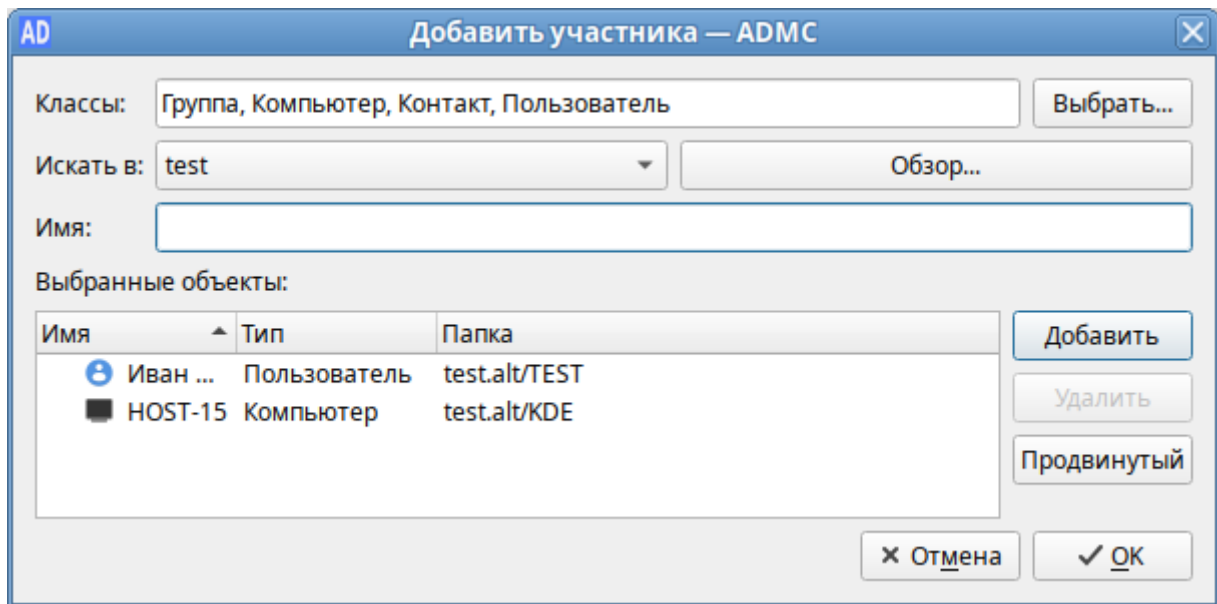


Рис. 290 – Выбор объектов, которые нужно добавить в группу

Для изменения области действия/типа группы:

- 1) в контекстном меню группы выбрать пункт «Свойства»;
- 2) в открывшемся диалоговом окне на вкладке «Общее» в выпадающем списке «Тип группы» выбрать тип группы, в выпадающем списке «Область группы» выбрать область действия группы (рис. 291);
- 3) нажать кнопку «OK» или «Применить» для сохранения изменений.

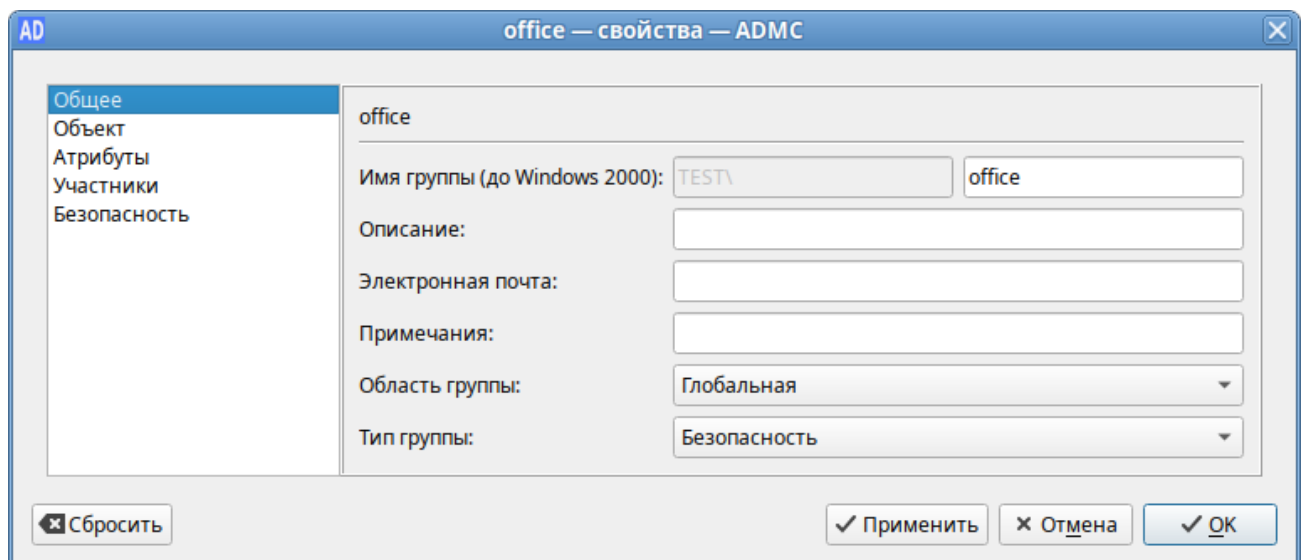


Рис. 291 – Изменение области действия/типа группы

10.4.5.8. Управление компьютерами

Учетные записи компьютеров представляют собой устройства, подключенные к «Альт Домен». Они хранятся в базе данных домена после того, как их подключат к домену.

10.4.5.8.1. Создание учетной записи компьютера

Учетная запись компьютера создается во время стандартной процедуры присоединения к домену.

Для создания вручную учетной записи компьютера следует в контекстном меню контейнера выбрать пункт «Создать» → «Компьютер».

При создании учетной записи компьютера (рис. 292) нужно указать название компьютера (поле «Имя») и название компьютера для старых систем (поле «Имя для входа (до Windows 2000)»).

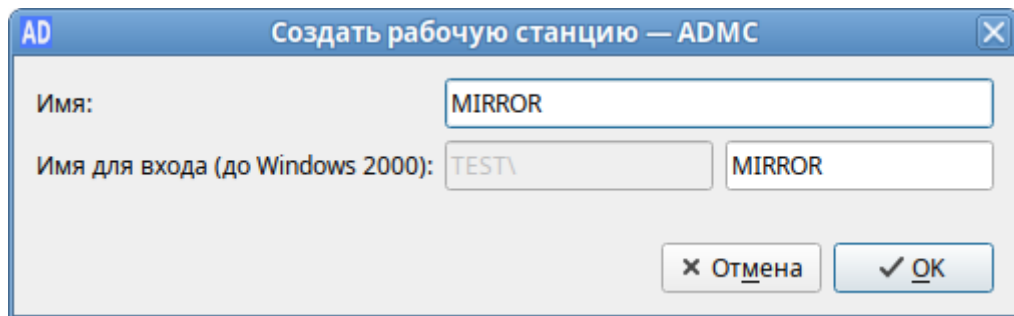


Рис. 292 – Создание учетной записи компьютера

10.4.5.8.2. Изменение учетной записи компьютера

Для изменения учетной записи компьютера следует в контекстном меню компьютера выбрать соответствующее действие (рис. 293).

Для включения/отключения учетной записи компьютера нужно в контекстном меню компьютера выбрать пункт «Отключить» или «Включить» (в зависимости от состояния учетной записи будет доступно одно из этих действий).

Для сброса учетной записи компьютера следует в контекстном меню компьютера выбрать пункт «Сбросить учетную запись». При этом учетная запись выбранного компьютера будет переустановлена. Переустановка учетной записи компьютера прекращает его подключение к домену и требует заново ввести данный компьютер в домен.

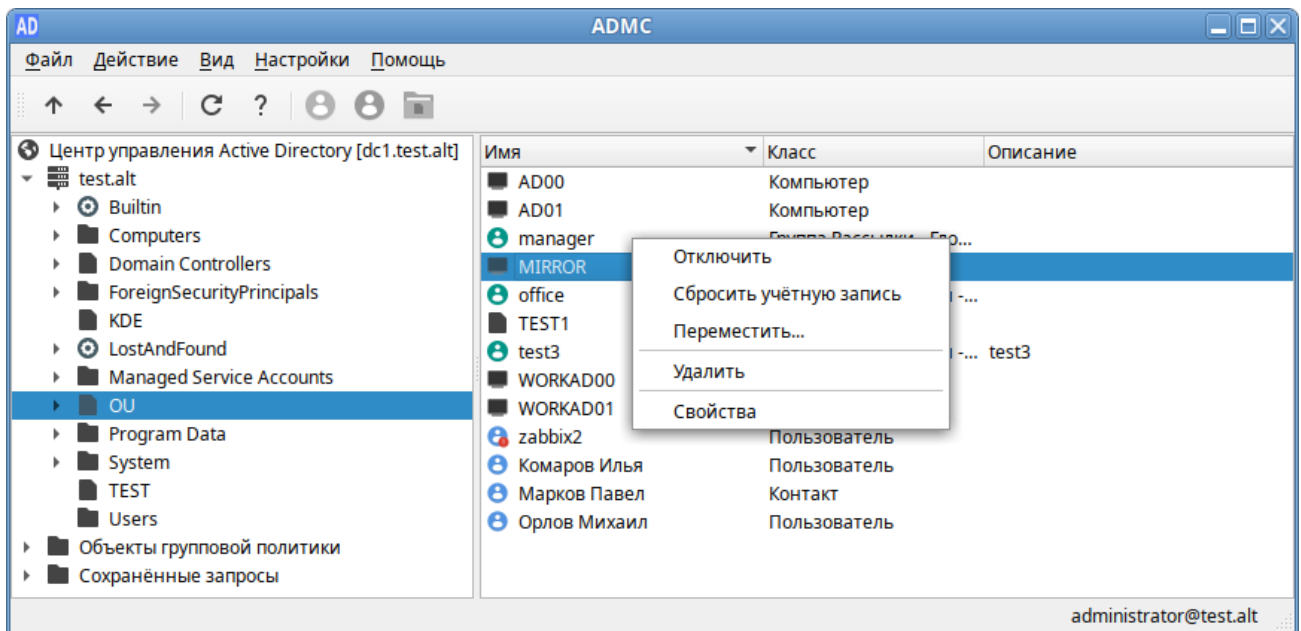


Рис. 293 – Контекстное меню учетной записи компьютера

Для перемещения компьютера в другой контейнер:

- 1) в контекстном меню компьютера выбрать пункт «Переместить...»;
- 2) в открывшемся окне выбрать контейнер (рис. 274), в который следует переместить учетную запись компьютера;
- 3) нажать кнопку «ОК».

Для удаления учетной записи компьютера следует в контекстном меню компьютера выбрать пункт «Удалить».

⚠ Если в настройках ADMC не отмечен пункт «Подтверждать действия», компьютер будет удален сразу после выбора пункта меню «Удалить».

10.4.5.9. Управление подразделениями

Организационная единица или подразделение (Organizational Unit, OU) – это субконтейнер в домене, в который можно помещать пользователей, группы, компьютеры и другие объекты домена. Подразделение – самая маленькая область или единица, для которой можно назначить параметры групповой политики. Подразделения могут быть вложенными.

10.4.5.9.1. Создание подразделения

Для создания подразделения следует в контекстном меню контейнера выбрать пункт «Создать» → «Подразделение».

При создании подразделения (рис. 294) нужно указать название подразделения (поле «Имя»).

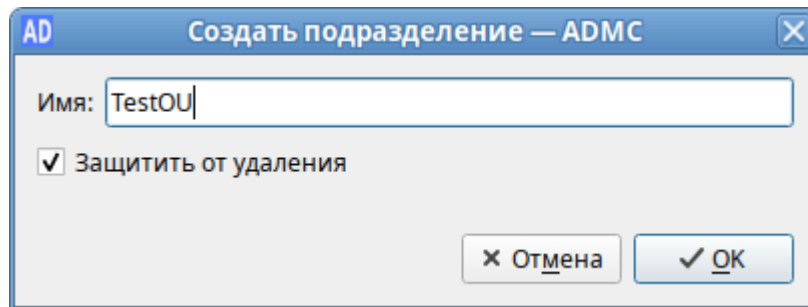


Рис. 294 – Окно мастера создания подразделения

Примечание. Если при создании подразделения отметить пункт «Защитить от удаления», то для удаления данного подразделения, нужно сначала снять данную отметку в окне свойств подразделения.

10.4.5.9.2. Изменение подразделения

Для изменения подразделения следует в контекстном меню подразделения выбрать соответствующее действие (рис. 295).

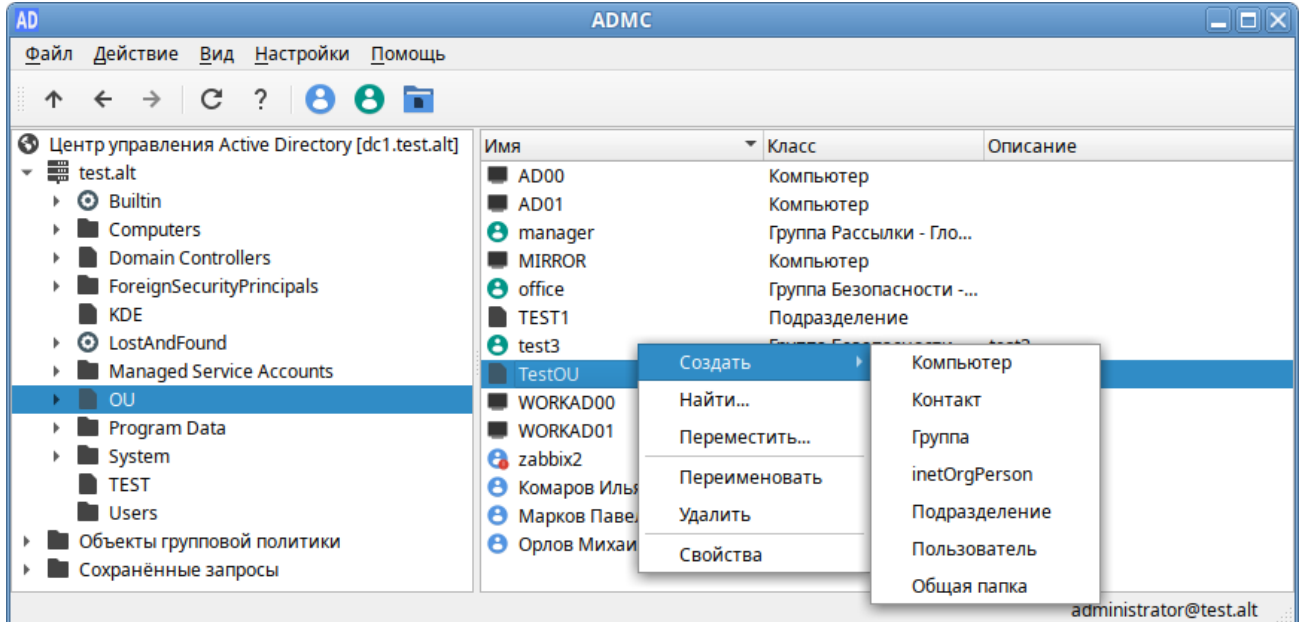


Рис. 295 – Контекстное меню подразделения

Для переименования подразделения:

- 1) в контекстном меню подразделения выбрать пункт «Переименовать»;
- 2) в открывшемся окне изменить имя подразделения (рис. 296);

3) нажать кнопку «ОК» для сохранения изменений.

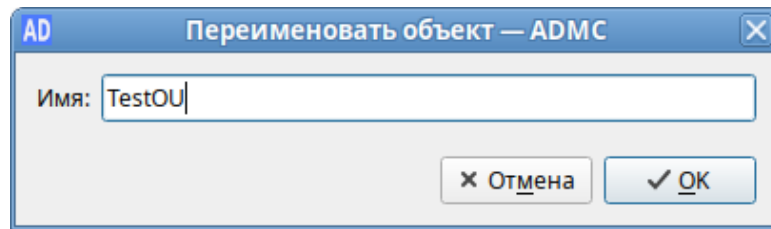


Рис. 296 – Переименование подразделения

Для удаления подразделения следует в контекстном меню подразделения выбрать пункт «Удалить».

⚠ Если при создании подразделения был отмечен пункт «Защитить от удаления», то сразу удалить подразделение не получится, нужно сначала снять данную отметку в окне свойств подразделения (рис. 297).

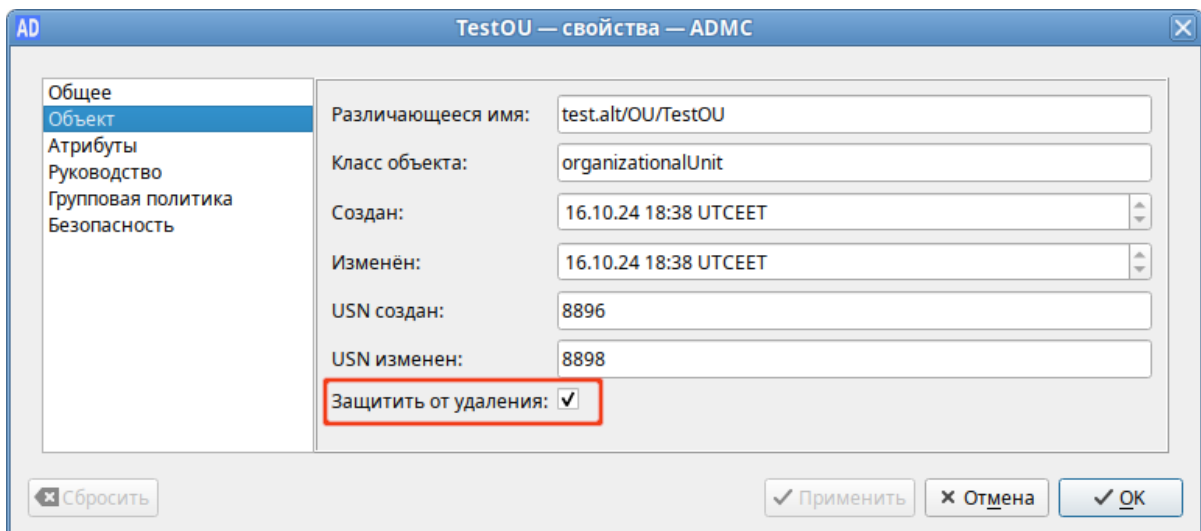


Рис. 297 – Свойства подразделения

Для перемещения подразделения в другой контейнер:

- 1) в контекстном меню подразделения выбрать пункт «Переместить...»;
- 2) в открывшемся окне выбрать контейнер, в который следует переместить подразделение (рис. 274);
- 3) нажать кнопку «ОК».

10.4.5.10. Управление объектами парольных настроек

Примечание. Для возможности работы с объектами парольных настроек необходимо в меню «Настройки» отметить пункт «Дополнительные возможности» (рис. 258).

10.4.5.10.1. Создание объекта парольных настроек

Для создания объекта парольных настроек следует в контекстном меню контейнера «Password Settings Container» (вкладка «System») выбрать пункт «Создать объект парольных настроек» (рис. 298). Откроется окно мастера создания объекта парольных настроек (рис. 299).

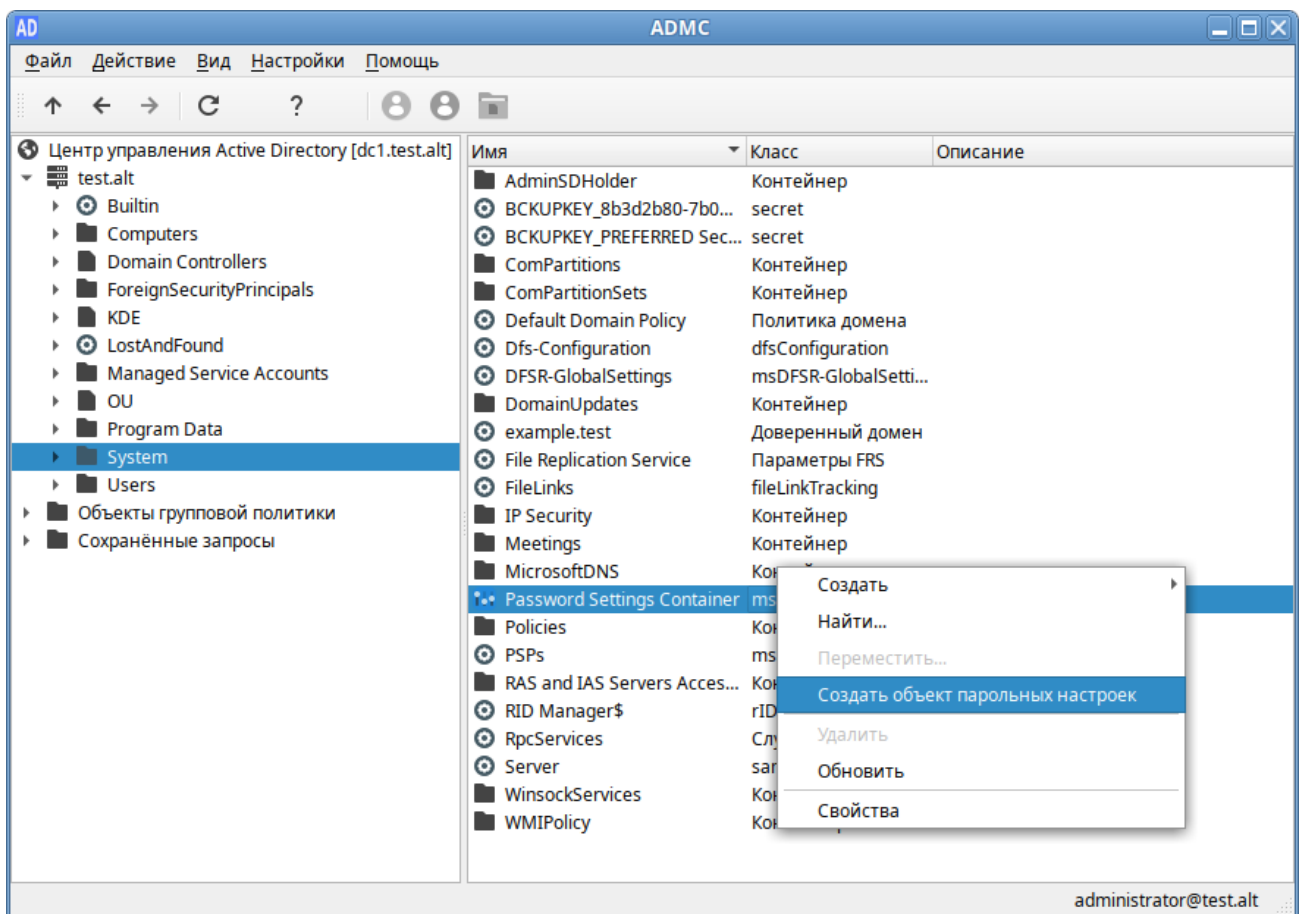


Рис. 298 – Контейнер «Password Settings Container»

The screenshot shows a Windows dialog box titled "Создание объекта парольных настроек — ADMS" (AD Password Settings). The window has a blue title bar with "AD" on the left and a close button on the right. The main content area is titled "Password Settings" and contains several input fields and checkboxes. The fields are arranged in two columns:

Field Name	Value
Имя (Name)	PwPolicyUser
Приоритет (Priority)	1
Минимальная длина пароля (Minimum password length)	10
Длина истории паролей (Password history length)	24
Разрешено неудачных попыток входа (Allow failed logon attempts)	0
Время до сброса блокировки (минуты) (Lockout time (minutes))	30
Минимальный срок действия пароля (дни) (Minimum password age (days))	1
Максимальный срок действия пароля (дни) (Maximum password age (days))	42
Длительность блокировки учетной записи (минуты) (Lockout duration (minutes))	30

Below the fields, there are two checkboxes:

- Включить требования сложности (Require password complexity)
- Хранить пароли, используя обратимое шифрование (Store passwords using reversible encryption)

At the bottom, there is a section "Применить к пользователю/группе" (Apply to user/group) with a list box containing "office" and buttons "Добавить..." (Add...) and "Удалить" (Remove). Below this is a checkbox "Защитить от удаления" (Protect from deletion) which is checked. At the very bottom right are "Отмена" (Cancel) and "ОК" buttons.

Рис. 299 – Создание объекта парольных настроек

При создании объекта парольных настроек необходимо в поле «Имя» указать имя объекта парольных настроек (имя должно быть уникальным на уровне домена).

В поле «Приоритет» можно указать приоритет политики (precedence), который будет учитываться в том случае, если к пользователю или группе пользователей применяются несколько политик. Чем меньше значение этого параметра, тем выше приоритет.

Далее можно указать следующие параметры объекта парольных настроек:

- «Минимальная длина пароля» – минимальное количество символов в пароле (по умолчанию 7);
- «Длина истории паролей» – число хранимых предыдущих паролей пользователей (требование неповторяемости паролей) (по умолчанию 24);

- «Разрешено неудачных попыток входа» – допустимое количество неудачных попыток ввода пароля перед блокировкой учетной записи (по умолчанию 0 – никогда не блокировать);
- «Время до сброса блокировки» – интервал времени (в минутах), по истечении которого записанное количество попыток начинается заново (по умолчанию 30);
- «Минимальный срок действия пароля» – минимальный срок действия пароля (по умолчанию один день);
- «Максимальный срок действия пароля» – максимальный срок действия пароля (по умолчанию 42 дня);
- «Длительность блокировки учетной записи» – интервал времени (в минутах), в течение которого возможность аутентификации для пользователя, превысившего количество попыток входа, будет заблокирована (по умолчанию 30);
- «Включить требования сложности» – должен ли пароль отвечать требованиям сложности (по умолчанию включено);
- «Хранить пароли, используя обратимое шифрование» – хранить пароли, используя обратимое шифрование (по умолчанию выключено).

Примечание. Для создания политики требуется передать новое значение хотя бы для одной парольной настройки.

В окне «Применить к пользователю/группе» следует добавить пользователей и/или группы, к которым должен применяться этот объект парольных настроек.

Примечание. Если при создании объекта парольных настроек отметить пункт «Защитить от удаления», то для удаления данного объекта, необходимо сначала снять данную отметку в окне свойств объекта.

10.4.5.10.2. Изменение объекта парольных настроек

Для удаления объекта парольных настроек следует в контекстном меню объекта выбрать пункт «Удалить» (рис. 300).

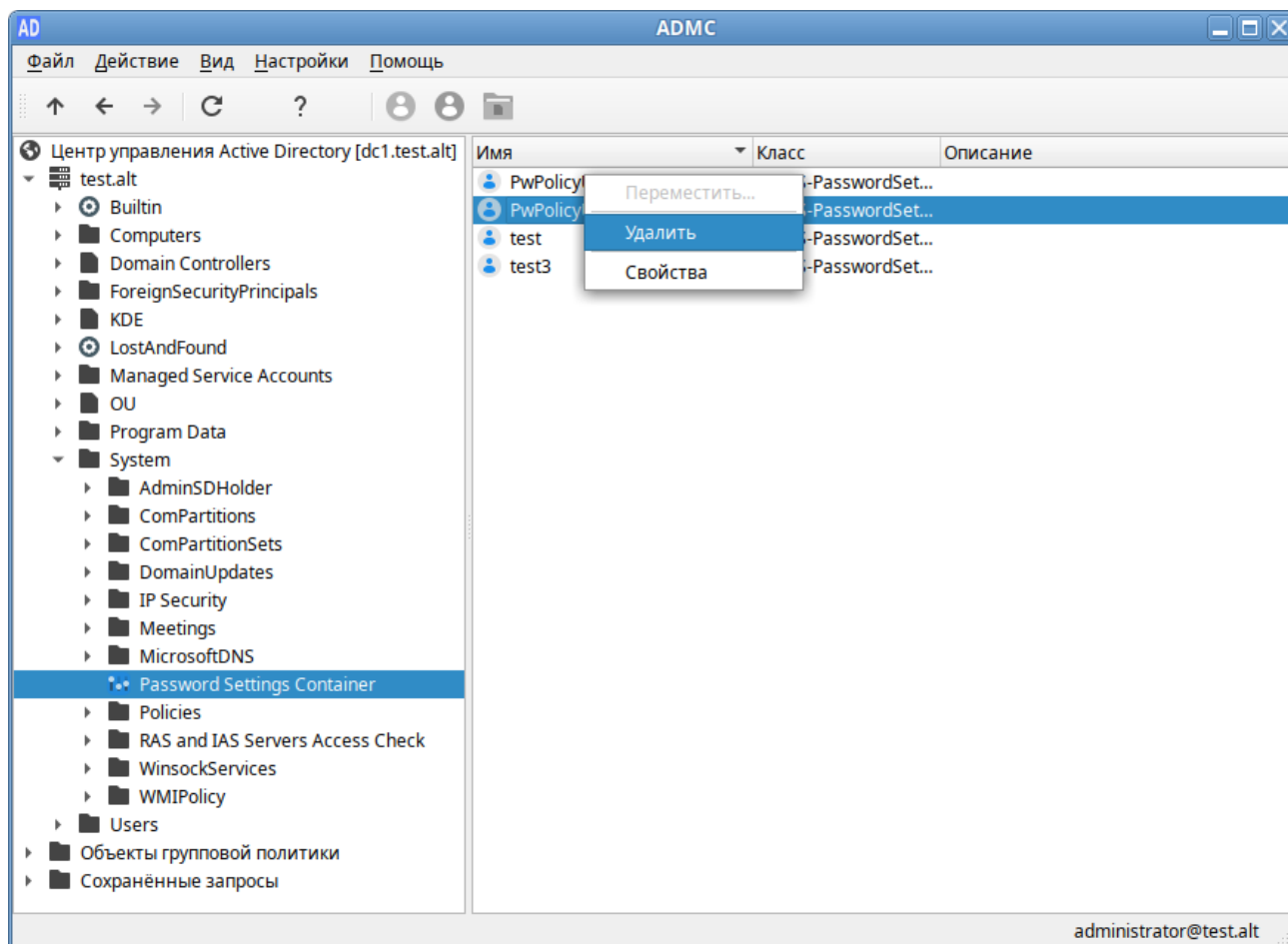


Рис. 300 – Контекстное меню объекта парольных настроек

Примечание. Если при создании объекта парольных настроек был отмечен пункт «Защитить от удаления», то сразу удалить объект не получится, необходимо сначала снять данную отметку в окне свойств объекта парольных настроек (рис. 301).

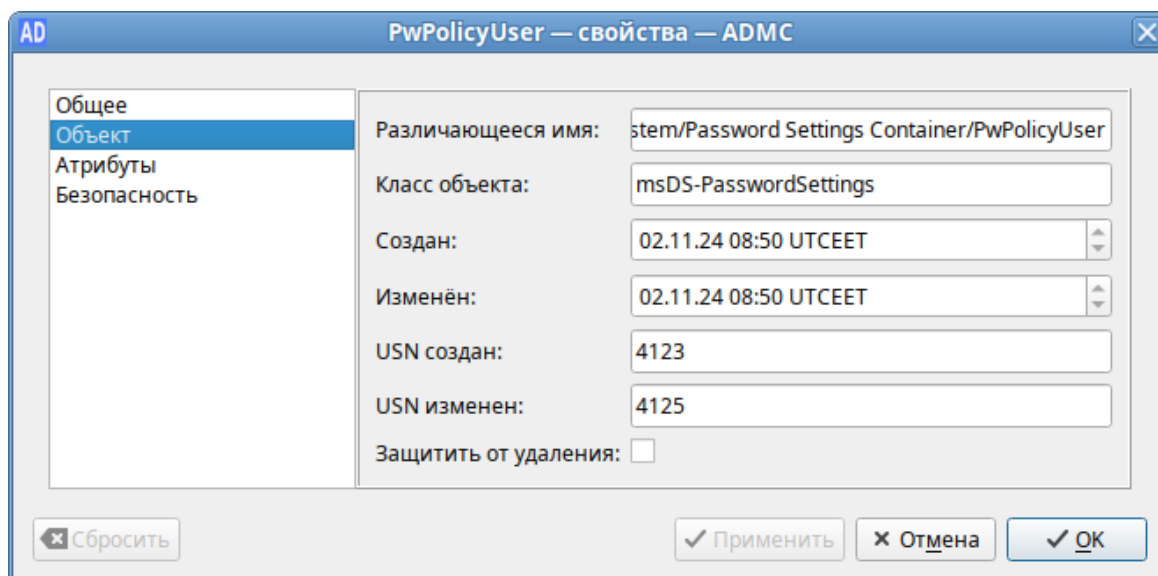


Рис. 301 – Свойства объекта парольных настроек

10.4.5.11. Управление общими папками

Общая папка является ссылкой на общий сетевой ресурс и не содержит никаких данных.

Для создания общей папки следует в контекстном меню контейнера выбрать пункт «Создать» → «Общая папка». Окно мастера создания общей папки (рис. 302).

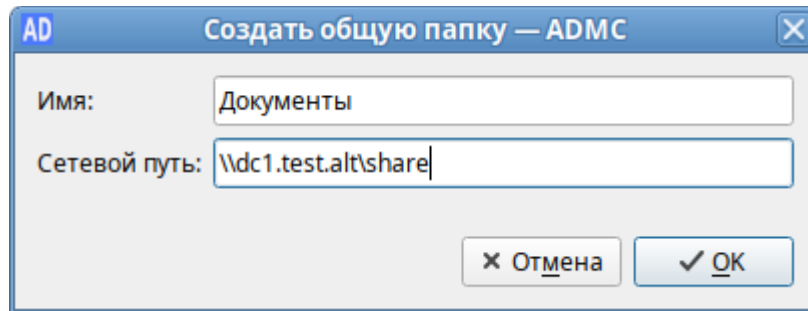


Рис. 302 – Создание общей папки

В поле «Имя» следует ввести название папки, под которым она будет отображаться в каталоге «Альт Домен», а в поле «Сетевой путь» – полный сетевой путь к общей папке.

Для изменения общей папки следует в контекстном меню общей папки выбрать соответствующее действие (рис. 303).

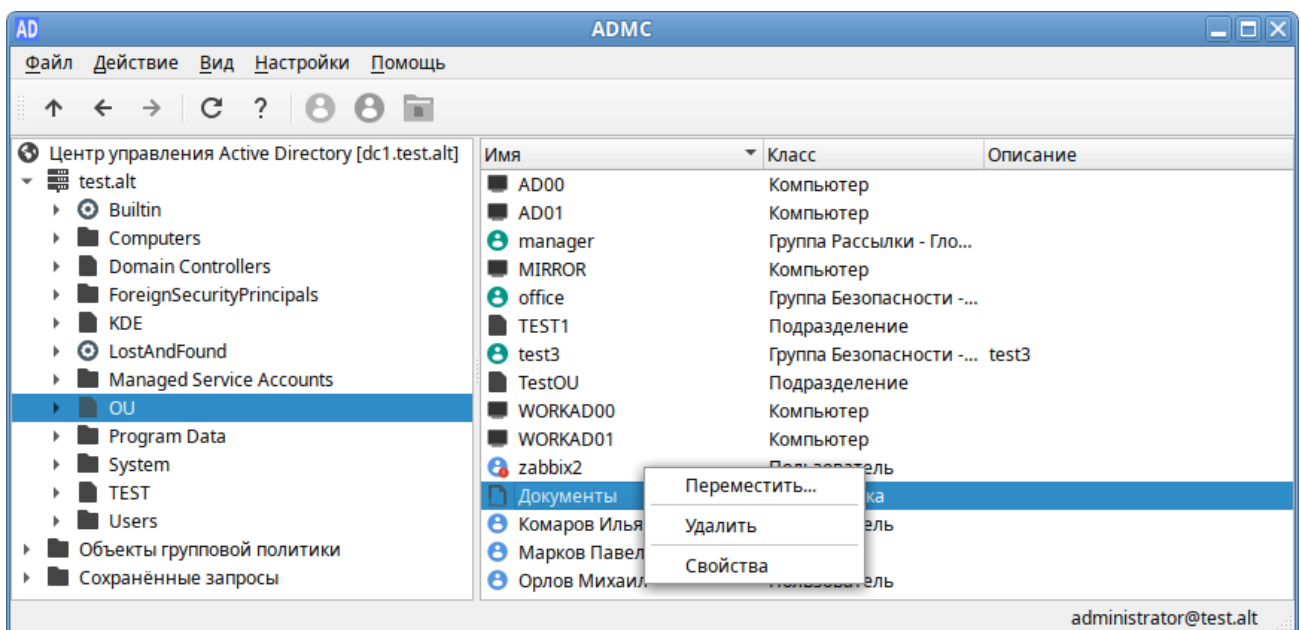


Рис. 303 – Изменение общей папки

Примечание. Чтобы просмотреть содержимое общей папки, на машине Windows в дереве консоли управления «Active Directory – пользователи и компьютеры» в контекстном меню общей папки следует выбрать пункт «Проводник». Откроется новое окно «Проводника», в котором будет показано содержимое общей папки.

10.4.5.12. Управление объектами групповых политик

Групповая политика состоит из набора политик, называемых объектами групповой политики. Для вступления настроек в силу, объект групповой политики нужно связать с одним или несколькими контейнерами домена. Любой объект групповой политики может быть связан с несколькими контейнерами, и, наоборот, с конкретным контейнером может быть связано несколько объектов групповой политики. Контейнеры наследуют объекты групповой политики, например, объект групповой политики, связанный с подразделением, применяется ко всем пользователям и компьютерам в его дочерних подразделениях. Аналогичным образом, объект групповой политики, применяемый к OU, применяется не только ко всем пользователям и компьютерам в этом OU, но и наследуется всем пользователям и компьютерам в дочерних OU.

ADMC позволяет управлять объектами групповых политик: создавать, удалять, создавать ссылки на групповые политики.

В разделе «Объекты групповой политики» (рис. 304) отображаются групповые политики, которые назначены на различные OU (отображается вся структура OU). Полный список политик в текущем домене доступен в разделе «Все политики».

Примечание. В «Альт Домен» по умолчанию создаются два объекта групповой политики, которые действуют на все компьютеры и контроллеры домена соответственно:

- Default Domain Policy;
- Default Domain Controller Policy.

Примечание. Эти объекты групповой политики очень важны, поэтому не рекомендуется вносить в них изменения без крайней необходимости.

Групповые политики можно назначить на OU или весь домен. Чаще всего политики привязываются к OU с компьютерами или пользователями.

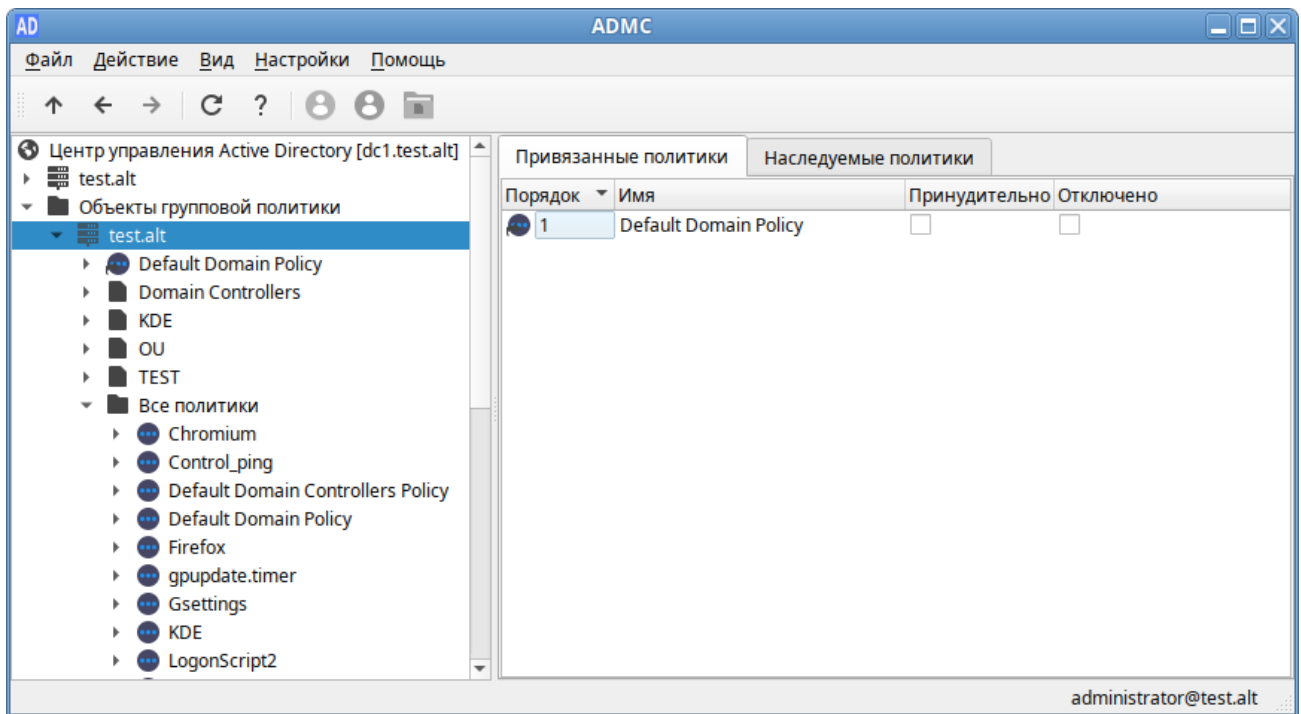


Рис. 304 – Объекты групповой политики

10.4.5.12.1. Создание объекта групповой политики

Для того чтобы создать новый объект групповой политики и сразу назначить его на OU нужно выполнить следующие действия:

- 1) в контекстном меню нужного контейнера выбрать пункт «Создать политику и связать с этим подразделением» (рис. 305);

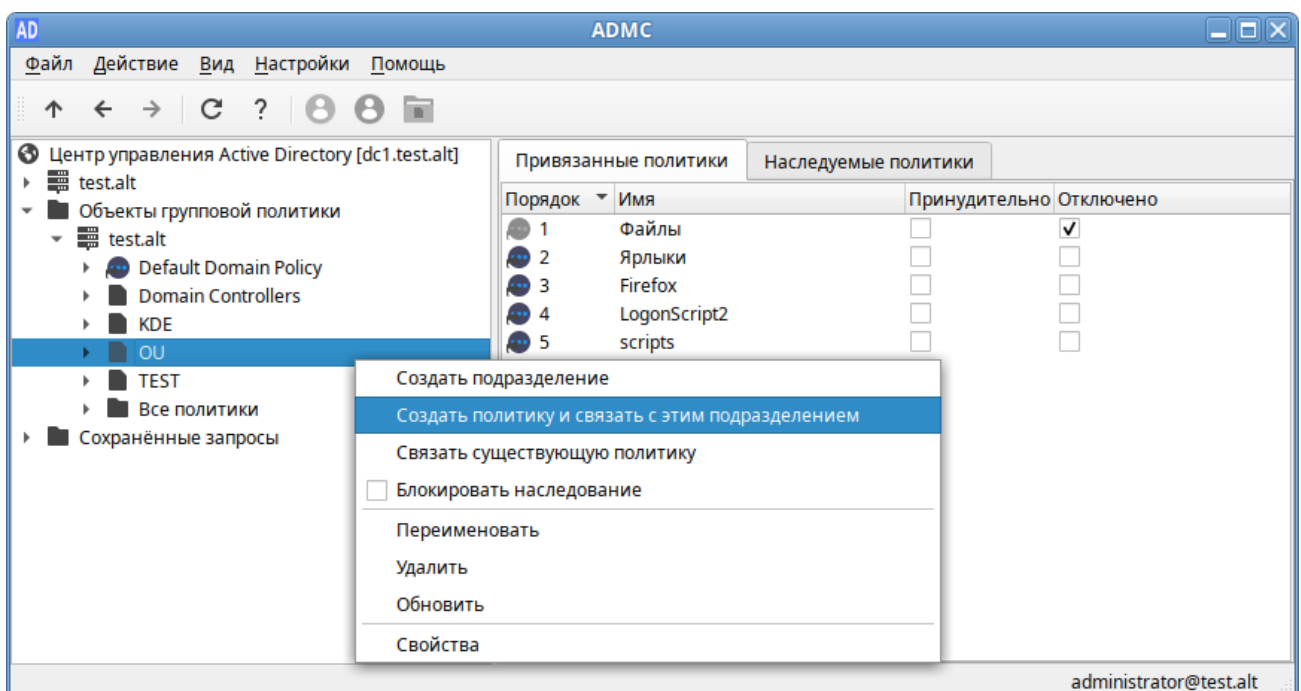


Рис. 305 – Контекстное меню контейнера

- 2) в открывшемся окне задать имя политики (рис. 306);
- 3) нажать кнопку «ОК».

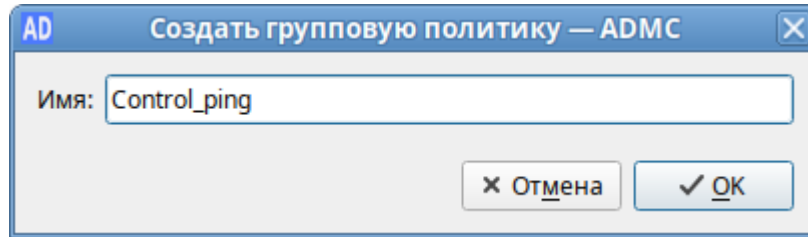


Рис. 306 – Создание объекта групповой политики

Для того чтобы создать новый объект групповой политики, не назначая его на OU, нужно выполнить следующие действия:

- 1) в контекстном меню папки «Все политики» выбрать пункт «Создать политику» (рис. 307);

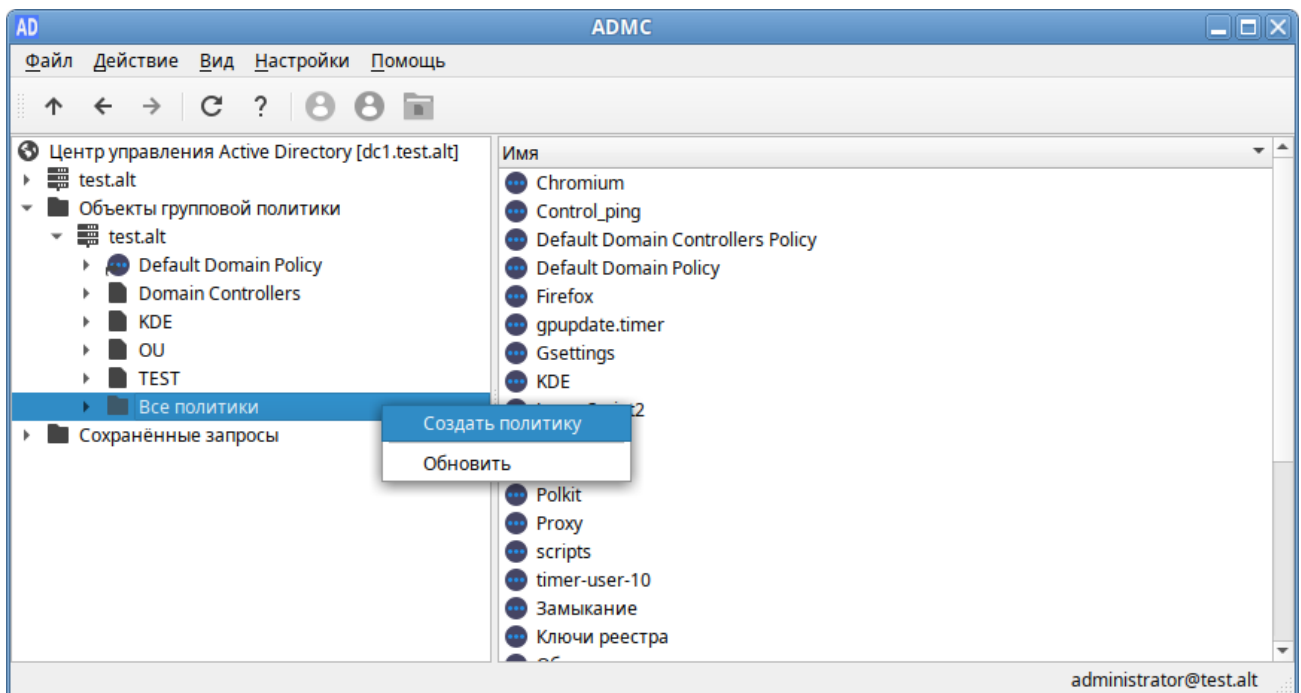


Рис. 307 – Контекстное меню папки «Все политики»

- 2) в открывшемся окне задать имя политики (рис. 306);
- 3) нажать кнопку «ОК».

Созданный объект групповой политики не будет задействован, пока не будет привязан к подразделению.

Примечание. Редактирование групповых политик реализуется в модуле редактирования настроек клиентской конфигурации (GPUI).

10.4.5.12.2. Изменение объекта групповой политики

Для изменения объекта групповой политики следует в контекстном меню политики выбрать соответствующее действие (рис. 308, рис. 309).

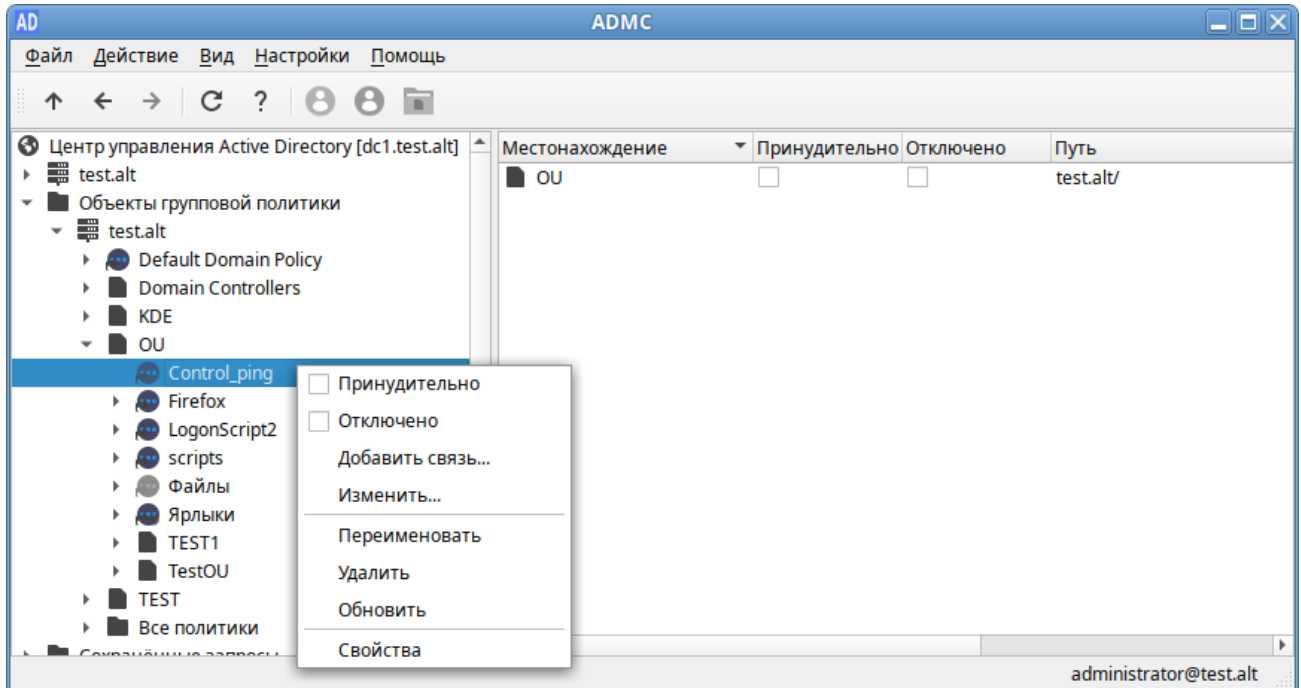


Рис. 308 – Контекстное меню объекта групповой политики

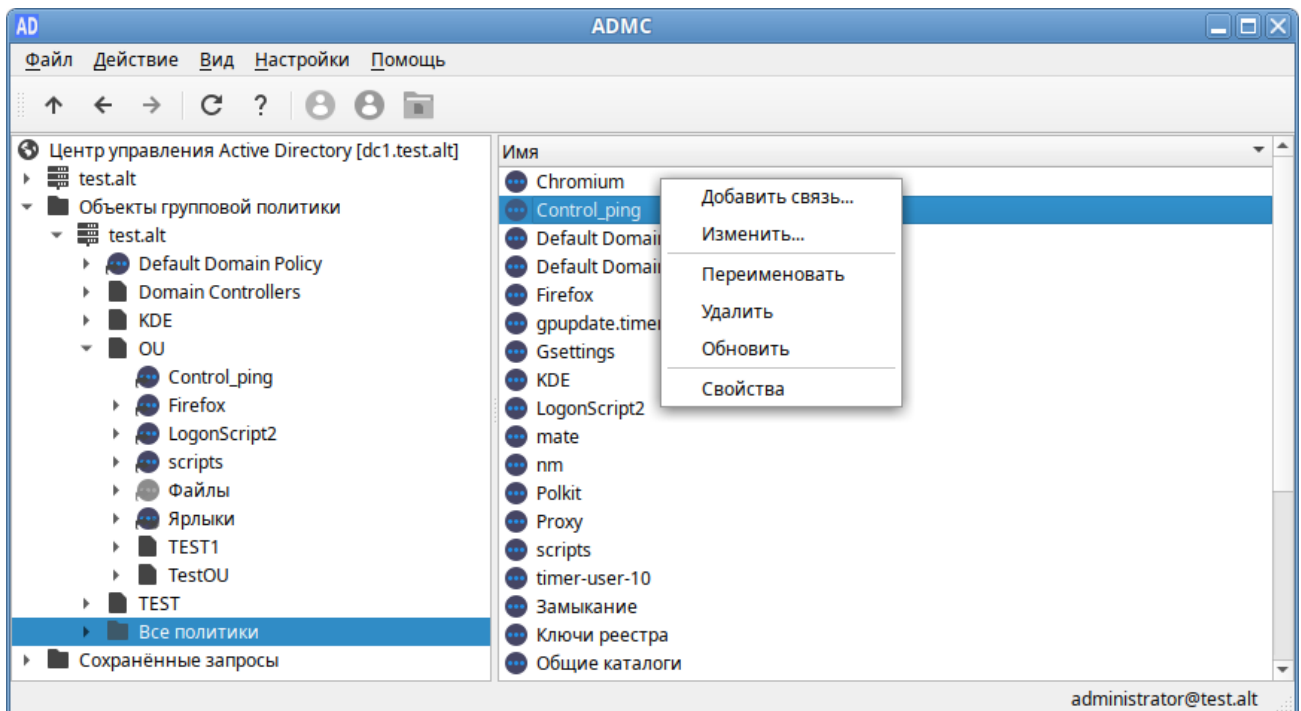


Рис. 309 – Контекстное меню объекта групповой политики

10.4.5.12.2.1. Переименование объекта групповой политики

Для переименования политики:

- 1) в контекстном меню политики выбрать пункт «Переименовать»;
- 2) в открывшемся окне ввести новое название (рис. 310);

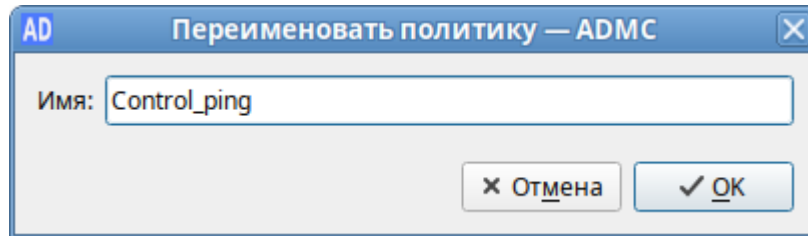


Рис. 310 – Переименование объекта групповой политики

- 3) нажать кнопку «ОК» для сохранения изменений.

10.4.5.12.2.2. Удаление объекта групповой политики

Для удаления политики:

- 1) в контекстном меню политики в разделе «Все политики» выбрать пункт «Удалить» (рис. 309);
- 2) подтвердить удаление, нажав кнопку «Да» (рис. 311).

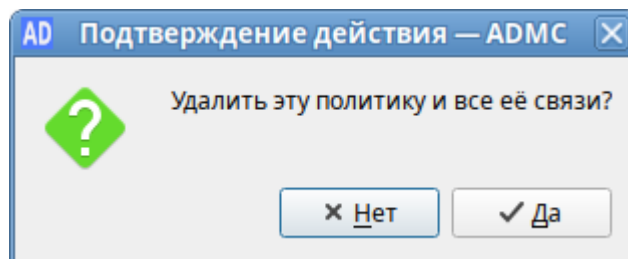


Рис. 311 – Подтверждение удаления

Примечание. Если выбрать пункт «Удалить» в контекстном меню политики в подразделении (см. рис. 308), на которое она назначена, будет удалена только связь между политикой и подразделением (рис. 312).

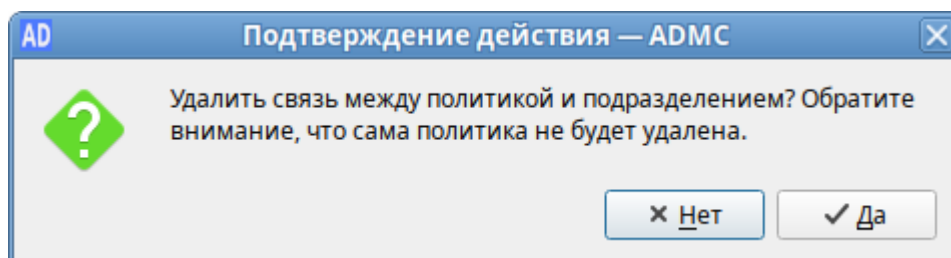


Рис. 312 – Подтверждение действия

10.4.5.12.2.3. Создание и удаление связи между политикой и подразделением
Для связи между политикой и подразделением (создания ссылки на политику):

- 1) в контекстном меню политики выбрать пункт «Добавить связь...»;
- 2) выбрать объекты, которые нужно связать с политикой;
- 3) нажать кнопку «ОК» (рис. 313).

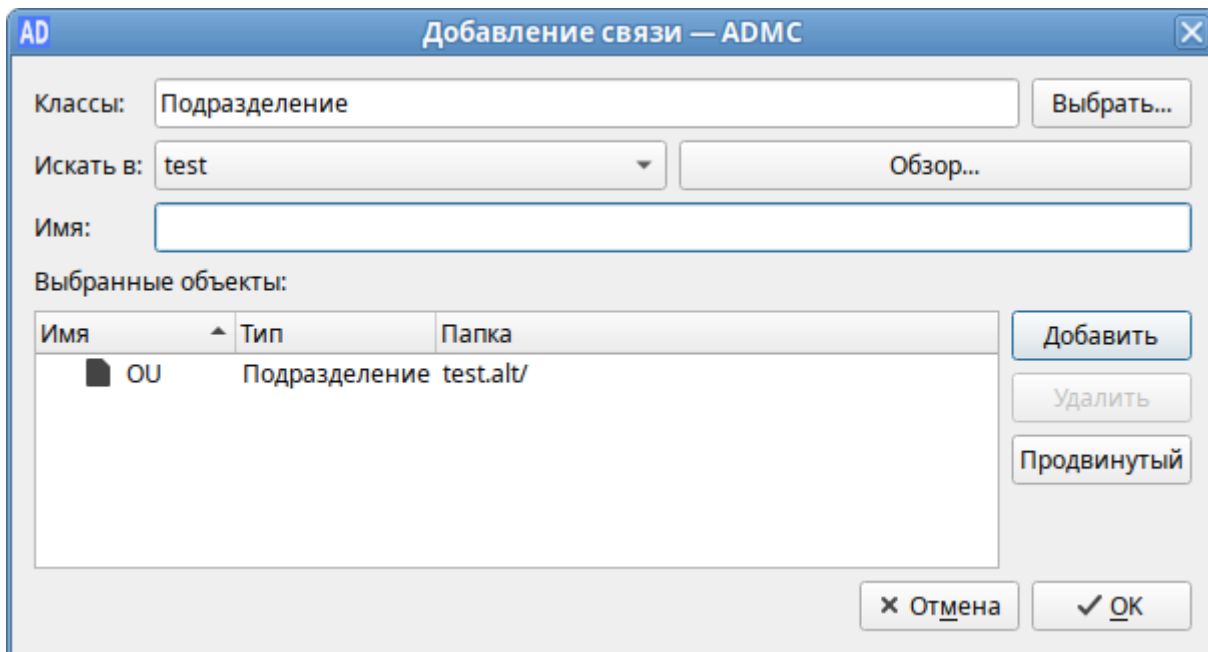


Рис. 313 – Добавление связи

Для удаления ссылки на объект групповой политики:

- выбрать политику, которую следует изменить (в папке «Все политики» или в папке соответствующего OU);
- в контекстном меню подразделения, связь с которым нужно отключить от политики, выбрать пункт «Удалить связь» (рис. 314).

Удалить связь между политикой и подразделением также можно, выбрав пункт «Удалить» в контекстном меню политики в подразделении, на которое она назначена (см. рис. 308).

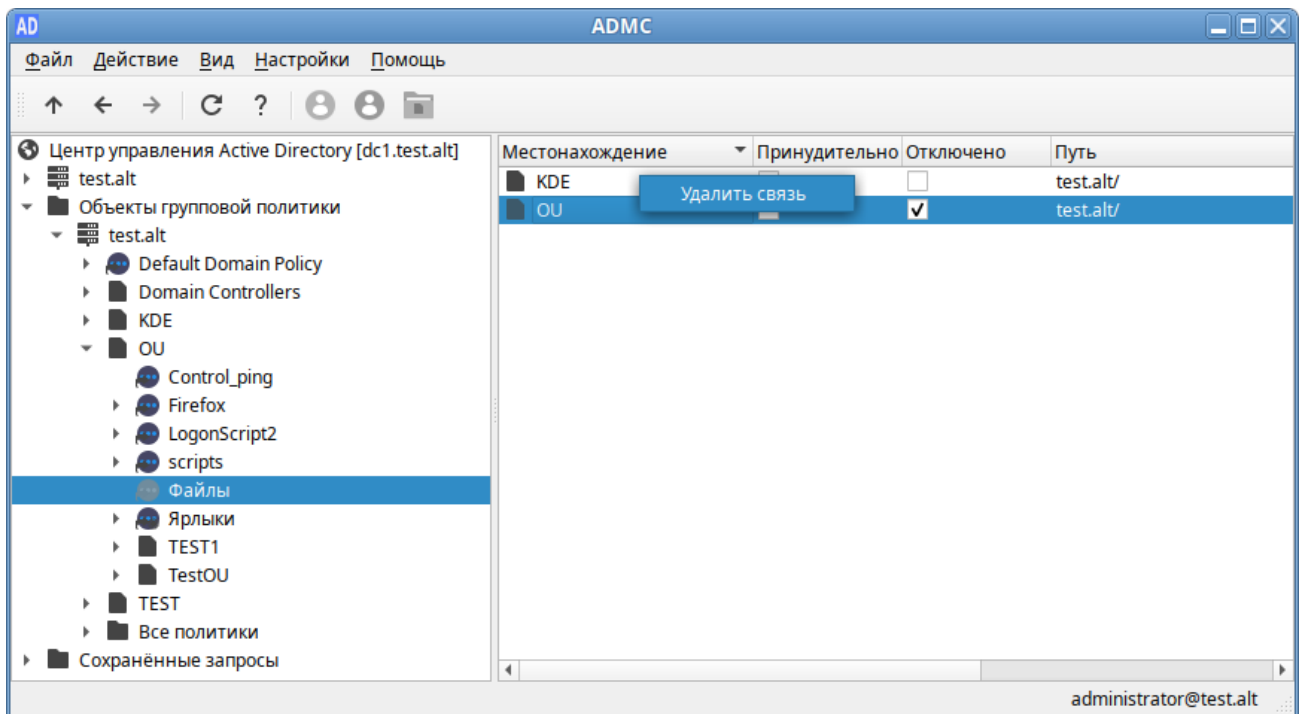


Рис. 314 – Пункт «Удалить связь»

В ADMC можно изменить параметры ссылки на объект групповой политики:

- опция «Принудительно» – принудительное применение политик более высокого уровня к объекту;
- опция «Отключено» – временно отключить связь политики с подразделением.

Чтобы отредактировать параметры ссылки, нужно:

- 1) выбрать политику, которую следует отредактировать;
- 2) на панели результатов найти подразделение, для которого нужно изменить параметры ссылки (рис. 315);
- 3) включить опцию «Принудительно», чтобы запретить переопределение параметров политик (см. п. 10.4.5.12.3). Политика, с включенной опцией «Принудительно», отображается в списке политик с красным кружком;
- 4) включить опцию «Отключено», чтобы временно отключить действие политики. Отключенная политика, в списке политик отображается серым цветом.

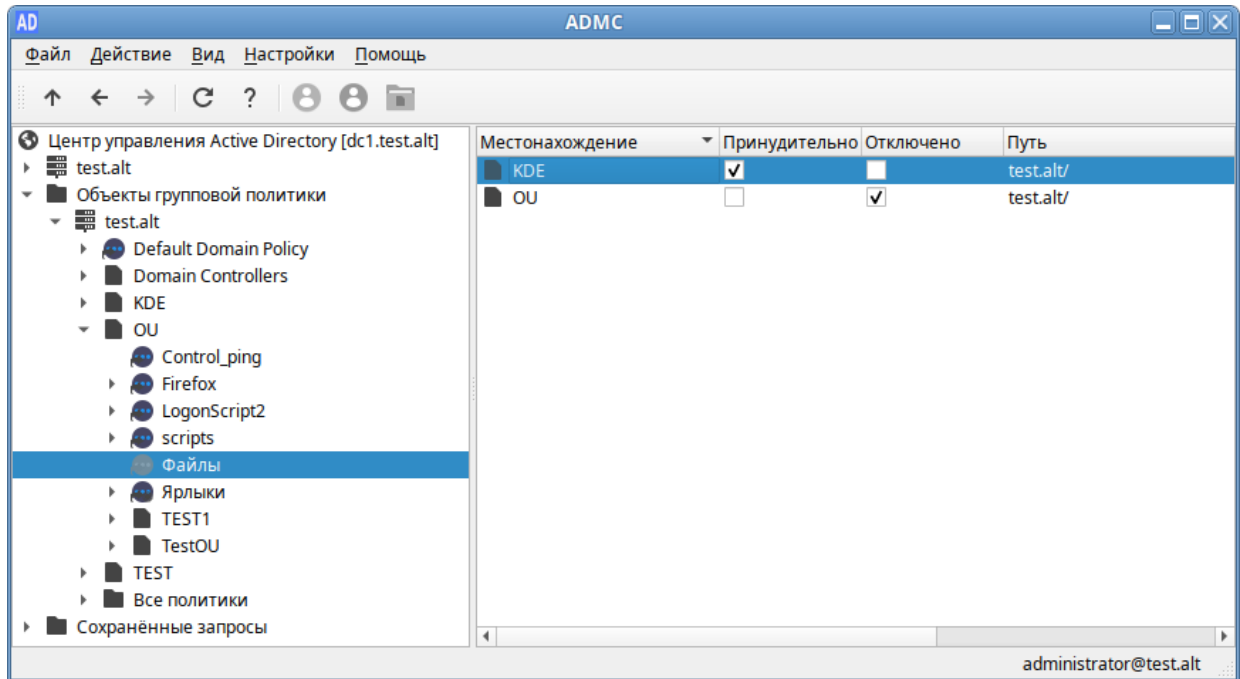


Рис. 315 – Редактирование параметров ссылки

Примечание. Если нужно, чтобы политика перестала действовать на клиентов в данном подразделении, можно либо удалить ссылку (при этом сама объект ГП не будет удален), либо временно отключить действие политики.

Включить/отключить опции «Принудительно» и «Отключено» также можно:

- в контекстном меню политики в подразделении (см. рис. 308);
- на вкладке «Привязанные политики» подразделения (рис. 316).

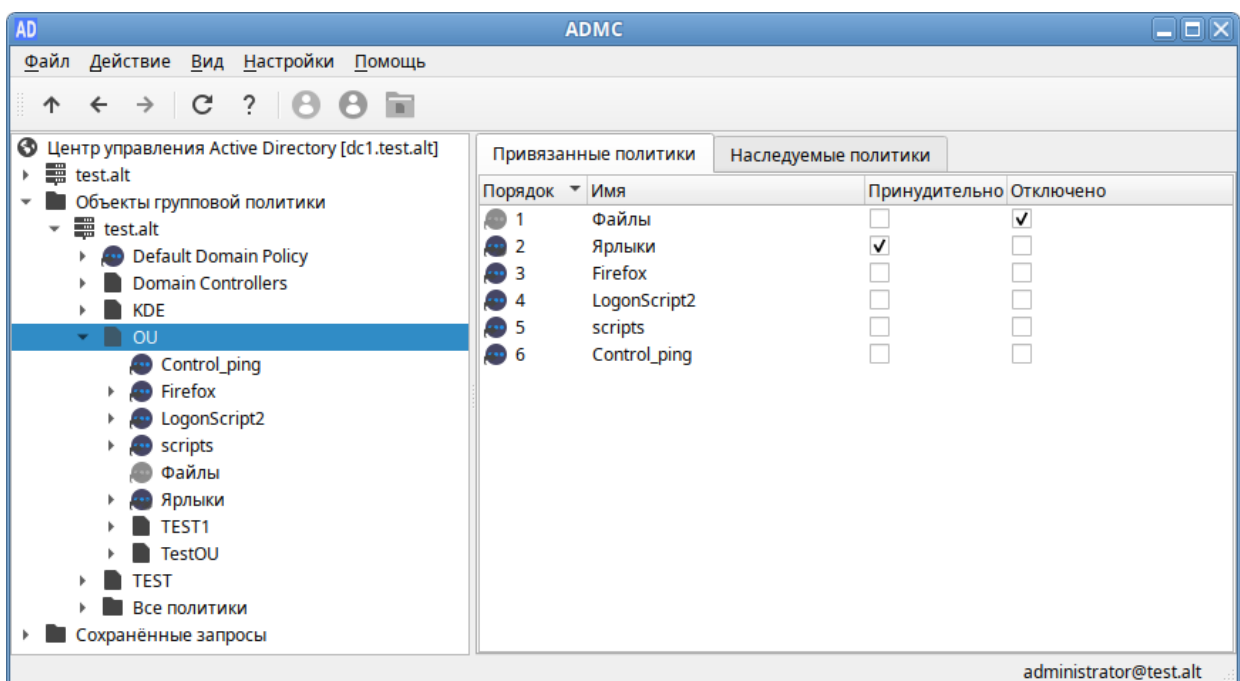


Рис. 316 – Опции «Принудительно» и «Отключено» на вкладке подразделения

10.4.5.12.2.4. Редактирование настроек групповой политики

Примечание. Для возможности редактирования настроек политики, на машине должен быть установлен модуль редактирования настроек клиентской конфигурации (GPUI).

Для изменения настроек политики нужно в контекстном меню политики выбрать пункт «Изменить...», будет запущен модуль редактирования настроек клиентской конфигурации, где можно изменить параметры групповой политики.

При создании каждого нового объекта групповой политики, в базе данных домена создается контейнер групповой политики (Group Policy Container, GPC). Для возможности просмотра контейнера групповой политики (это дочерний контейнер Policies контейнера System) в настройках ADMC должен быть отмечен пункт «Дополнительные возможности».

В «Альт Домен» контейнер групповой политики создается как тип groupPolicyContainer, причем его GUID можно увидеть в ADMC в столбце «Имя» (рис. 317).

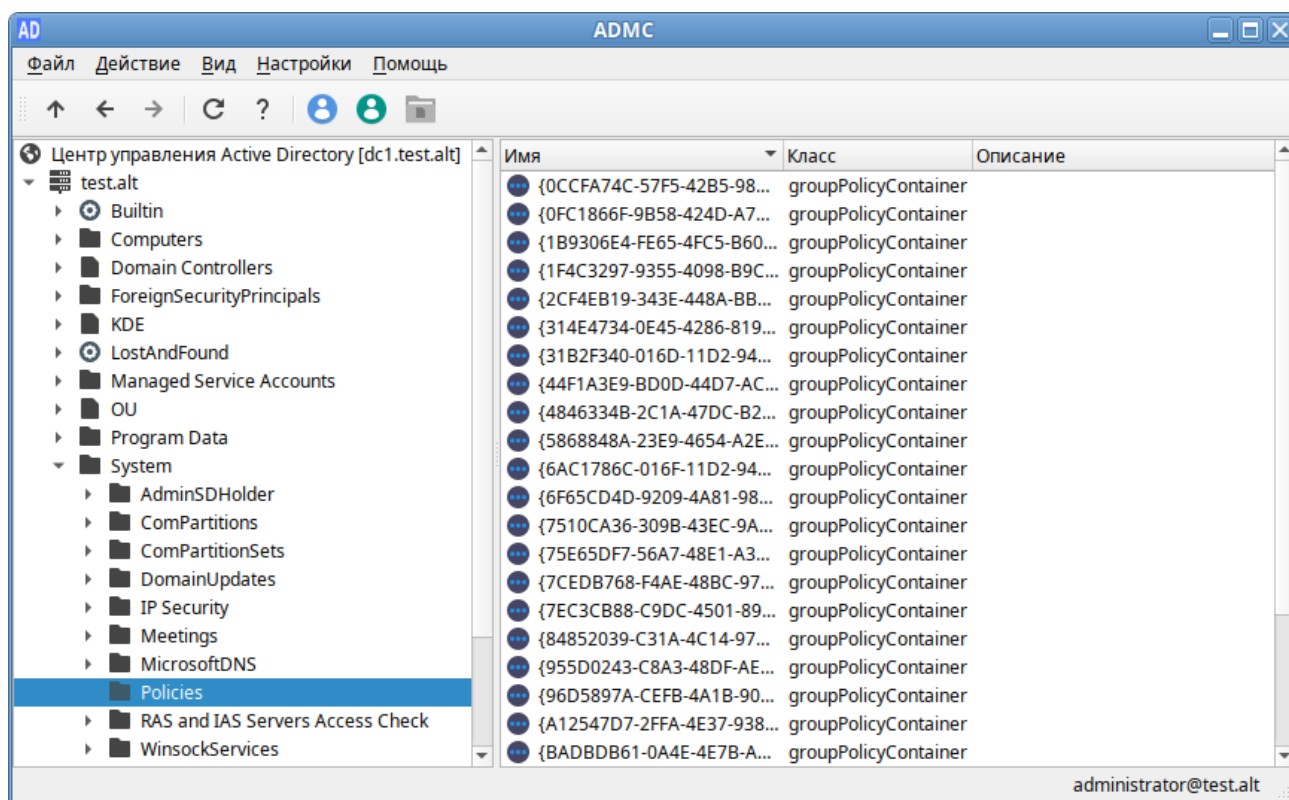


Рис. 317 – Контейнеры групповых политик

Ниже перечислены некоторые атрибуты, позволяющие описать различные типы данных объекта групповой политики (рис. 318):

- `displayName` – атрибут, определяющий имя объекта групповой политики;
- `gPCFileSysPath` – атрибут, указывающий путь к расположению текущего шаблона групповой политики с соответствующим именем GUID;
- `gPCMachineExtensionNames` – атрибут, определяющий список расширений клиентской стороны конфигурации компьютера, используемых для обработки объекта групповой политики. Значение атрибута выглядит следующим образом: `[{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{D02B1F72-3407-48AE-BA88-E8213C6761F1}]`, что представляет собой `[{GUID CSE-расширения}{GUID расширения MMC}{GUID второго расширения MMC}][GUID-идентификаторы последующих CSE- и MMC-расширений]`;
- `gPCUserExtensionNames` – атрибут, определяющий список расширений клиентской стороны конфигурации пользователя, используемых для обработки объекта групповой политики;
- `versionNumber` – в этом атрибуте определен номер версии контейнера GPO объекта групповой политики, который, для осуществления синхронизации двух объектов, должен быть идентичным с номером версии шаблона групповой политики;
- `flags` – состояние объекта групповой политики: объект ГП включен (значение 0), отключен раздел «Конфигурация пользователя» (значение 1), отключен раздел «Конфигурация компьютера» (значение 2), объект GPO полностью отключен (значение 3).

Примечание. Вручную изменять атрибуты объекта групповой политики не рекомендуется.

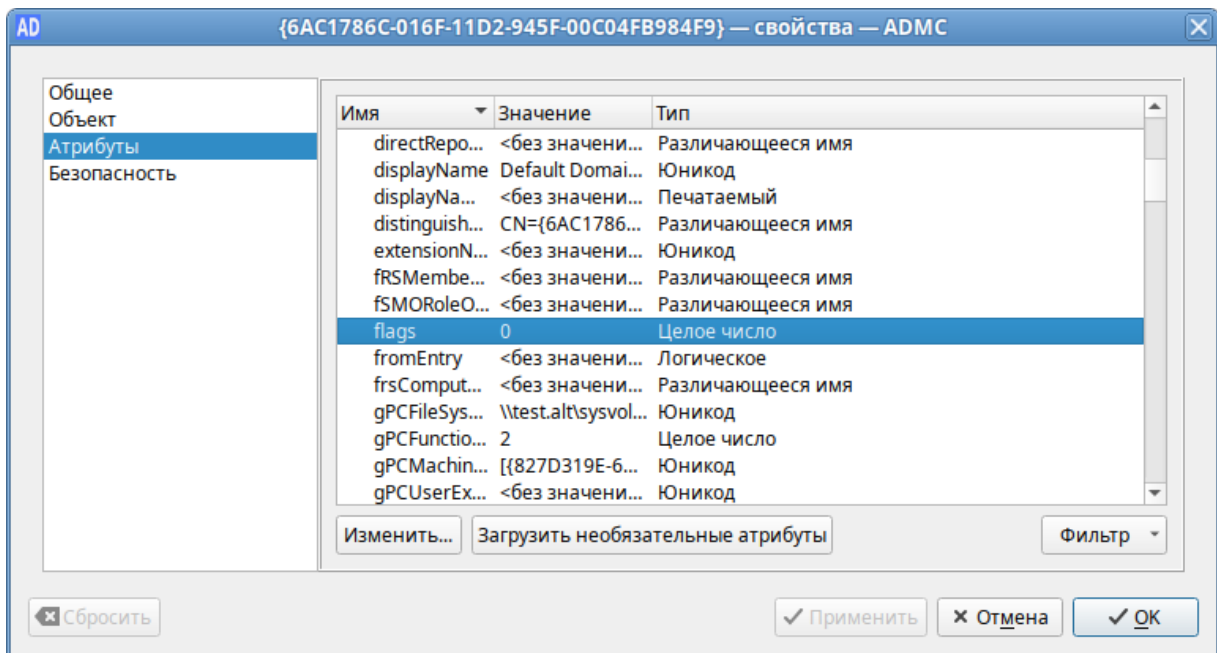


Рис. 318 – Атрибуты объекта групповой политики

10.4.5.12.3. Блокирование наследования

Для того чтобы параметры групповой политики, определенные на уровне вышестоящих контейнеров, не распространялись на содержимое конфигурируемого контейнера нужно выполнить одно из следующих действий:

- 1) в контекстном меню контейнера, к которому привязан объект групповой политики, установить отметку «Блокировать наследование» (рис. 319);

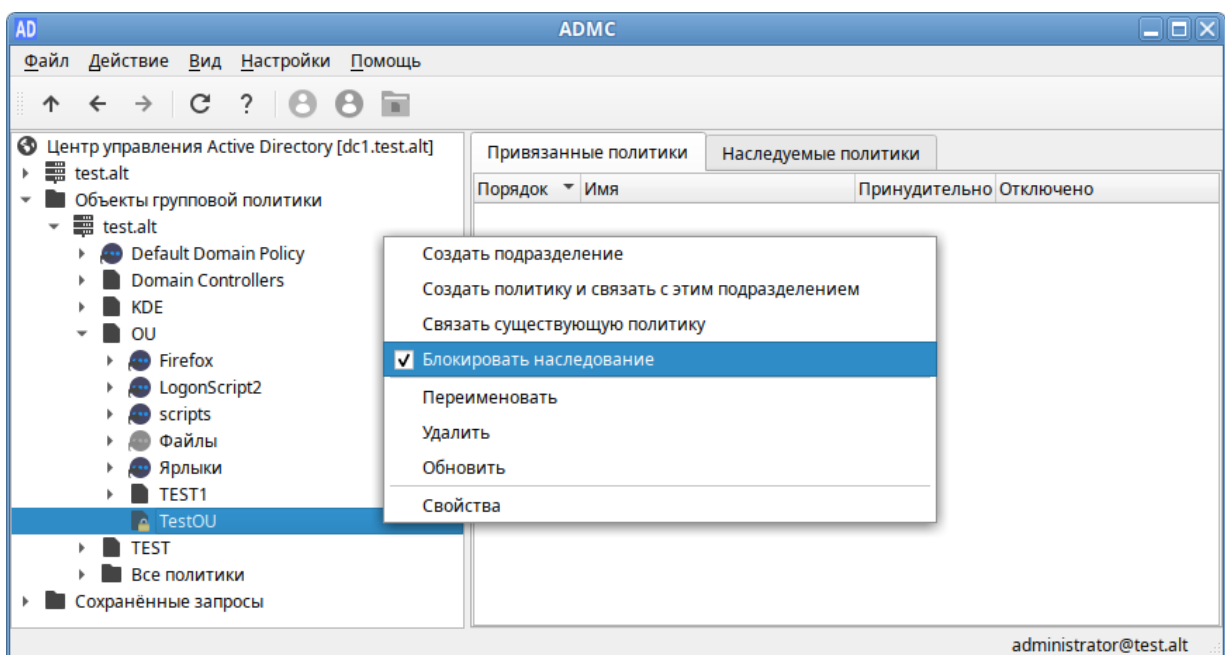


Рис. 319 – Отметка «Блокировать наследование»

- 2) в окне свойств контейнера, к которому привязан объект групповой политики, на вкладке «Групповая политика» установить отметку «Заблокировать наследование политик» (рис. 320);

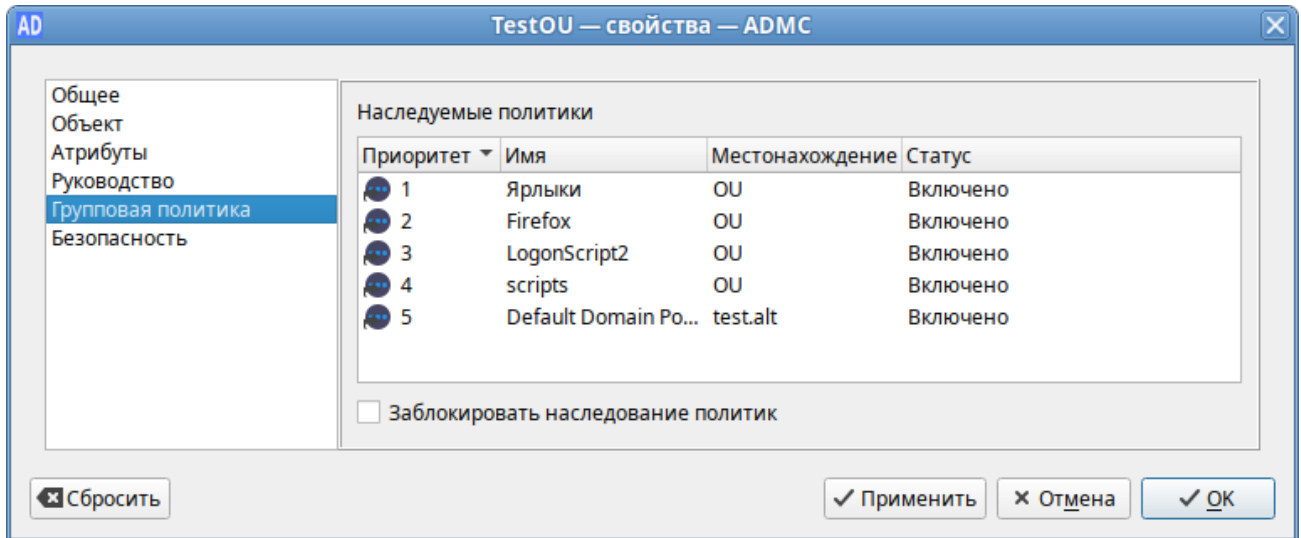


Рис. 320 – Окно свойств контейнера

Так как администратор домена может не согласиться с тем, что администратор подразделения блокирует параметры политики домена, существует возможность запретить переопределение параметров с помощью отметки «Принудительно» (рис. 321).

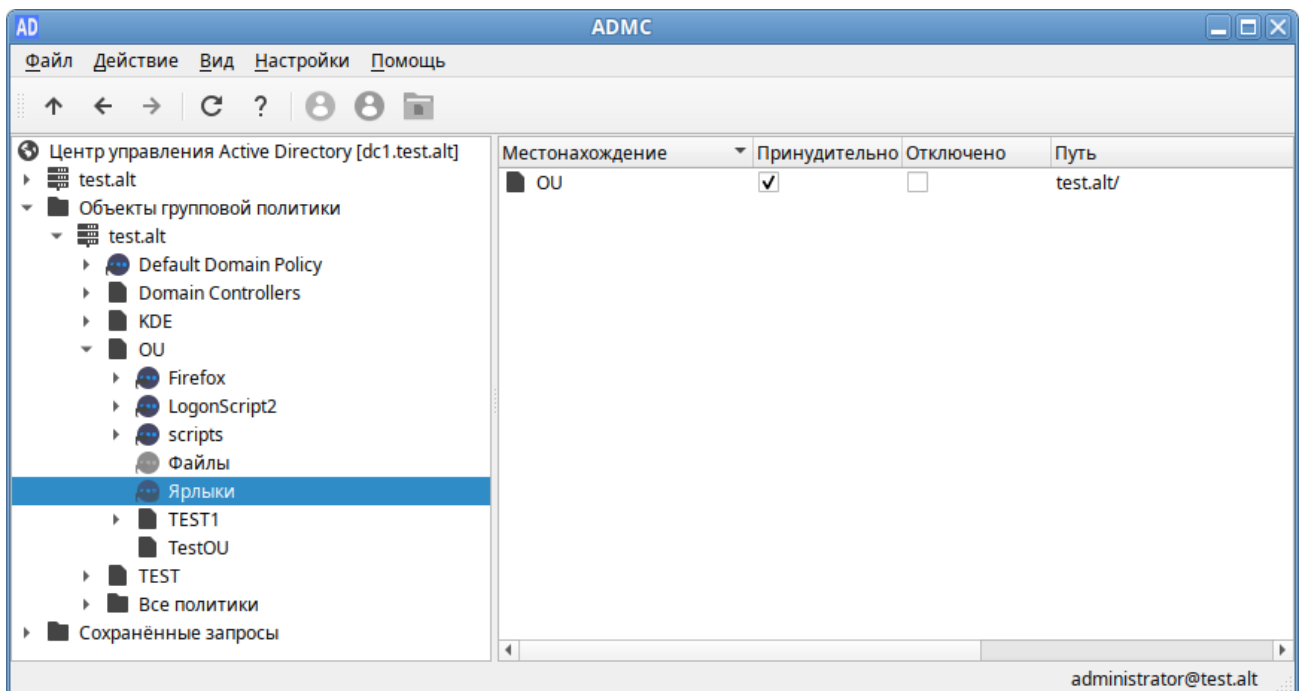


Рис. 321 – Переопределение параметров с помощью отметки «Принудительно»

Отметка в поле «Принудительно» означает, что связь установлена принудительно. Это приведет к принудительному применению политик более высокого уровня к объектам более низкого уровня, например, применение политики домена ко всем дочерним подразделениям, или применения политики сайта ко всем доменам и подразделениям в пределах сайта.

При использовании параметра «Принудительно» выигрывает та политика, которая находится выше в иерархии домена (например, при включении «Принудительно» у политики Default Domain Policy, она выигрывает у всех других групповых политик).

Примечание. Подразделение с заблокированным наследованием отображается в дереве консоли со значком замка.

После установки параметра «Принудительно», на значке групповой политики появится красный кружок, означающий, что для данной политики запрещено переопределение параметров.

На вкладке «Наследуемые политики» подразделения можно увидеть, какие политики применяются к подразделению, а также местонахождение политики (рис. 322).

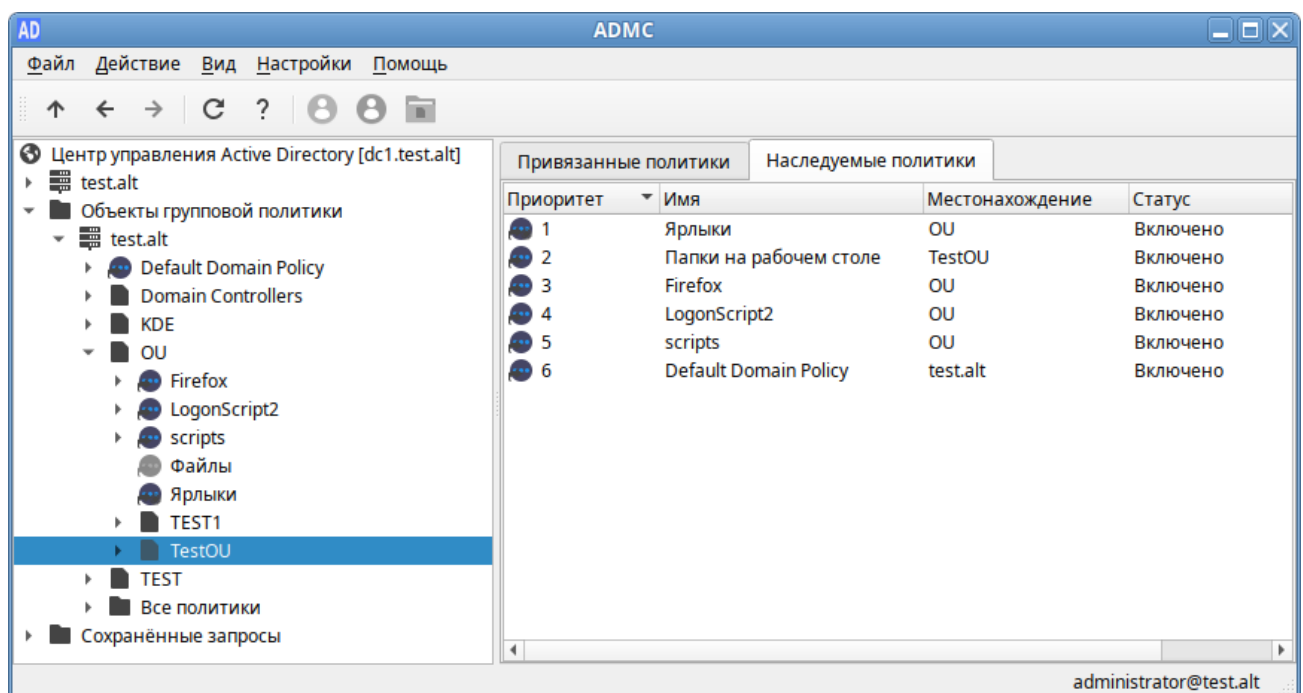


Рис. 322 – Вкладка «Наследуемые политики»

10.4.5.12.4. Фильтрация безопасности ГП

Фильтрация безопасности ГП (Security Filtering) предполагает выборочное применение параметров ГП к конкретным пользователям, компьютерам или группам на основе их разрешений безопасности.

По умолчанию, когда объект ГП связан с ОУ, он применяется ко всем пользователям и компьютерам в этой ОУ. Фильтрация безопасности позволяет администраторам сузить область применения объекта ГП, гарантируя, что только определенные объекты будут затронуты политиками, определенными в объекте групповой политики.

По умолчанию на всех новых объектах групповой политики в домене присутствуют разрешения для группы «Authenticated Users», которая включает в себя всех пользователей и все компьютеры домена. Это означает, что данная политика будет применяться на всех компьютерах и для всех пользователей, которые попадают в область ее действия.

Если необходимо сузить круг объектов, к которым будет применяться данная политика, то следует выполнить следующие действия:

- 1) в контекстном меню групповой политики выбрать пункт «Свойства» (рис. 323);
- 2) на вкладке «Безопасность» у группы «Authenticated Users» убрать разрешение на применение групповых политик (снять отметку с пункта «Применить групповые политики» в столбце «Разрешено») (рис. 324);
- 3) добавить объект, к которому будет применяться групповая политика. Для этого нажать «Добавить...» и выбрать необходимый объект (можно выбрать пользователя, компьютер или группу). В данном примере будет добавлена группа «office» (рис. 325);
- 4) для добавленного объекта выставить разрешения «Читать» и «Применить групповые политики» (рис. 326) и нажать кнопку «Применить».

Примечание. Если выставить все разрешения, групповые политики применяться не будут.

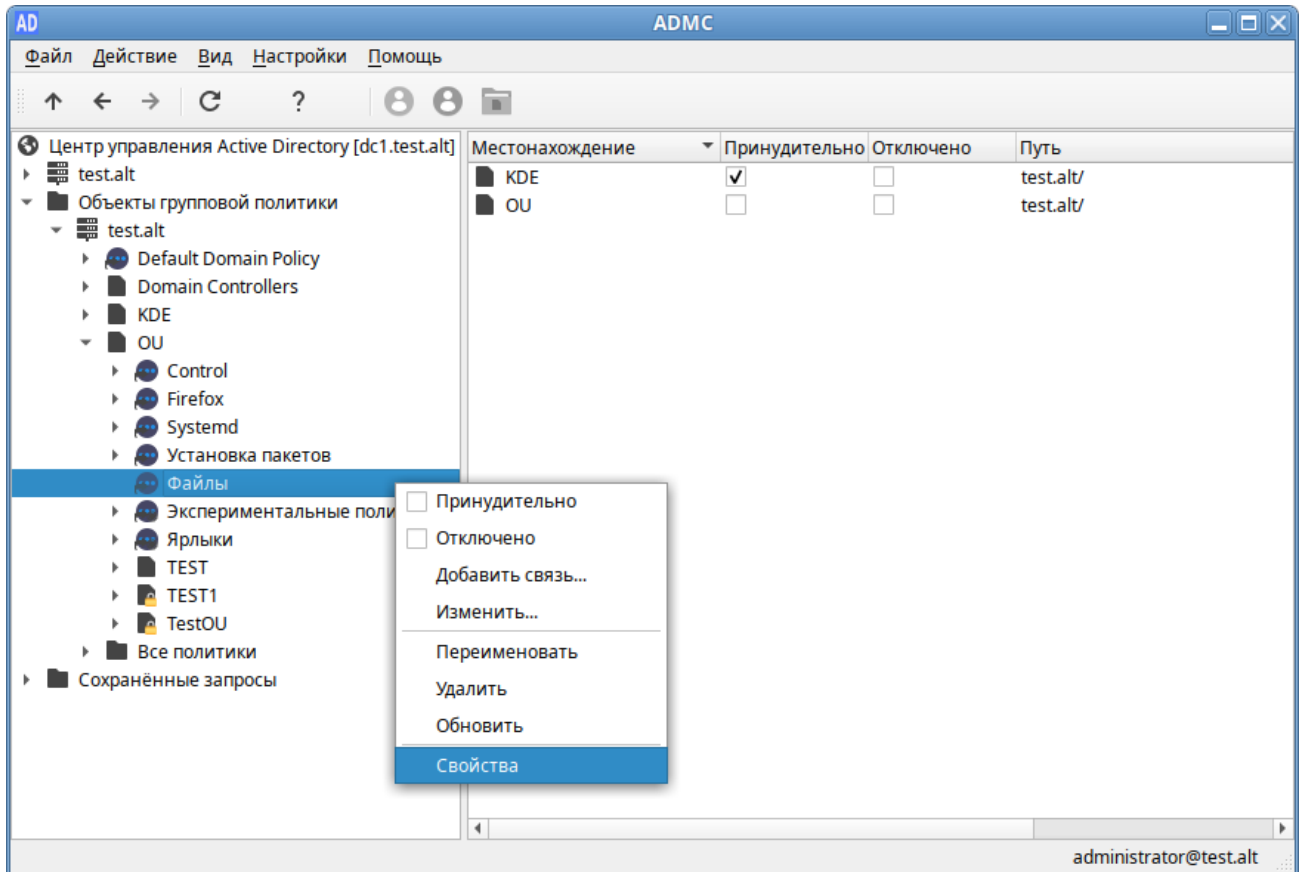


Рис. 323 – Контекстное меню групповой политики

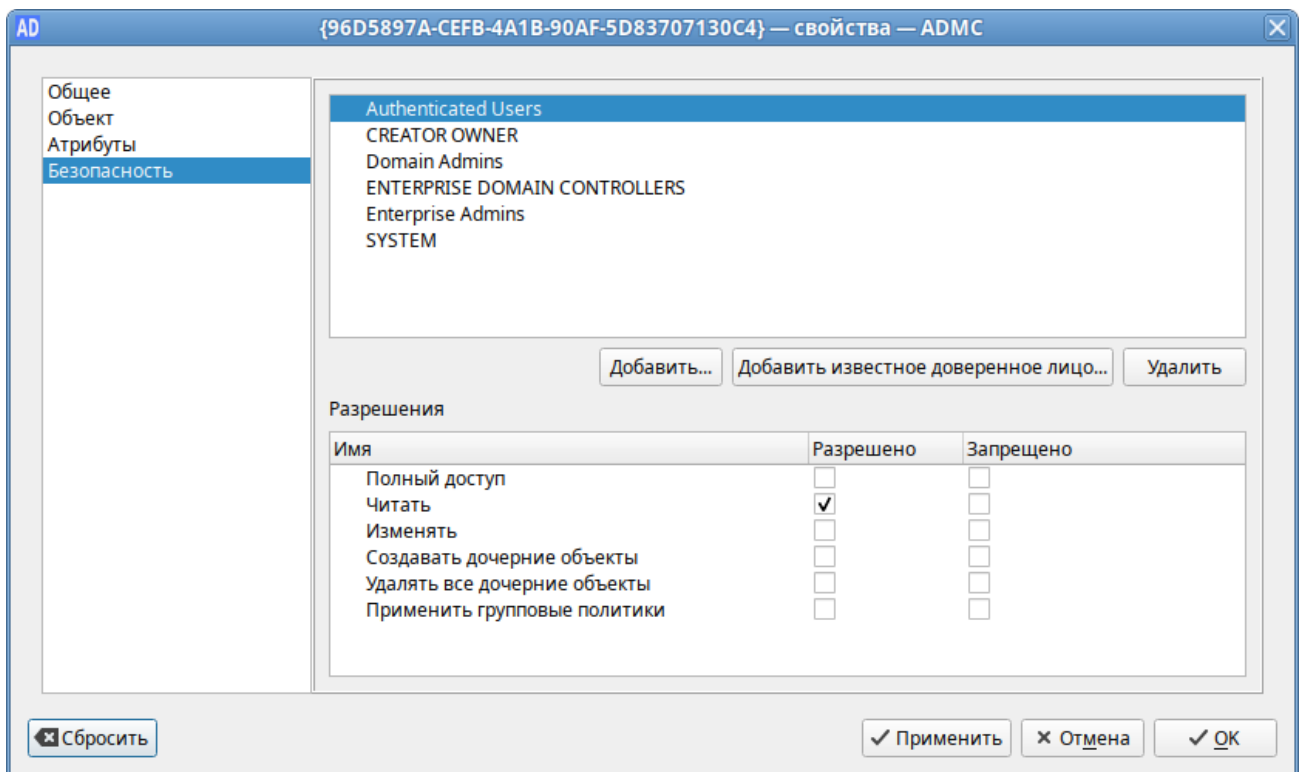


Рис. 324 – Вкладка «Безопасность» свойства групповой политики

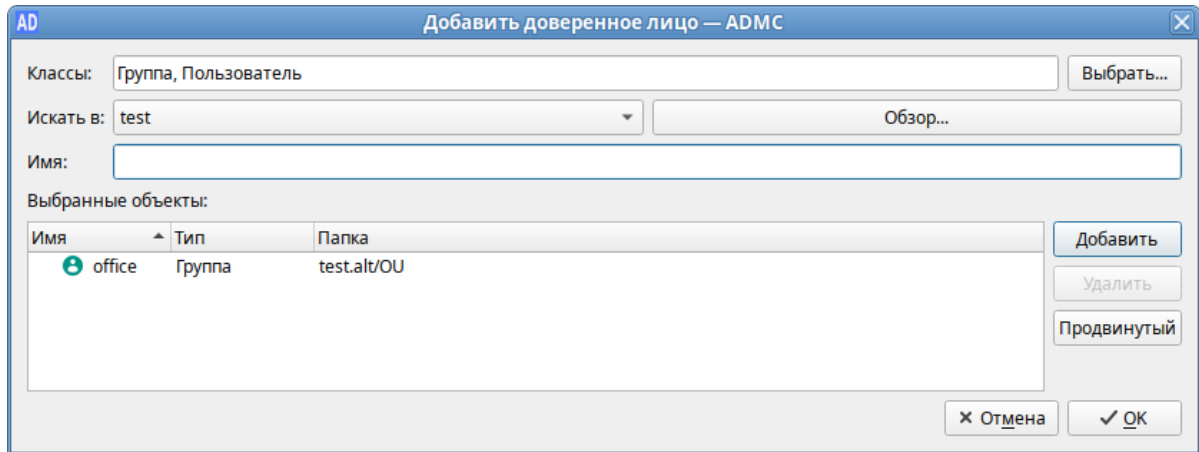


Рис. 325 – Добавление доверенного лица

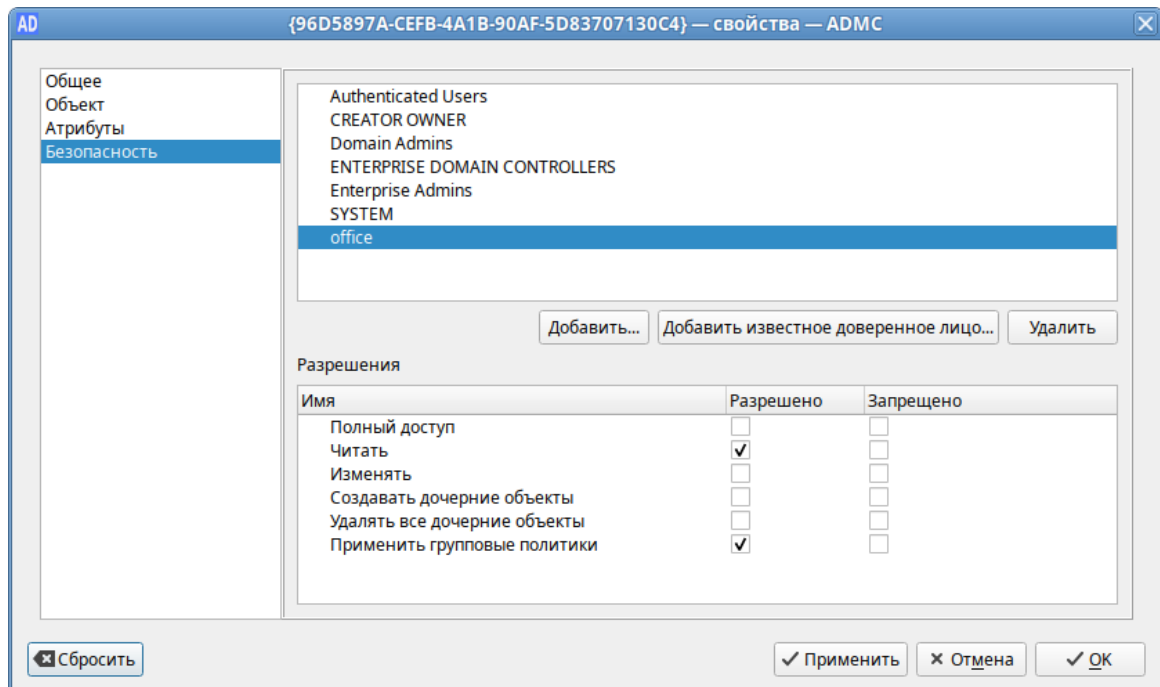


Рис. 326 – Разрешение на применение групповой политики

Чтобы определенному объекту запретить применение групповой политики, следует выполнить следующие действия:

- 1) в контекстном меню групповой политики выбрать пункт «Свойства» (см. рис. 323);
- 2) на вкладке «Безопасность» у группы «Authenticated Users» оставить разрешение на применение групповых политик (не снимать отметку с пункта «Применить групповые политики» в столбце «Разрешено») (рис. 327);

- 3) добавить объект, к которому не будет применяться групповая политика. Для этого нажать «Добавить...» и выбрать необходимый объект (можно выбрать пользователя, компьютер или группу). В данном примере будет добавлен компьютер «EDU» (рис. 328);
- 4) для добавленного объекта установить запрет применения групповых политик (установить отметку в пункте «Применить групповые политики» в столбце «Запрещено») и нажать кнопку «Применить» (рис. 329).

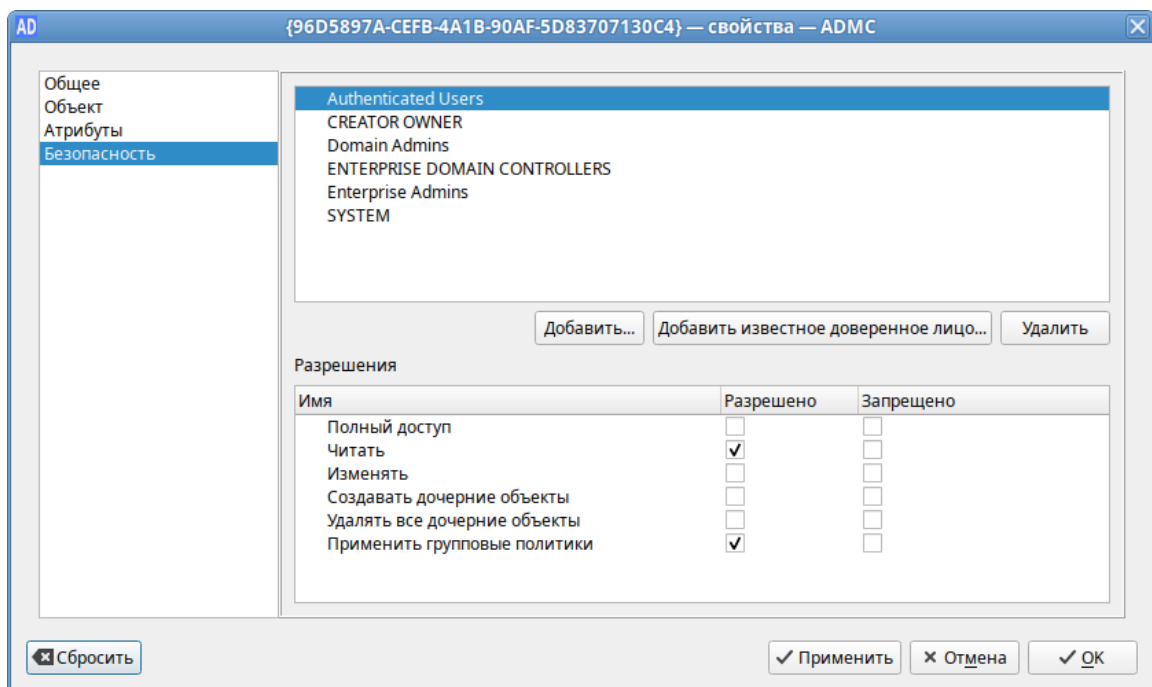


Рис. 327 – Вкладка «Безопасность» свойства групповой политики

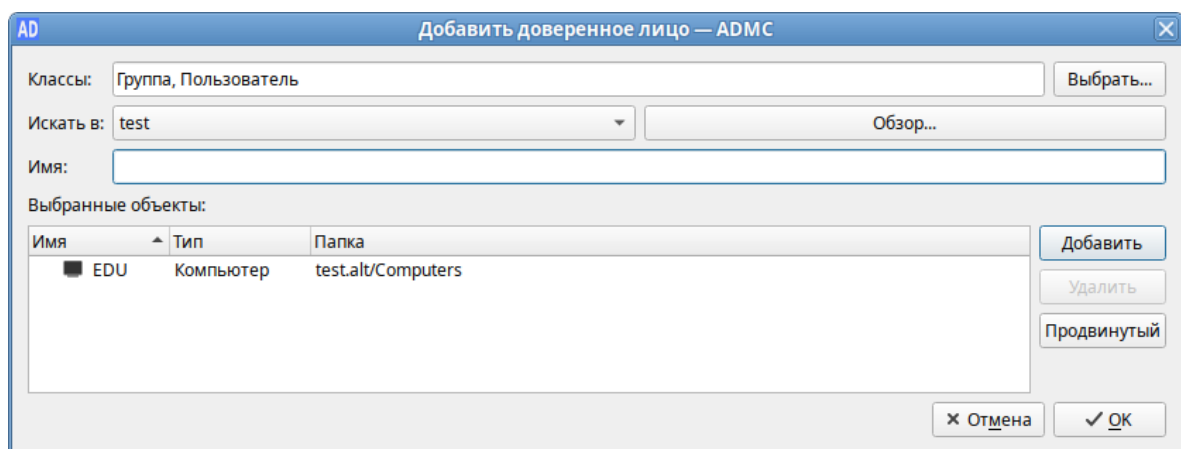


Рис. 328 – Добавить компьютер как доверенное лицо

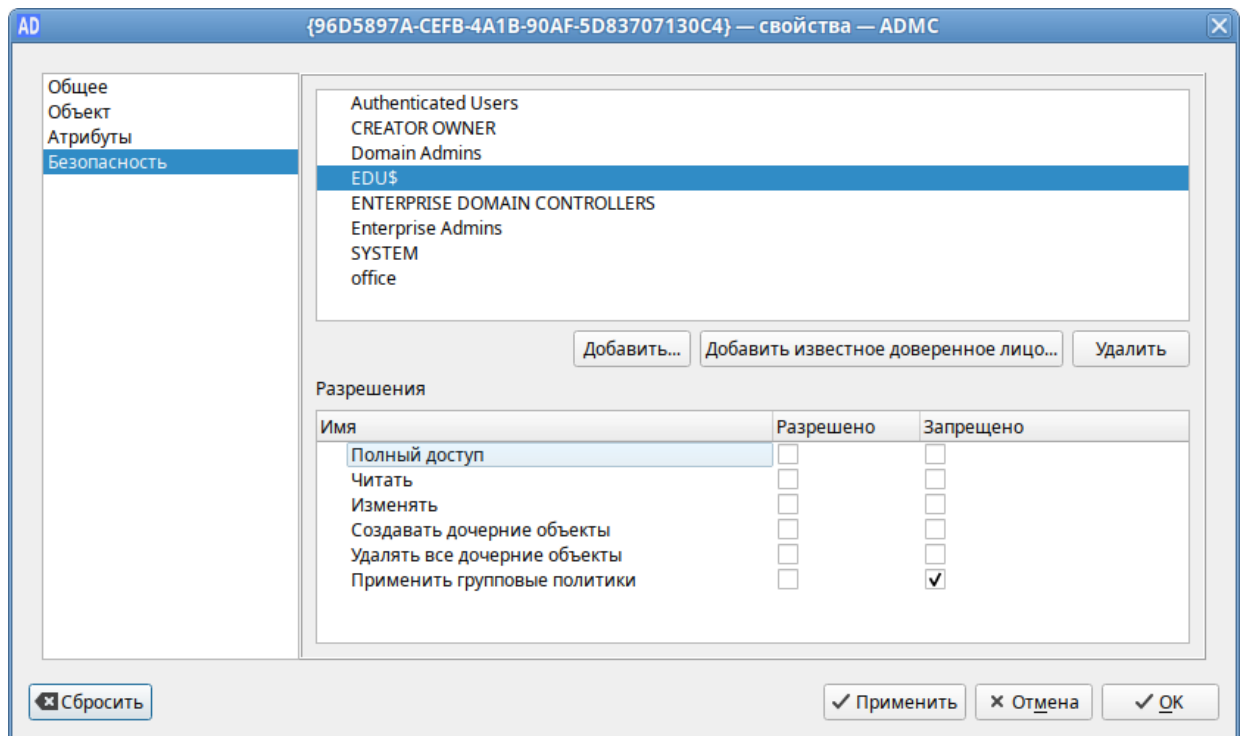


Рис. 329 – Запрет на применение групповых политик

10.4.5.13. Добавление/Удаление UPN суффиксов

UserPrincipalName (UPN) – имя для входа пользователя в формате email-адреса, например, ivanov@test.alt. Здесь ivanov это UPN-префикс (имя пользователя в «Альт Домен»), test.alt – UPN-суффикс. По умолчанию в «Альт Домен» в качестве UPN-суффикса используется DNS имя домена. Добавление дополнительных имен доменов позволяет упростить процесс входа и повысить безопасность.

Для того чтобы добавить/удалить дополнительный UPN-суффикс, нужно выполнить следующие шаги:

- 1) в контекстном меню домена выбрать пункт «Изменить суффиксы UPN» (рис. 330);
- 2) в открывшемся диалоговом окне нажать кнопку «Добавить...» (рис. 331);

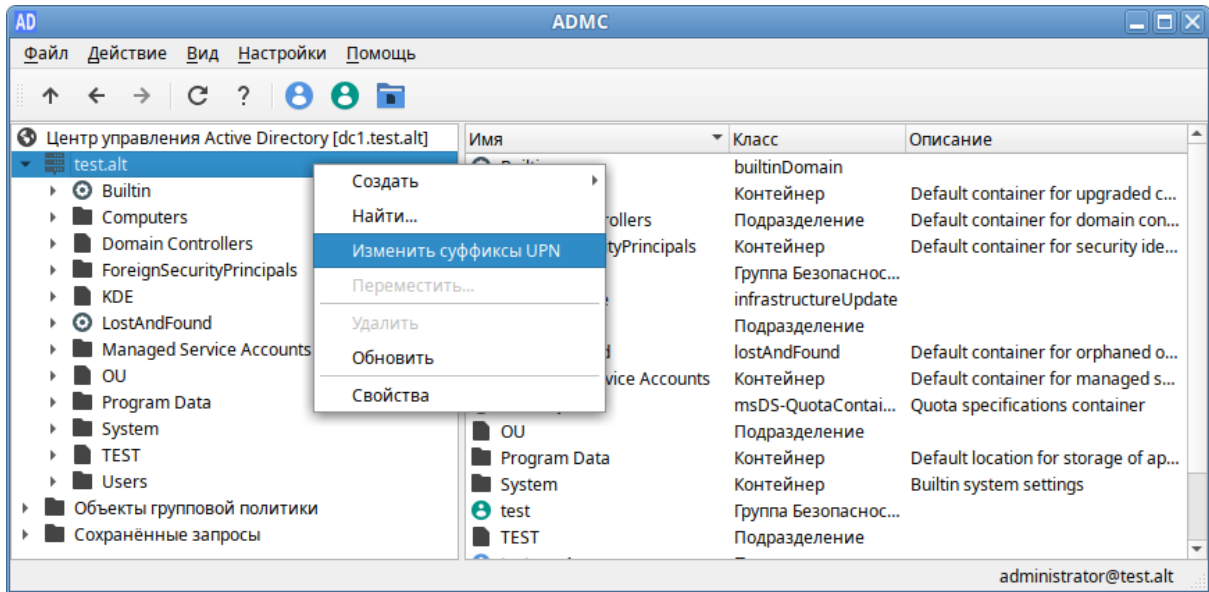


Рис. 330 – Пункт «Изменить суффиксы UPN»

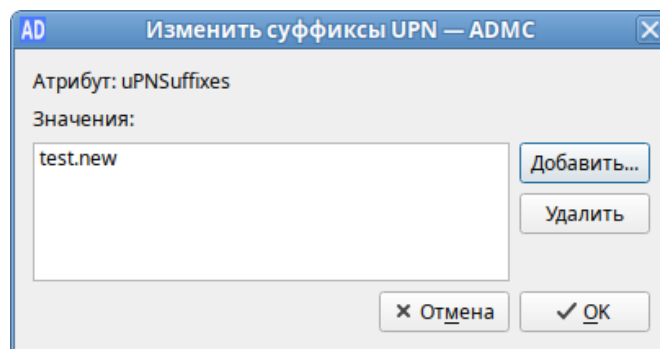


Рис. 331 – Кнопка «Добавить...»

- 3) ввести альтернативный суффикс (рис. 332). Не требуется, чтобы суффикс UPN был действительным DNS-именем домена. Суффиксы UPN должны соответствовать условиям DNS-имен в отношении допустимых символов и синтаксиса;
- 4) нажать кнопку «ОК», чтобы добавить новый суффикс в список.

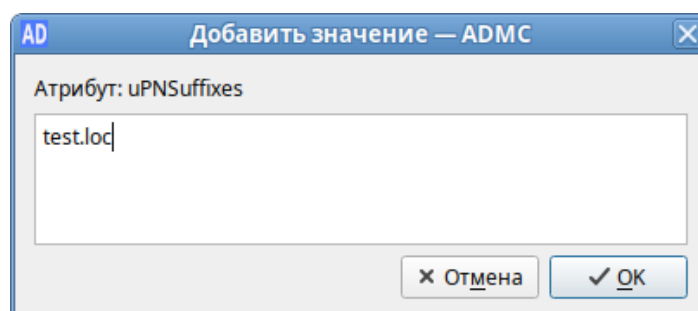


Рис. 332 – Введение альтернативного суффикса

Чтобы удалить существующий суффикс, нужно выбрать его в списке и нажать кнопку «Удалить» (рис. 333).

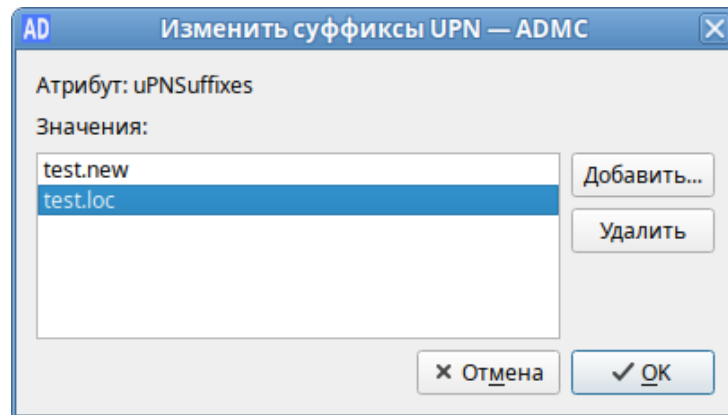


Рис. 333 – Удаление существующего суффикса

10.4.5.14. Роли FSMO

FSMO, или Flexible single-master operations (операции с одним исполнителем) – это операции, выполняемые контроллерами домена AD, которые требуют обязательной уникальности сервера для каждой операции. В зависимости от типа операции уникальность FSMO подразумевается в пределах одного домена или леса доменов. Различные типы FSMO могут выполняться как на одном, так и на нескольких контроллерах домена. Выполнение FSMO сервером называют ролью сервера, а сами сервера – хозяевами операций.

Для просмотра текущего владельца роли нужно выбрать пункт меню «Файл» → «Мастера Операций». В открывшемся окне в списке слева выбрать роль и в поле «Текущий мастер» будет показан владелец роли (рис. 334).

Список возможных ролей:

- «DNS домена» – Domain DNS Zone Master role;
- «DNS леса» – Forest DNS Zone Master role;
- «PDC эмуляция» – эмулятор PDC (PDC Emulator);
- «Схема» – хозяин схемы (Schema Master);
- «Имена домена» – хозяин именования доменов (Domain Naming Master);
- «Инфраструктура» – хозяин инфраструктуры (Infrastructure Master);
- «RID распределение» – хозяин RID (RID Master).

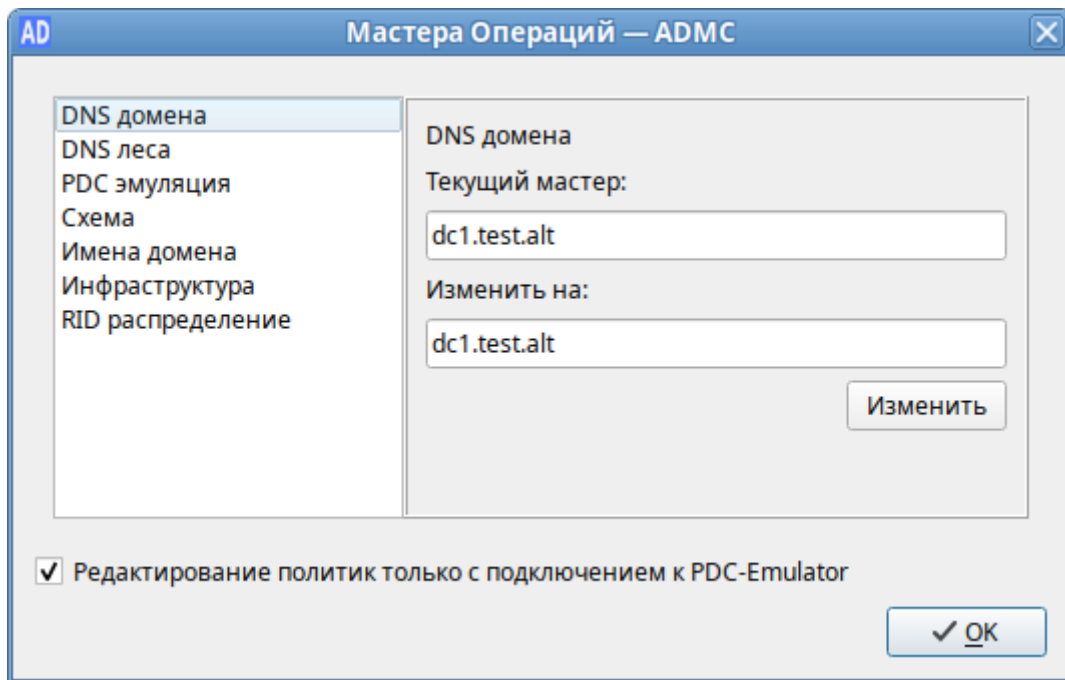


Рис. 334 – Просмотр текущего владельца роли

Если отмечен пункт «Редактирование политик только с подключением к PDC-Emulator», при отсутствии подключения к контроллеру домена с ролью PDC-эмуляции, действия, затрагивающие шаблоны групповых политик (редактирование/изменение/удаление политик) будут запрещены, появится сообщение, показанное на рис. 335.

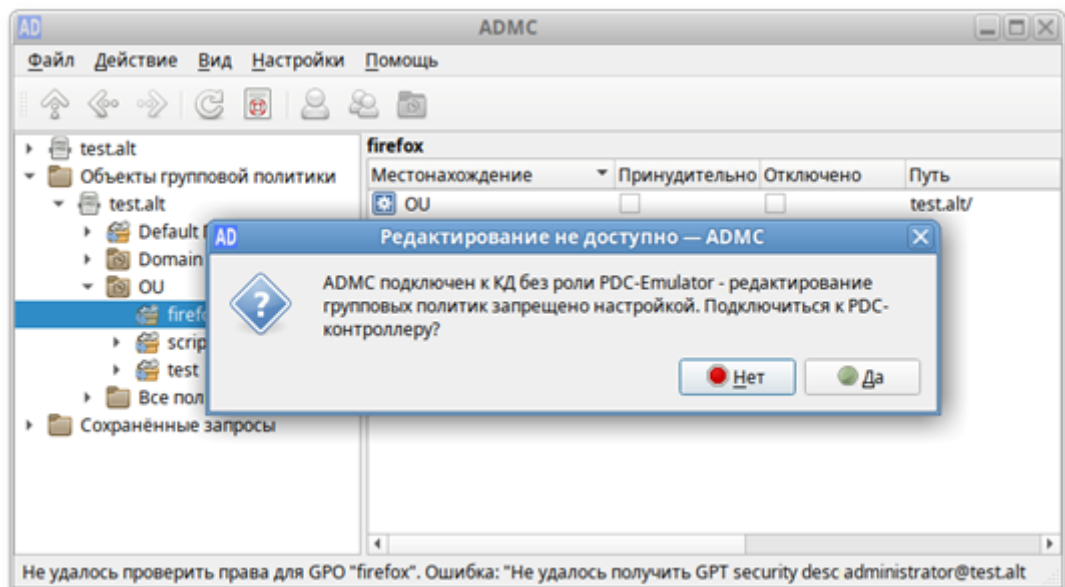


Рис. 335 – Окно «Редактирование не доступно»

Для штатной передачи роли нужно выполнить следующие действия:

- 1) в окне «Параметры подключения – ADMS» («Файл» → «Параметры подключения») выбрать контроллер домена, который должен стать новым владельцем роли, и нажать кнопку «ОК» (рис. 336);

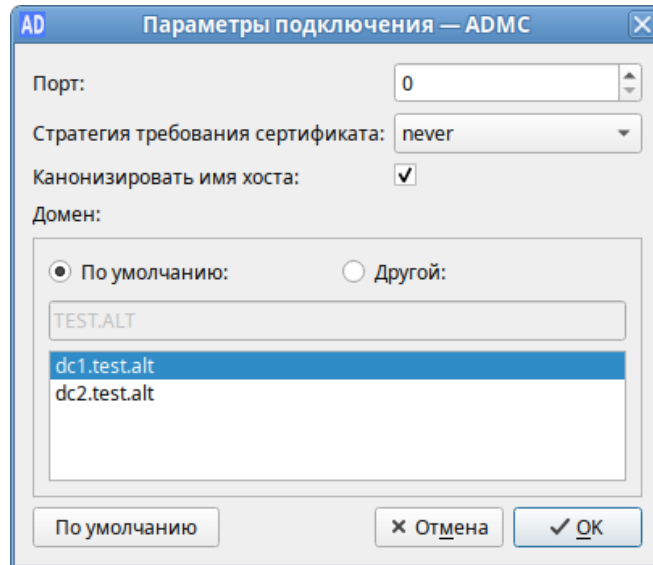


Рис. 336 – Окно «Параметры подключения – ADMS»

- 2) в окне «Мастера Операций – ADMS» («Файл» → «Мастера Операций») выбрать роль (при этом в поле «Текущий мастер» будет показан текущий владелец роли, а в поле «Изменить на» – контроллер домена, который должен стать новым владельцем роли) и нажать кнопку «Изменить» (рис. 337);

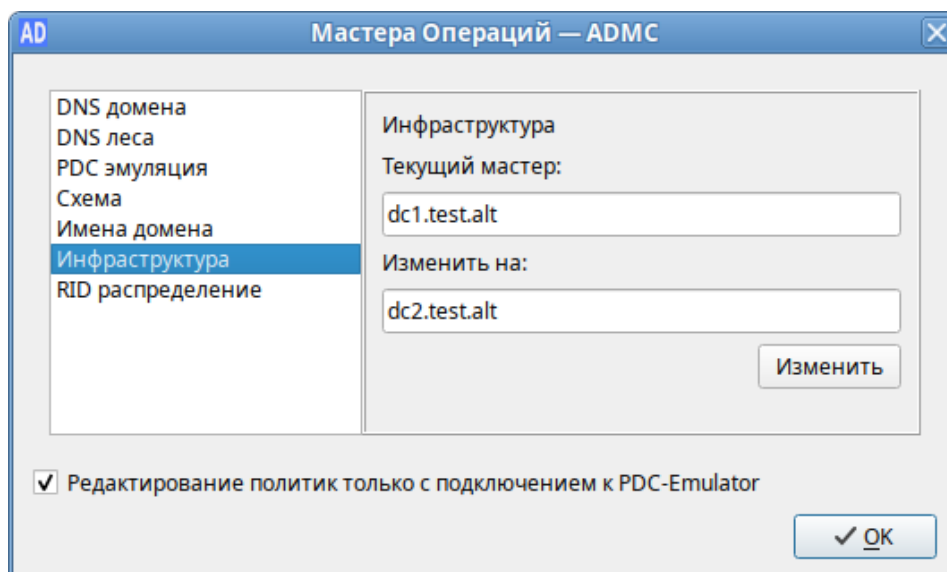


Рис. 337 – Передача роли на новый DC

3) владелец роли будет изменен (рис. 338).

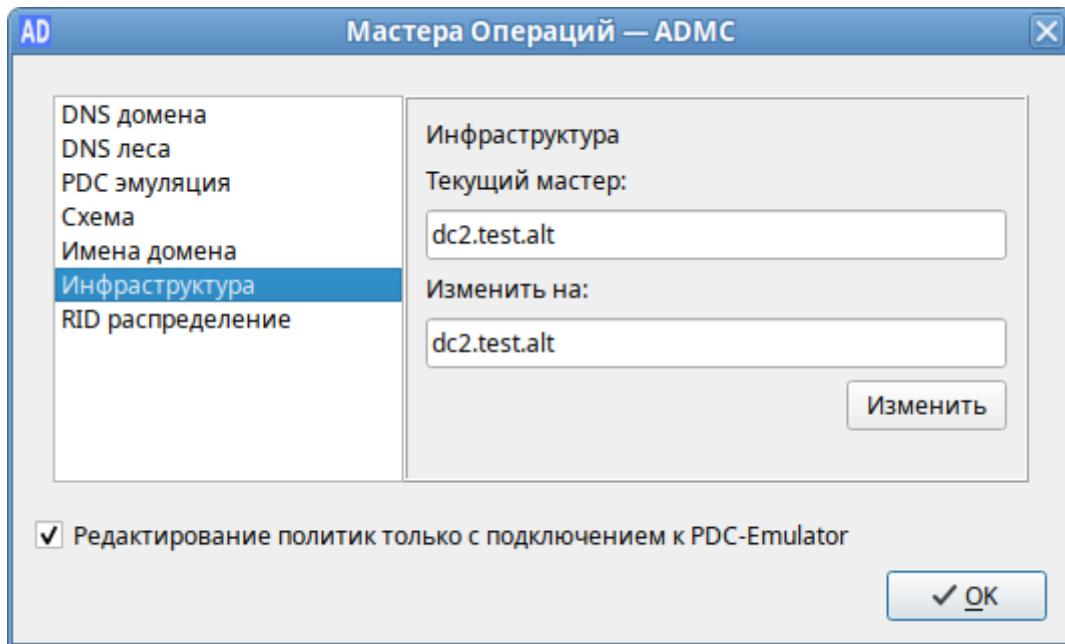


Рис. 338 – Новый владелец роли

10.4.5.15. Выбор объектов

Выбор объектов осуществляется в диалоговом окне «Выбрать объекты – ADMS» (рис. 339). Доступ к этому диалоговому окну можно получить из разных мест, например, при выборе действия «Добавить в группу...» в контекстном меню учетной записи пользователя.

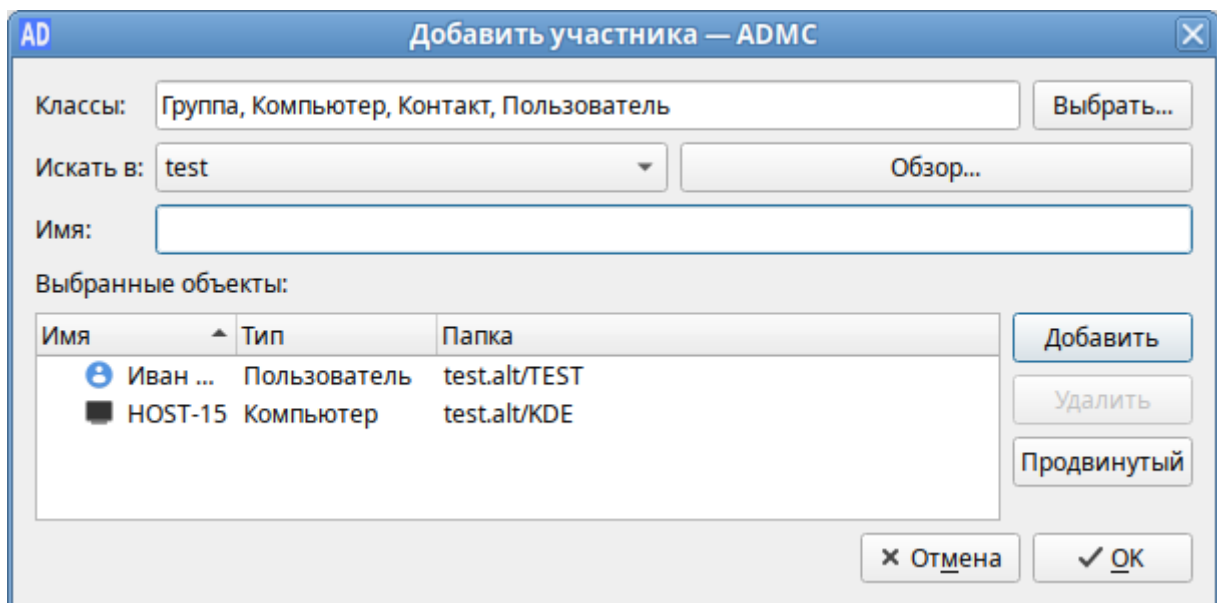


Рис. 339 – Диалоговое окно выбора объектов

Для выбора объекта достаточно указать класс объекта, выбрать расположение, с которого требуется начать поиск, и в поле «Имя» ввести имена объектов:

- 1) в поле «Классы», нажав кнопку «Выбрать...», выбрать типы объектов, которые будут использоваться для поиска (в большинстве случаев это поле будет заполнено автоматически, в зависимости от контекста задачи);
- 2) в поле «Искать в» выбрать объект, который будет использоваться в качестве основы для поиска;
- 3) в поле «Имя» ввести имя объекта (можно ввести часть имени или выполнить поиск по имени для входа);
- 4) нажать кнопку «Добавить» для поиска объекта по названию;
- 5) если объект найден, он будет добавлен в список найденных объектов;
- 6) если объект не найден, исправить имя и повторить попытку;
- 7) если есть несколько совпадений, откроется диалоговое окно, в котором можно выбрать одно или несколько совпадений (рис. 340);

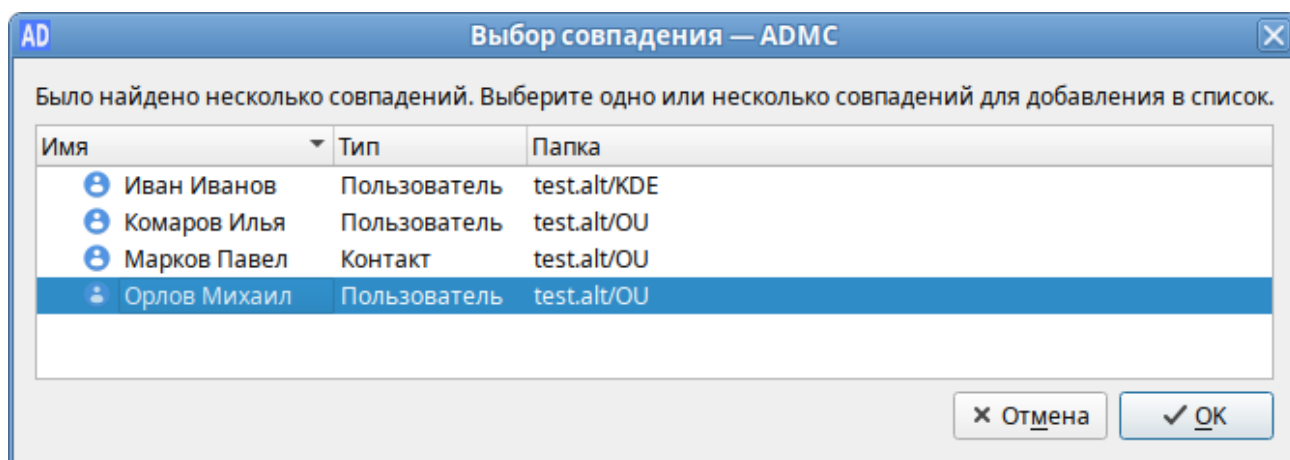


Рис. 340 – Выбор объектов из списка совпадений

- 8) повторить пункты 1) – 7), пока не будут добавлены все объекты;
- 9) чтобы удалить объект из списка, нужно выбрать объект и нажать кнопку «Удалить».

Для выбора объектов можно также использовать продвинутый поиск, который можно открыть, нажав кнопку «Продвинутый».

10.4.5.16. Поиск объектов

Поиск объектов осуществляется в диалоговом окне «Поиск объектов – ADMS» (рис. 341). Доступ к этому диалоговому окну можно получить, выбрав пункт «Найти...» в меню «Действие» или в контекстном меню контейнера.

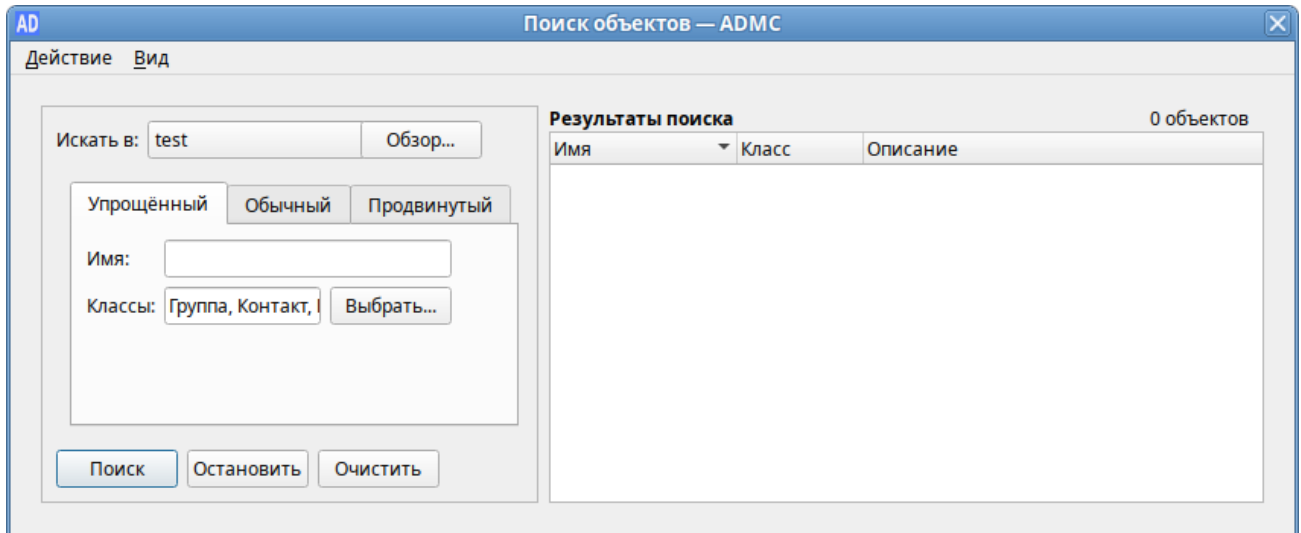


Рис. 341 – Поиск объектов

Поиск объектов в домене возможен по разным критериям:

- по типу и имени (простой поиск) – вкладка «Упрощенный»;
- по атрибутам – вкладка «Обычный»;
- в синтаксисе запросов LDAP – вкладка «Продвинутый».

Примечание. В диалоговом окне, вызываемом меню «Вид» → «Настроить колонки», можно выбрать поля, которые будут отображаться в списке результатов поиска (рис. 342).

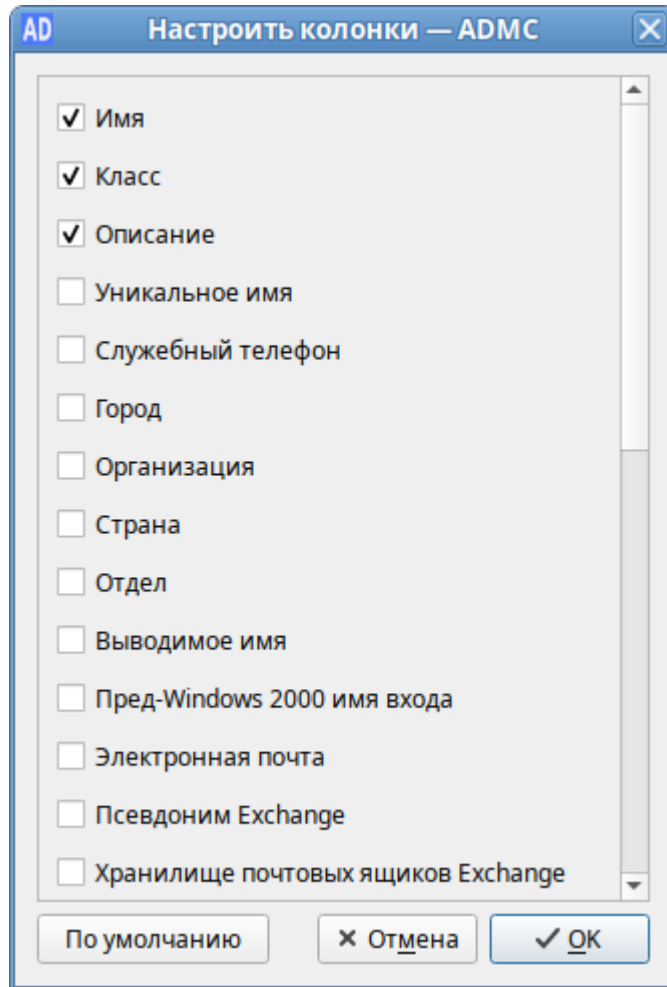


Рис. 342 – Поля, отображаемые в результатах

10.4.5.16.1. Простой поиск

Процедура простого поиска:

- 1) в диалоговом окне «Поиск объектов – ADMS» выбрать вкладку «Упрощенный» (см. рис. 341);
- 2) в поле «Классы», нажав кнопку «Выбрать...», выбрать классы объектов для поиска (рис. 343);

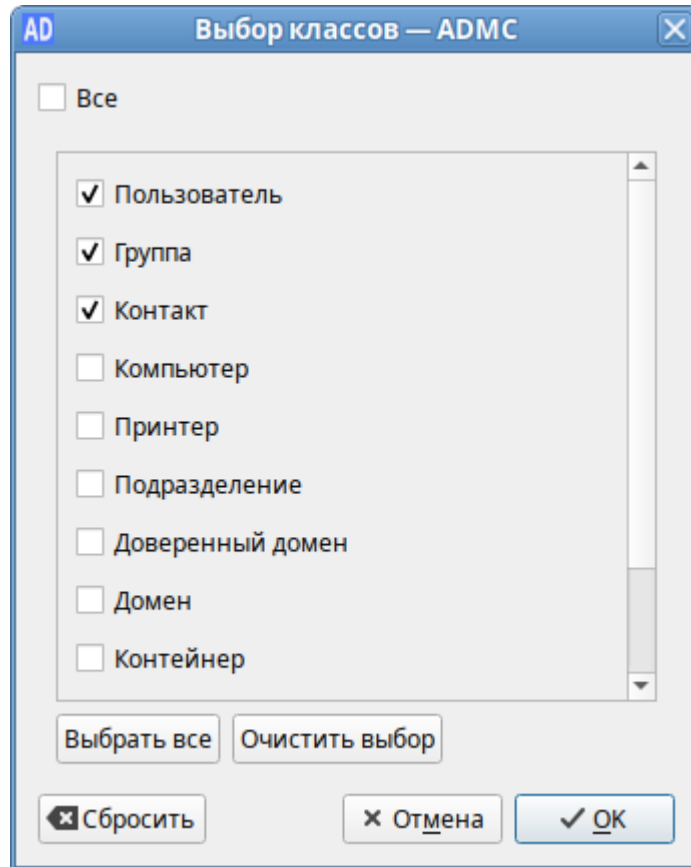


Рис. 343 – Выбор классов объектов для поиска

3) в поле «Имя» ввести имя объекта и нажать кнопку «Поиск» (рис. 344).

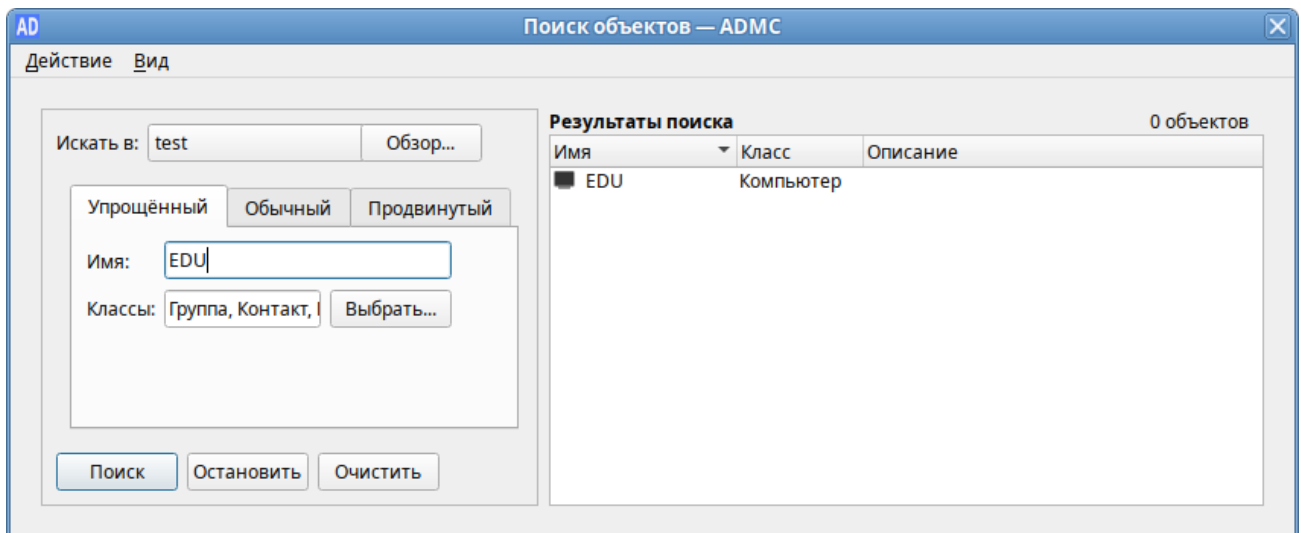


Рис. 344 – Простой поиск

10.4.5.16.2. Обычный поиск

При использовании обычного поиска создаются фильтры, определяющие критерии поиска:

- 1) в диалоговом окне «Поиск объектов – АDMC» (см. рис. 341) выбрать вкладку «Обычный»;
- 2) в поле «Классы», нажав кнопку «Выбрать...», выбрать классы объектов для поиска (рис. 343);
- 3) создать фильтр:
 - в списке «Класс атрибута» выбрать класс атрибута;
 - в списке «Атрибут» выбрать атрибут (список атрибутов зависит от выбранного класса атрибутов);
 - в списке «Состояние» выбрать условие, которое будет использоваться для фильтра;
 - в поле «Значение» ввести значение условия (не для всех условий нужно вводить значения);
- 4) нажать кнопку «Добавить»;
- 5) повторить пункты 2) – 3), чтобы добавить больше фильтров (фильтры для создания критериев поиска объединяются логическим И);
- 6) нажать кнопку «Удалить», если нужно удалить фильтр из списка;
- 7) нажать кнопку «Очистить», если нужно очистить список фильтров;
- 8) нажать кнопку «Поиск» (рис. 345).

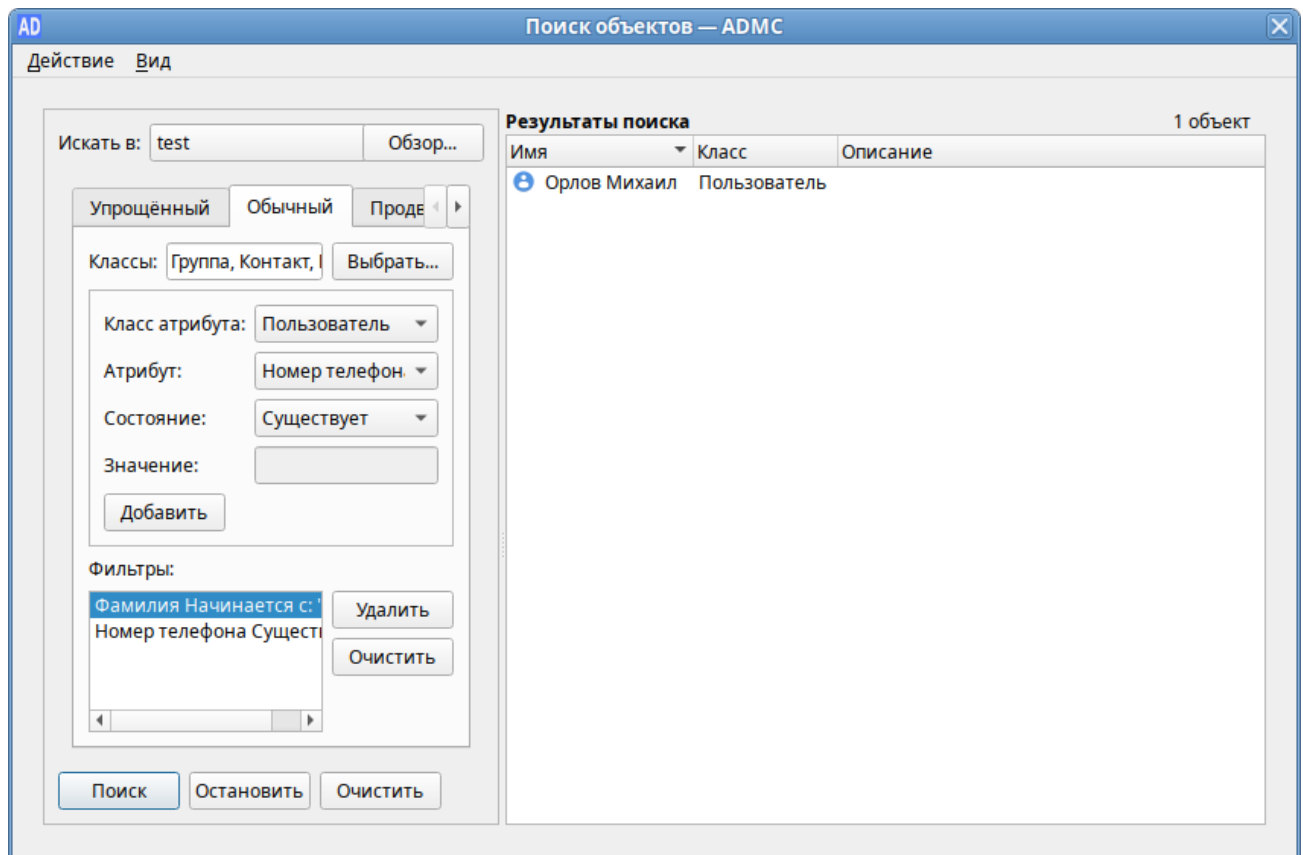


Рис. 345 – Обычный поиск

10.4.5.16.3. Продвинутый поиск

Продвинутый поиск предполагает использование LDAP-фильтров.

Использование LDAP-фильтров является наиболее эффективным способом поиска объектов в «Альт Домен».

Синтаксис LDAP-фильтра имеет вид:

<Фильтр>= (<Атрибут><оператор сравнения><значение>)

При наличии нескольких условий поиска фильтры можно комбинировать с помощью логических операторов.

Процедура продвинутого поиска:

- 1) в диалоговом окне «Поиск объектов – ADMS» (см. рис. 341) выбрать вкладку «Продвинутый»;
- 2) в поле «Искать в» выбрать область поиска (можно воспользоваться кнопкой «Обзор»);
- 3) ввести LDAP-фильтр в поле «Введите фильтр LDAP»;
- 4) нажать кнопку «Поиск» (рис. 346).

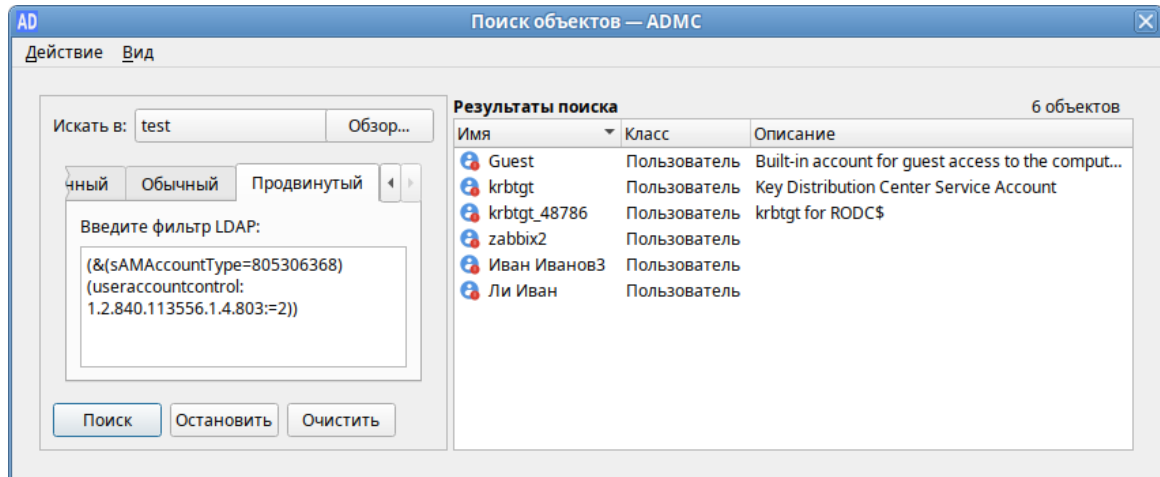


Рис. 346 – Продвинутый поиск

10.4.5.17. Использование сохраненных результатов поиска

Сохранение запросов (результатов поиска) – это удобный способ сохранять и воспроизводить поиск. Сохраненные запросы позволяют создавать различные LDAP-фильтры для выборки объектов домена. С помощью сохраненных запросов можно быстро и эффективно решать задачи поиска и выборки объектов по различным критериям.

При использовании сохраненных запросов администратор может выполнять групповые операции с объектами из разных OU домена. Например, можно выполнить массовую блокировку/разблокировку, удаление учетных записей, переименование.

Сохраненные запросы можно организовать в древовидную структуру (рис. 347).

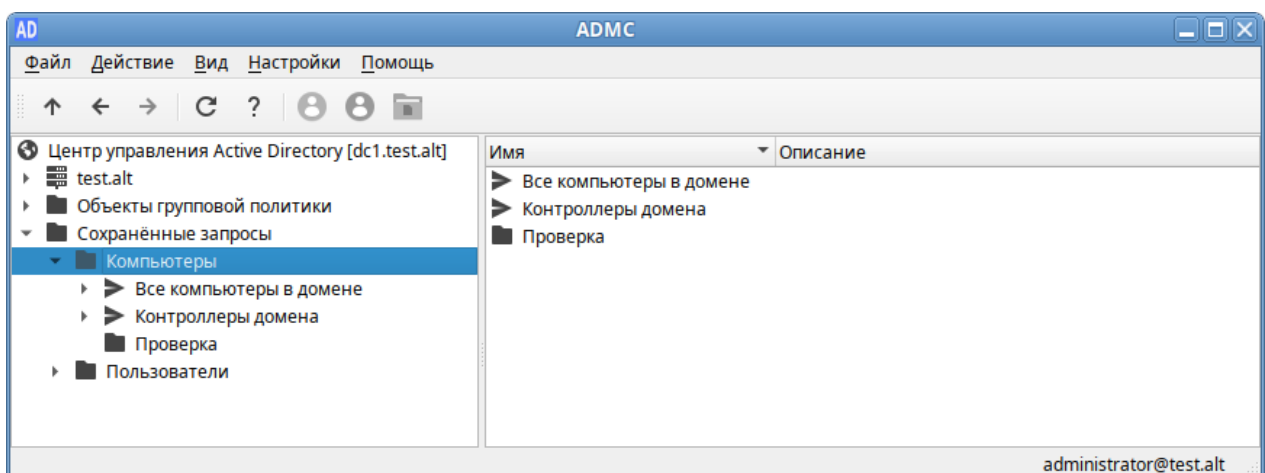


Рис. 347 – Структура сохраненных запросов

Создание папки запросов:

- 1) в контекстном меню папки «Сохраненные запросы» или ее подпапки выбрать пункт «Создать» → «Папка запросов» (рис. 348);

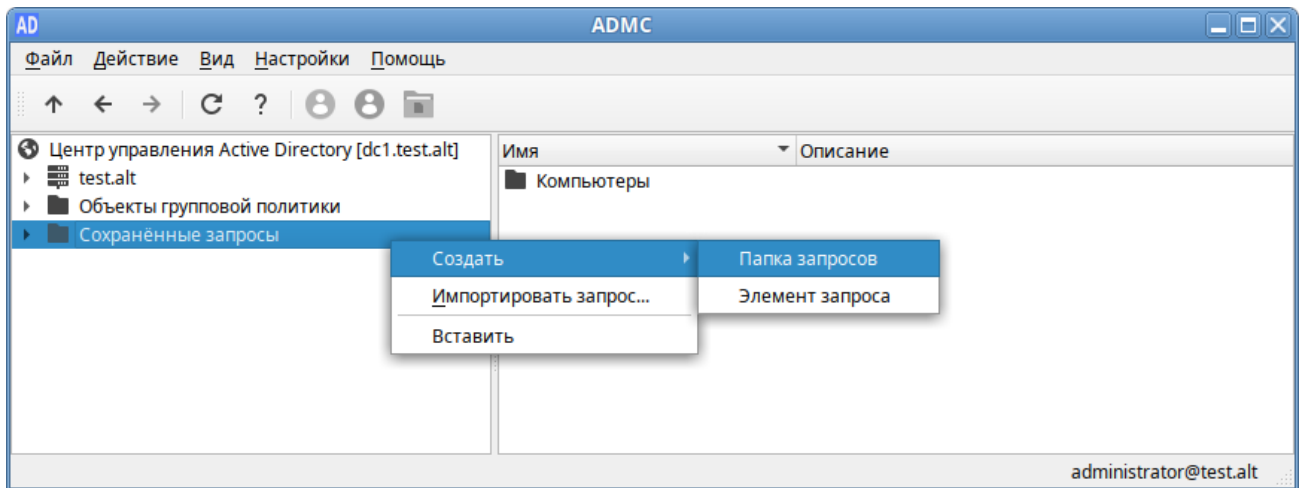


Рис. 348 – Контекстное меню папки «Сохраненные запросы»

- 2) в диалоговом окне «Создать папку запросов – ADMC» в поле «Имя» вести название папки, в поле «Описание» можно добавить описание папки (рис. 349);
- 3) нажать кнопку «ОК».

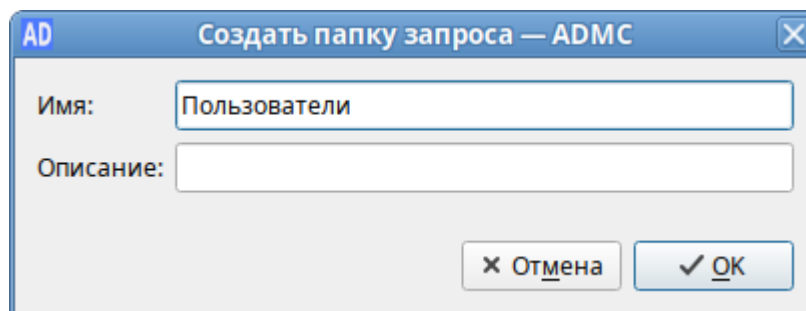


Рис. 349 – Создание папки запросов

Создание запроса:

- 1) в контекстном меню папки запроса выбрать пункт «Создать» → «Элемент запроса» (рис. 350);

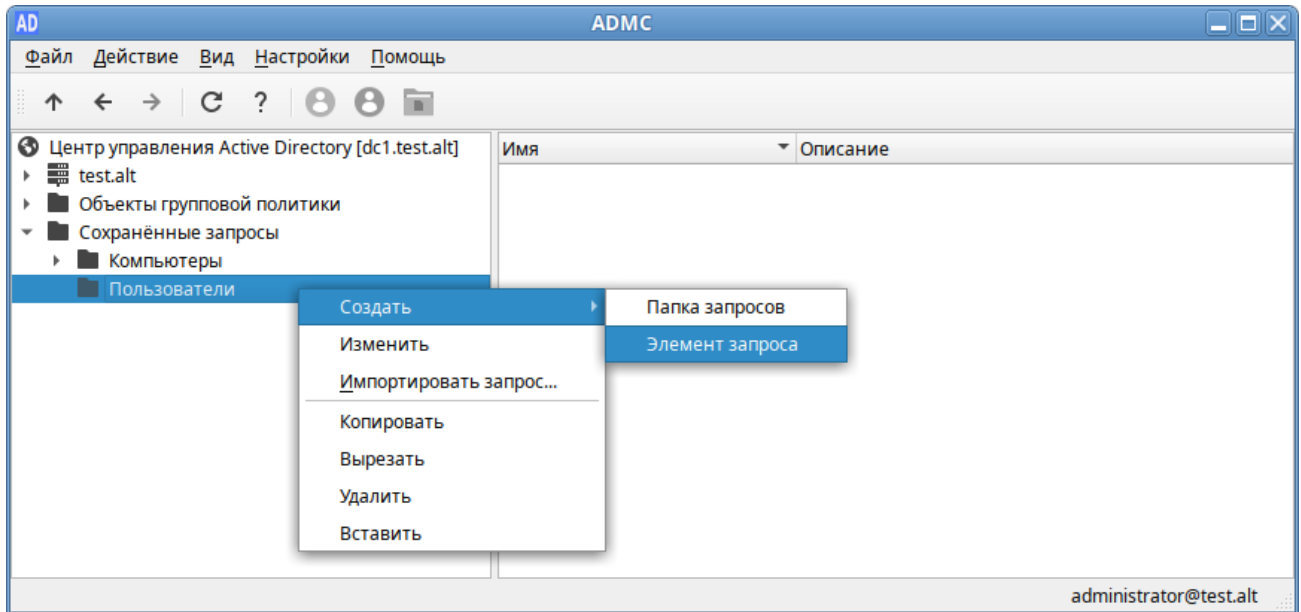


Рис. 350 – Контекстное меню папки запроса

2) в диалоговом окне создания запроса указать:

- «Имя» – название запроса;
- «Описание» – описание запроса;
- «Искать в» – объект, который будет использоваться в качестве основы для поиска. По умолчанию поиск выполняется по всему домену. Сузить область поиска можно, нажав кнопку «Обзор» и выбрав контейнер;
- «Рекурсивный поиск» – поиск должен включать объекты более чем одного уровня (рис. 351);

3) нажать кнопку «Изменить фильтр», чтобы создать фильтр поиска (для получения информации о том, как создавать фильтры, см. п. 10.4.5.16);

4) после создания фильтра он будет отображаться в поле «Фильтр» (в формате LDAP);

5) нажать кнопку «ОК».

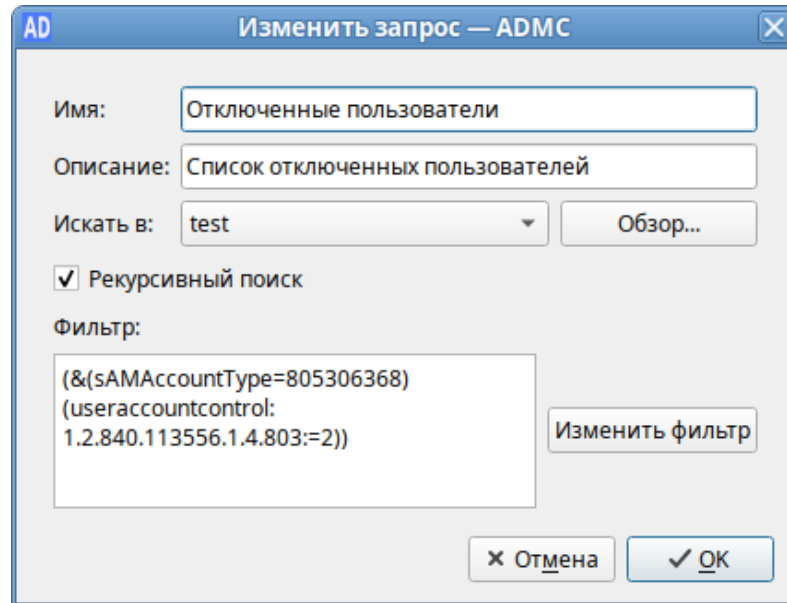


Рис. 351 – Диалоговое окно создания запроса

При выборе сохраненного запроса, в правом окне появится список объектов, который соответствует данному запросу (рис. 352).

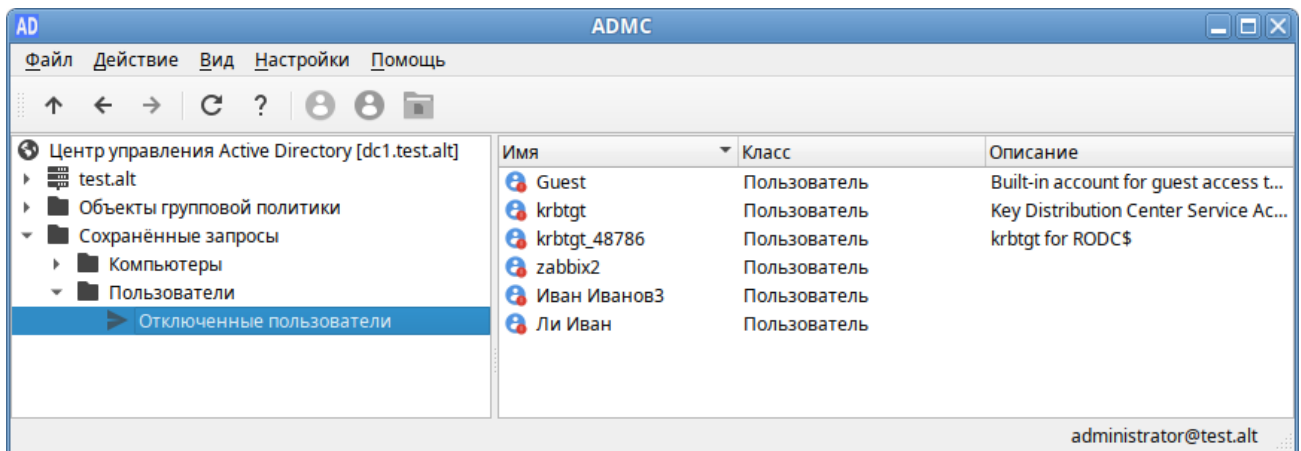


Рис. 352 – Результат выполнения запроса

В ADMS существует возможность переноса поисковых запросов между компьютерами (экспорт и импорт поисковых запросов).

Экспорт запроса:

- 1) в контекстном меню запроса выбрать пункт «Экспортировать запрос...»;
- 2) в открывшемся диалоговом окне указать название файла (<имя_файла>.json) и место назначения;
- 3) нажать кнопку «Сохранить».

Импорт запроса:

- 1) в контекстном меню папки, в которую будет импортирован запрос, выбрать пункт «Импортировать запрос...» (рис. 353);
- 2) в открывшемся диалоговом окне выбрать экспортированный файл поиска;
- 3) нажать кнопку «Открыть».

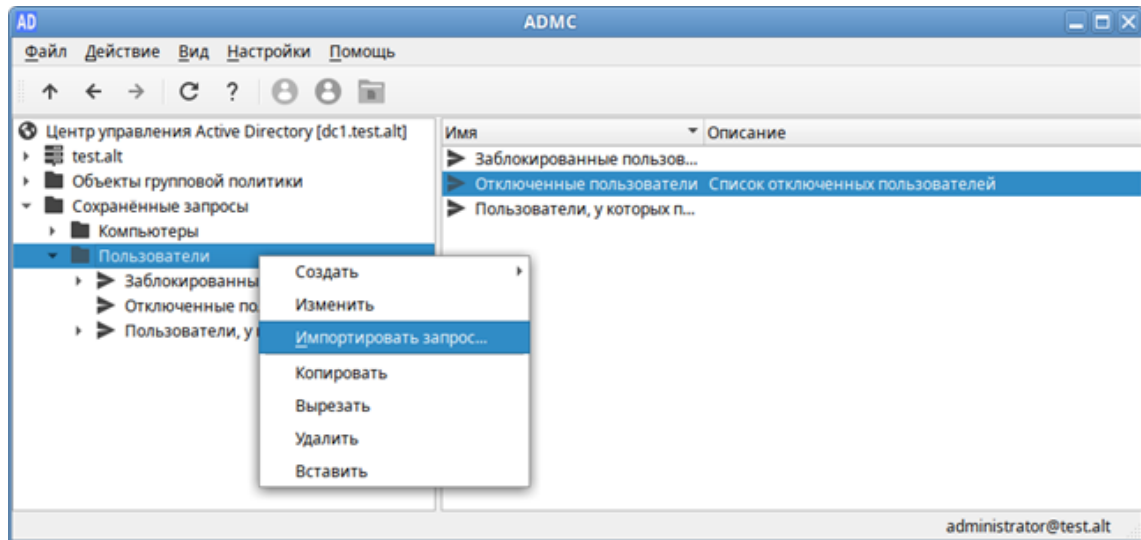


Рис. 353 – Импорт запроса

Для удаления запроса или папки запросов в контекстном меню объекта выбрать пункт «Удалить».

10.4.6. Модуль редактирования настроек клиентской конфигурации (GPUI)

Модуль редактирования настроек клиентской конфигурации (далее – GPUI) предназначен для настройки и изменения параметров групповой политики в объектах групповой политики, которые могут ссылаться на организационные подразделения в домене.

GPUI предоставляет администраторам иерархическую древовидную структуру для настройки параметров групповой политики в объектах групповой политики. Эти объекты групповой политики могут быть связаны с организационными единицами (OU), содержащими компьютерные или пользовательские объекты. Связать объекты групповой политики с OU можно в модуле ADMC.

GPUI состоит из двух основных разделов: конфигурация компьютера и конфигурация пользователя. Раздел конфигурация компьютера содержит параметры

всех политик, определяющих работу компьютера. Групповая политика применяется к компьютеру на этапе загрузки системы и в дальнейшем при выполнении циклов обновления. Раздел конфигурация пользователя содержит параметры всех политик, определяющих работу пользователя на компьютере. Групповая политика применяется к пользователю при его регистрации на компьютере и в дальнейшем при выполнении циклов обновления.

Каждая политика в объекте GPO может находиться в одном из трех состояний: «Включено», «Отключено», «Не сконфигурировано». В состоянии «Отключено» в настройках можно указать параметры политики. В состоянии «Не сконфигурировано» политика на объект не воздействует.

GPUИ является расширяемым инструментом. Самый простой способ для разработчиков расширить редактор объектов групповой политики для своих приложений – это написать файлы настраиваемых административных шаблонов, которые «подключаются» к редактору объектов групповой политики.

10.4.6.1. Запуск GPUИ для редактирования доменных политик

По умолчанию GPUИ не редактирует никаких политик. Для того чтобы редактировать политику, GPUИ нужно запустить либо из ADMS, выбрав в контекстном меню объекта групповой политики пункт «Изменить...» (рис. 354).

Те же действия можно произвести при помощи указания каталога групповой политики:

```
$ gpui-main -p "smb://dc1.test.alt/SysVol/test.alt/Policies/{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXXXXXXX}"
```

Ключ `-p` позволяет указать путь к шаблону групповой политики, который нужно редактировать, `dc1.test.alt` – имя контроллера домена, а `{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXXXXXXX}` – GUID шаблона групповой политики для редактирования. Можно указывать как каталоги `smb`, так и локальные каталоги.

Пример запуска GPUИ для редактирования политики:

```
$ gpui-main -p "smb://dc1.test.alt/SysVol/test.alt/Policies/{2E80AFBE-BBDE-408B-B7E8-AF79E02839D6}"
```

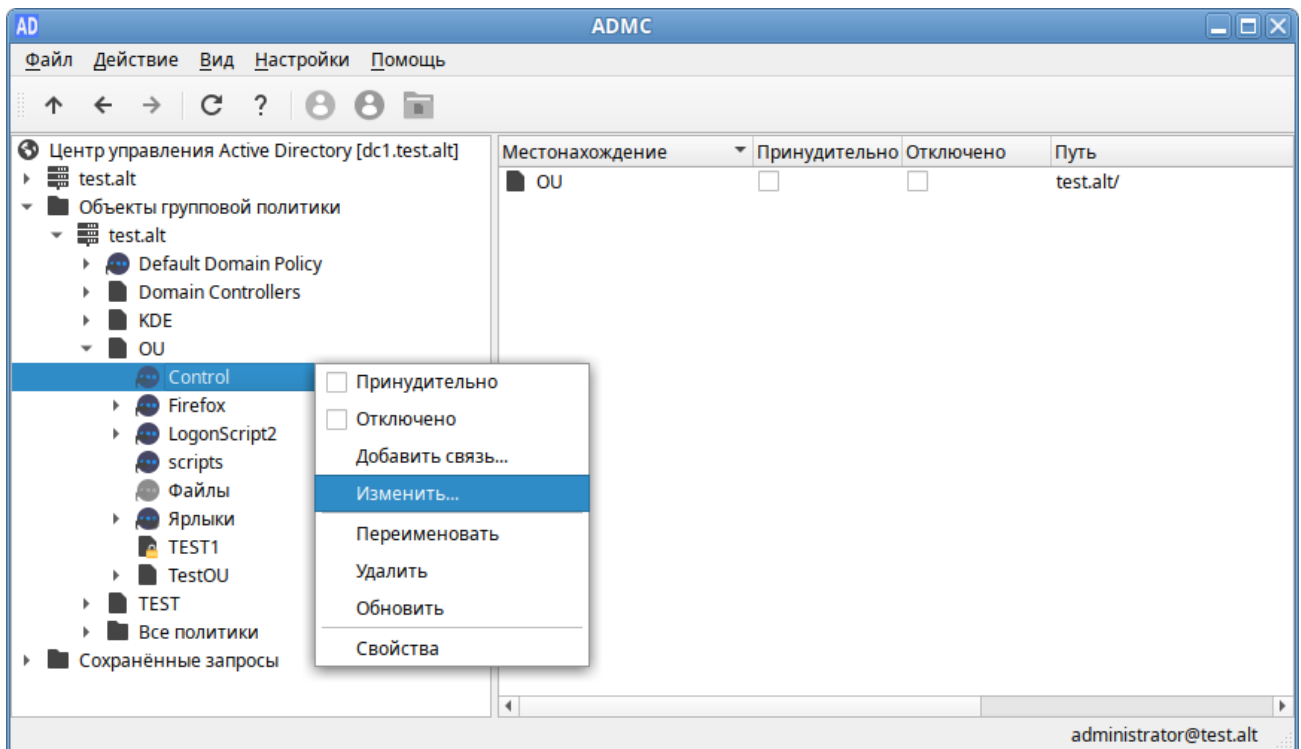


Рис. 354 – Запуск GPOUI из ADMC

Примечание. GUID шаблона групповой политики можно узнать в ADMC (это дочерний контейнер Policies контейнера System), в настройках должен быть отмечен пункт «Дополнительные возможности» (рис. 355).

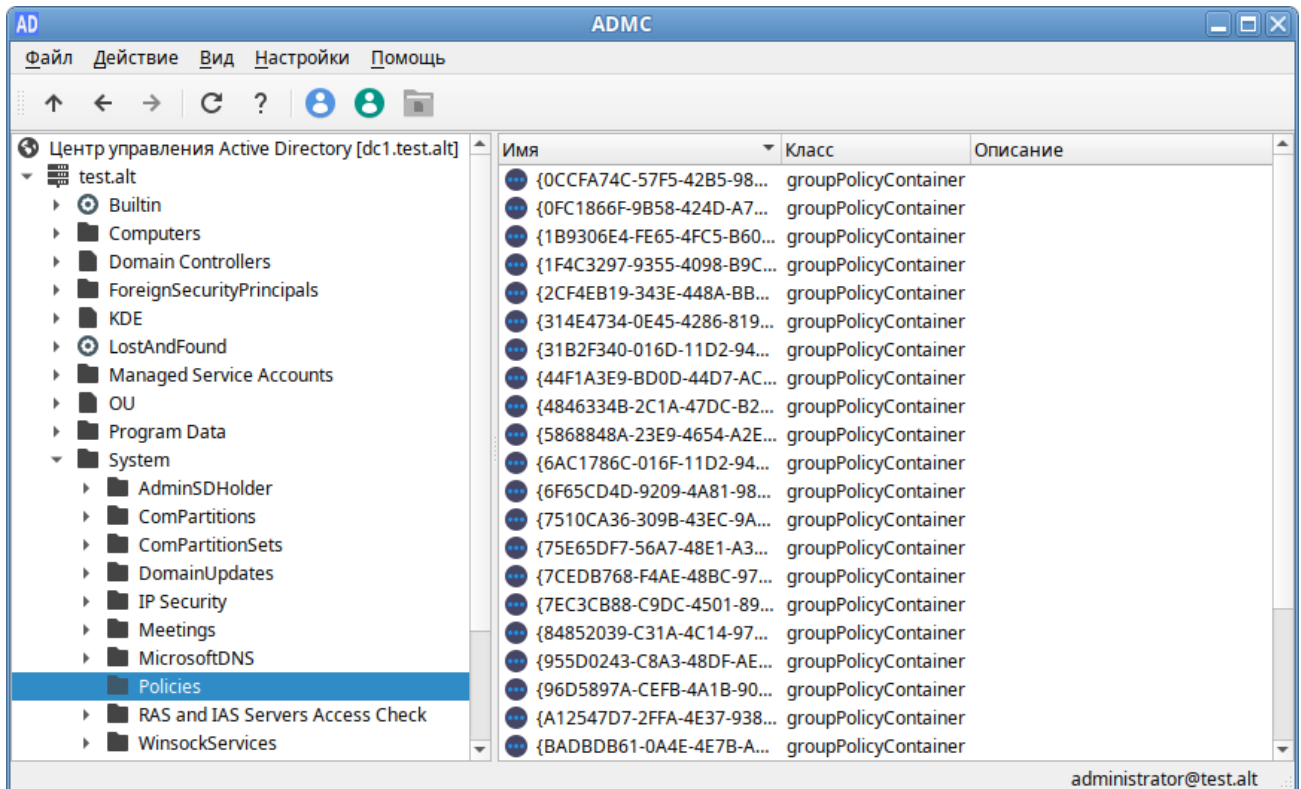


Рис. 355 – Контейнеры групповых политик

10.4.6.2. Выбор набора шаблонов групповых политик

По умолчанию GPUI загружает ADMX-файлы, содержащие описание шаблонов групповых политик, из каталога `/usr/share/PolicyDefinitions`.

Для того чтобы указать другой набор шаблонов групповых политик, GPUI можно запустить с ключом `-b`:

```
$ gpui-main -b "/usr/share/PolicyDefinitions"
```

Каталог шаблонов групповых политик можно также выбрать в графическом интерфейсе:

- 1) выбрать пункт меню «Файл» → «Открыть папку с ADMX файлами» (рис. 356);
- 2) открыть папку с шаблонами.

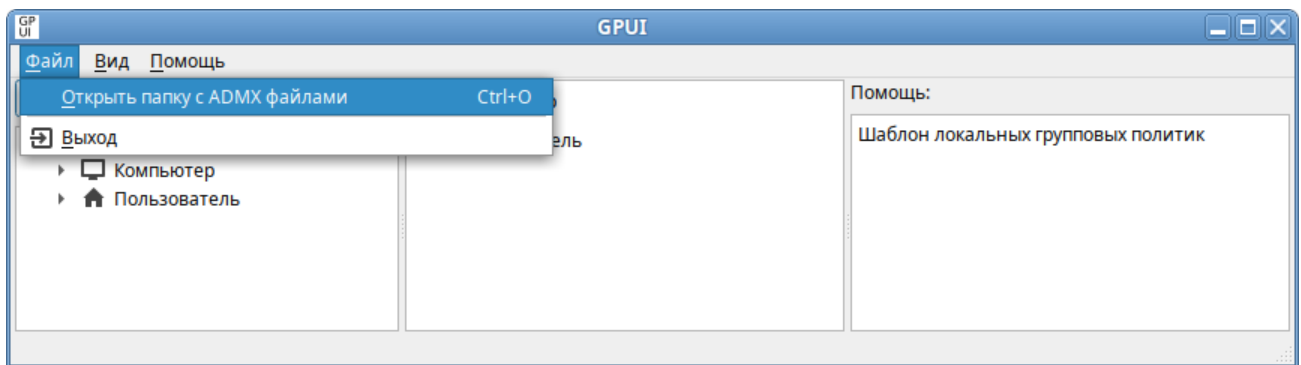


Рис. 356 – Подпункт «Открыть папку с ADMX файлами»

10.4.6.3. Интерфейс

Все настройки в GPUI разделены на два раздела:

- «Компьютер» («Machine») – раздел с настройками параметров компьютера;
- «Пользователь» («User») – раздел с настройками параметров пользователей домена (рис. 357).

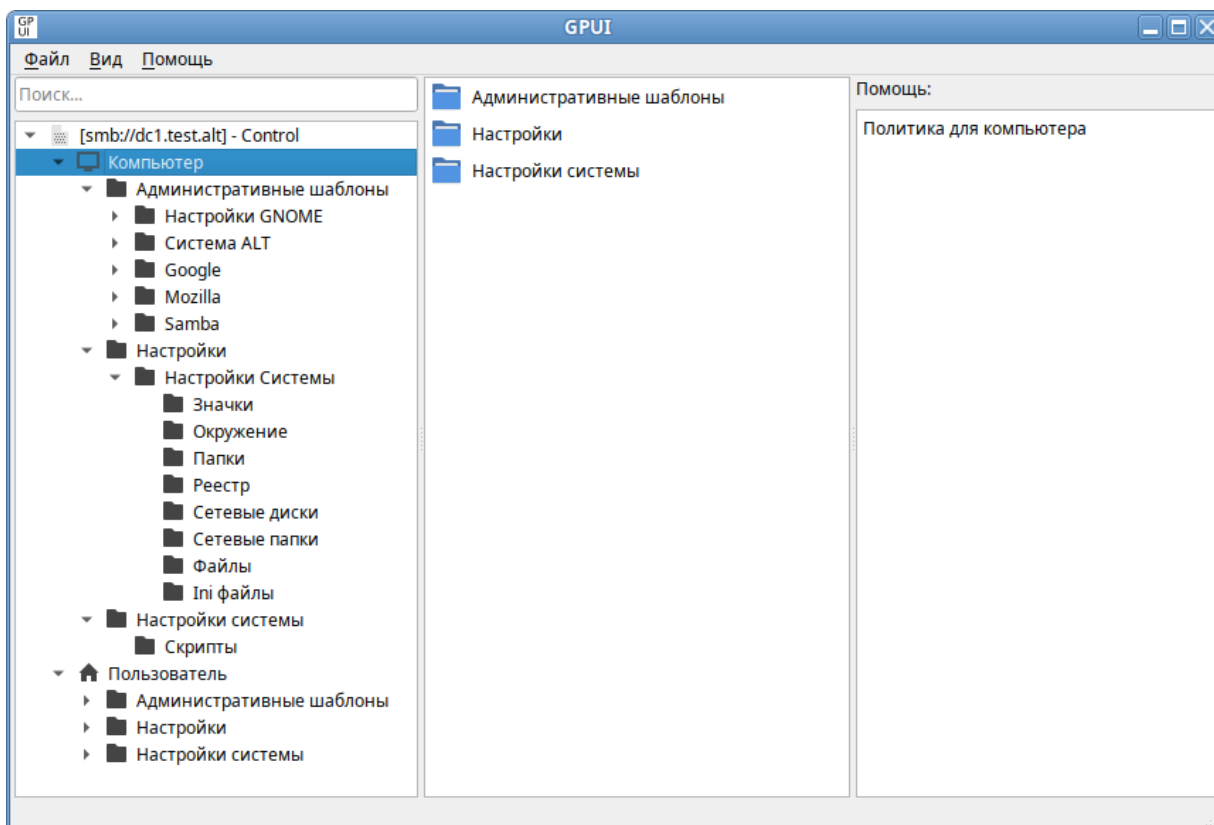


Рис. 357 – Интерфейс GPUI

Если параметр настраивается в секции «Компьютер», групповая политика должна быть привязана к OU с компьютерами. Соответственно, если настраиваемый параметр относится к конфигурации пользователя, нужно назначить политику на OU с пользователями. Также следует убедиться, что объект, к которому должна применяться политика находится в нужном OU с компьютерами или пользователями.

В каждом разделе есть три подраздела:

- «Административные шаблоны» («Administrative Templates») – содержит параметры различных компонентов. Здесь доступны как административные шаблоны ОС Альт СП и Windows, так и дополнительные ADMX-шаблоны (например, ADMX-шаблоны для Mozilla Firefox или для Google Chrome);
- «Настройки» («Preferences») – содержит дополнительный набор настроек (предпочтений). С помощью предпочтений можно настроить, в том числе такие параметры: создание ярлыков, подключение сетевых дисков, копирование файлов и папок на компьютеры;

- «Настройки системы» («System settings») – позволяет указать сценарии запуска и завершения работы компьютера, входа и выхода из системы пользователя.

Для быстрого доступа к политике можно воспользоваться поиском, для этого следует ввести в поле «Поиск...» ключевое слово.

10.4.6.3.1. Редактирование параметров в разделе «Административные шаблоны»

Чтобы изменить любой параметр групповой политики, нужно найти раздел, в котором он находится, и открыть его настройки в правой панели.

Параметры политики административных шаблонов могут иметь одно из трех состояний: «Не сконфигурировано»/ «Включено»/ «Отключено». Параметры политики в состоянии «Не сконфигурировано» не влияют на пользователей или компьютеры. Если параметр политики находится в состоянии «Включено», к пользователю или компьютеру применяется действие, описанное в заголовке параметра политики. Если параметр политики находится в состоянии «Отключено», к пользователю или компьютеру применяется действие, противоположное описанному в заголовке параметра политики. Как правило, состояния параметров политики «Не сконфигурировано» и «Отключено» приводят к одинаковым результатам (рис. 358).

В каждом параметре политики административных шаблонов предоставлены подробные сведения о состояниях «Включено», «Отключено» и «Не сконфигурировано». Можно просмотреть эти сведения в поле «Помощь» для каждого параметра политики административных шаблонов.

В поле «Поддерживается на» указаны версии ОС, для которых данная политика применима. Например, «10 платформа ALT как минимум» означает, что политика применима только к дистрибутивным решениям ОС «Альт» десятой (p10) и одиннадцатой платформ (p11). Данный параметр не будет работать на девятой платформе (p9).

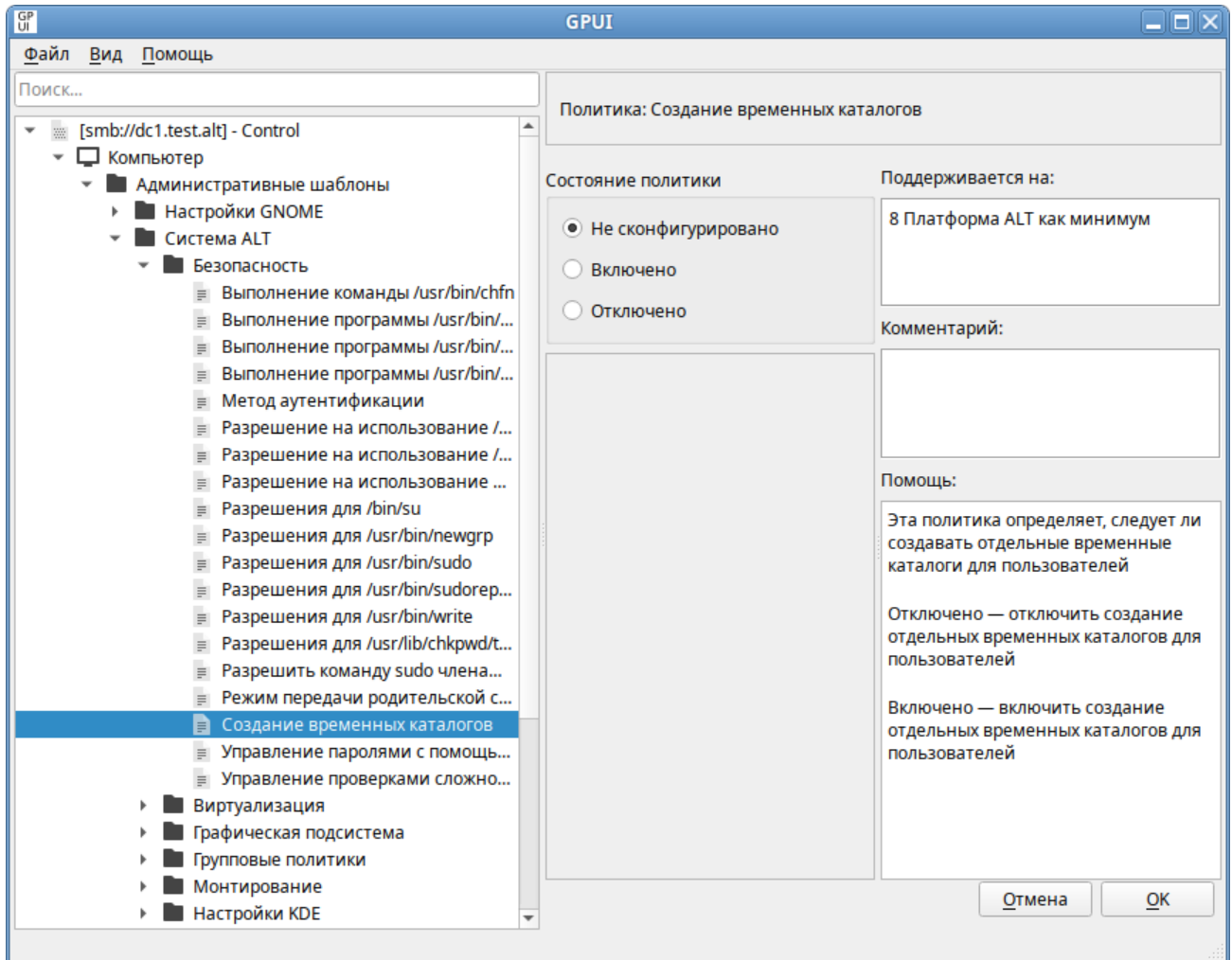


Рис. 358 – Состояние параметров политики

По умолчанию все параметры в разделе административных шаблонов не настроены (не сконфигурированы). Чтобы изменить настройку параметра групповой политики, достаточно выбрать новое состояние и нажать кнопку «ОК».

У некоторых настроек групповых политик можно задать дополнительные параметры, которые можно настроить в секции «Опции». Например, чтобы установить изображение в качестве фона рабочего стола через групповые политики, нужно включить политику и указать путь к файлу с изображением в поле «Файл» (рис. 359).

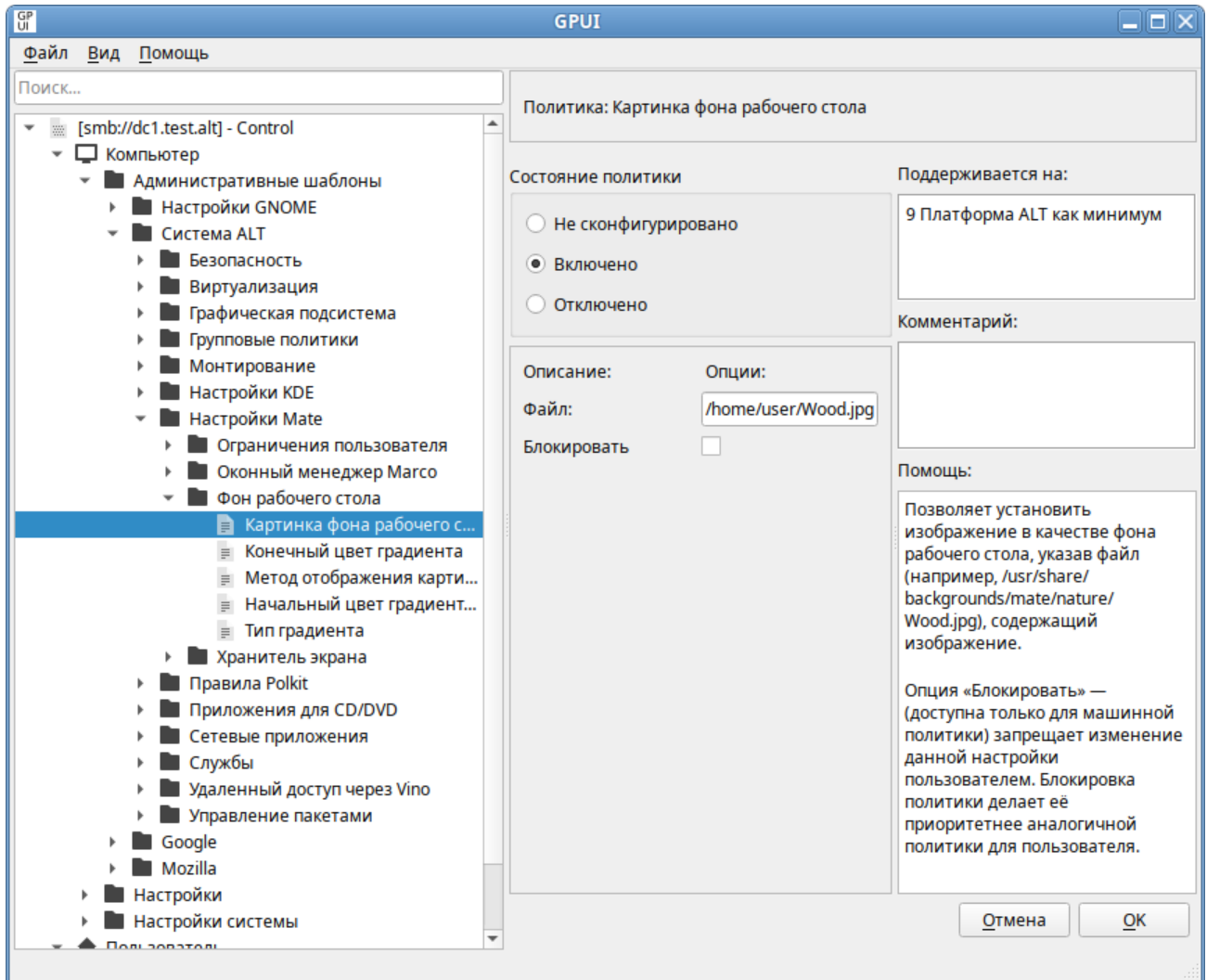


Рис. 359 – Установка изображения в качестве фона рабочего стола через групповые политики

В поле «Комментарий» можно указать примечание для групповой политики.

10.4.6.3.2. Фильтрация административных шаблонов

По умолчанию в GPUI отображаются все установленные административные шаблоны. Чтобы изменить отображение параметров политик административных шаблонов можно настроить фильтр административных шаблонов (рис. 360).

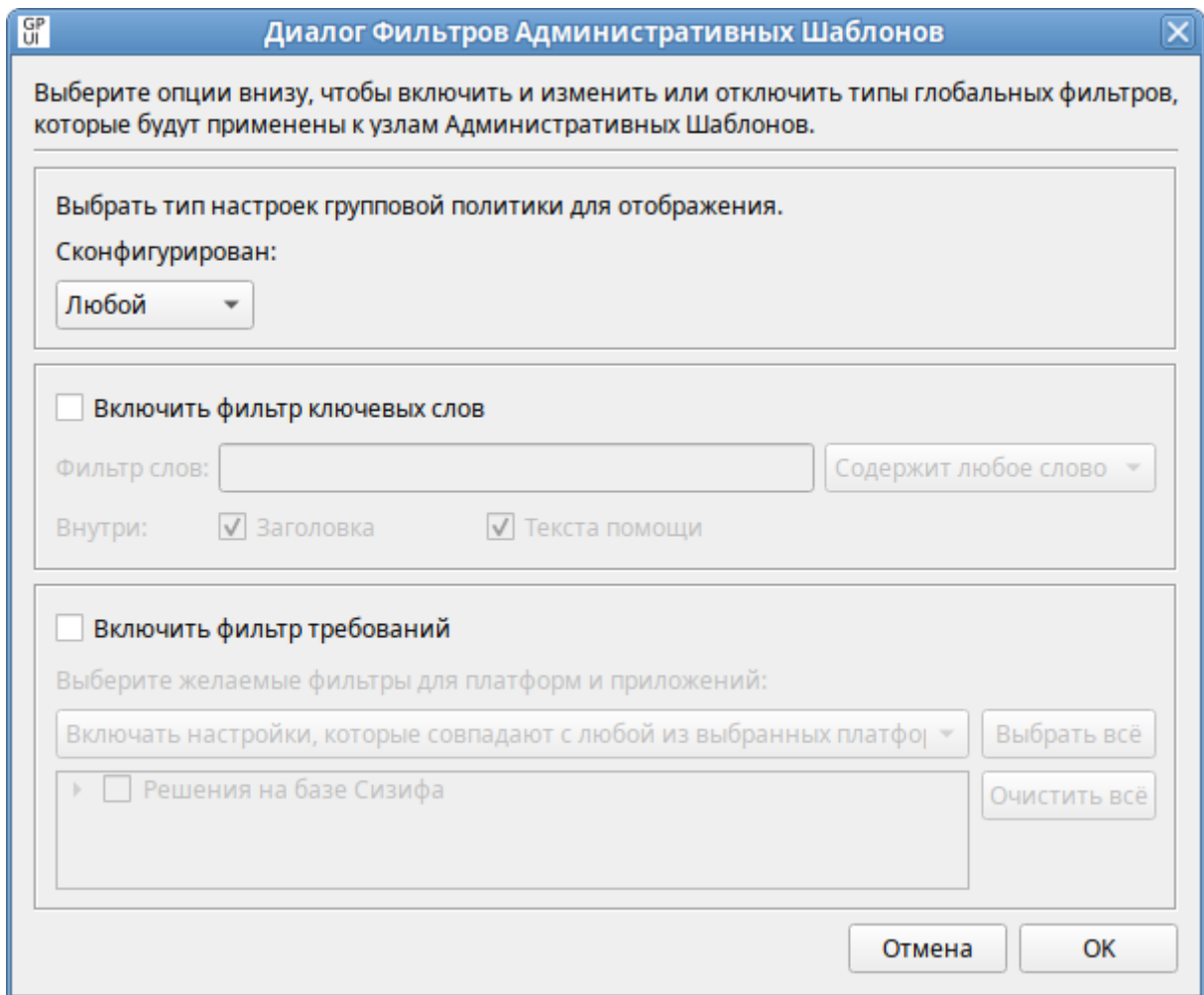


Рис. 360 – Диалог фильтров административных шаблонов

Фильтр административных шаблонов можно применять, если найти определенный параметр политики или ограничить количество параметров политики, отображаемых в GPUI.

Административные шаблоны можно отфильтровать на основе следующих факторов:

- настраиваемых параметров политики;
- ключевых слов в заголовке политики или тексте помощи к параметрам политики;
- требований параметров политики к платформам или приложениям.

Примечание. Фильтры являются включающими, поэтому необходимо выбирать элементы, которые следует отображать, а не исключаемые элементы.

10.4.6.3.2.1. Фильтр по настроенным параметрам

Фильтр по настроенным параметрам имеет три состояния:

- «Любой» – отображать все параметры политики административных шаблонов (по умолчанию);
- «Да» – отображать только сконфигурированные параметры политики административных шаблонов;
- «Нет» – отображать только не сконфигурированные параметры политики административных шаблонов.

Для установки фильтра по настроенным параметрам:

- 1) в меню выбрать «Вид» → «Фильтр» → «Редактировать фильтр» (рис. 361);

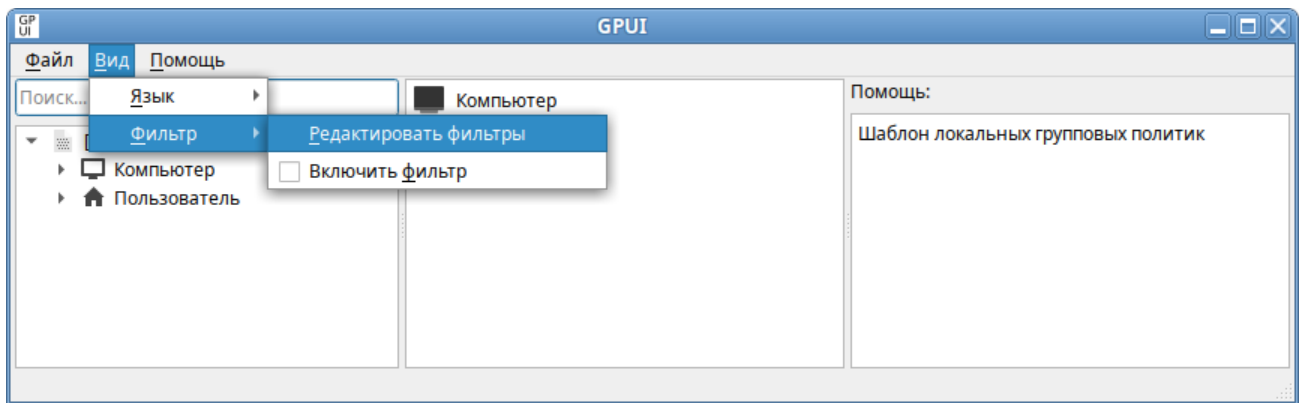


Рис. 361 – Фильтр по настроенным параметрам

- 2) в открывшемся окне в списке «Сконфигурирован» выбрать необходимый фильтр (рис. 362);
- 3) нажать кнопку «ОК», чтобы сохранить параметры фильтра;
- 4) чтобы применить фильтр в меню выбрать «Вид» → «Фильтр» → «Включить фильтр» (рис. 363).

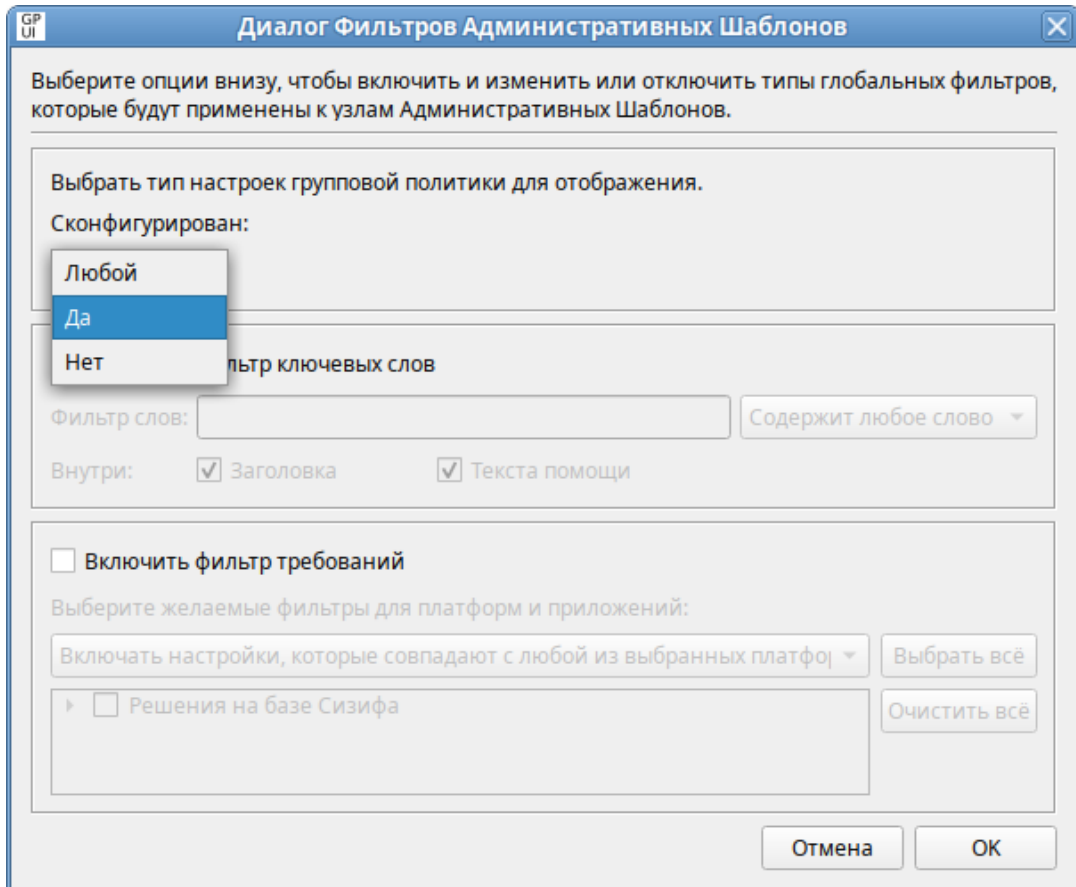


Рис. 362 – Фильтр по настроенным параметрам

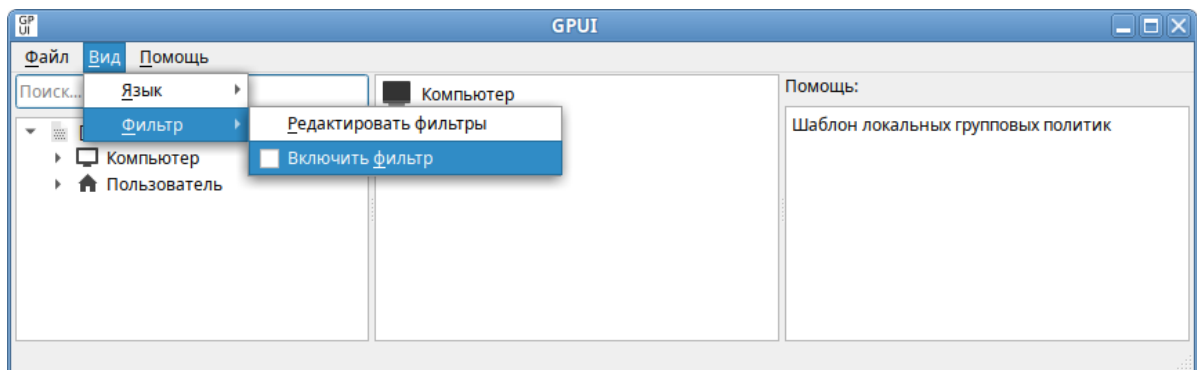


Рис. 363 – Включение фильтра административных шаблонов

10.4.6.3.2.2. Фильтр по ключевым словам

Для установки фильтра по ключевым словам:

- 1) в меню выбрать «Вид» → «Фильтр» → «Редактировать фильтр» (см. рис. 361);
- 2) в открывшемся окне установить отметку в поле «Включить фильтр ключевых слов» (рис. 364);

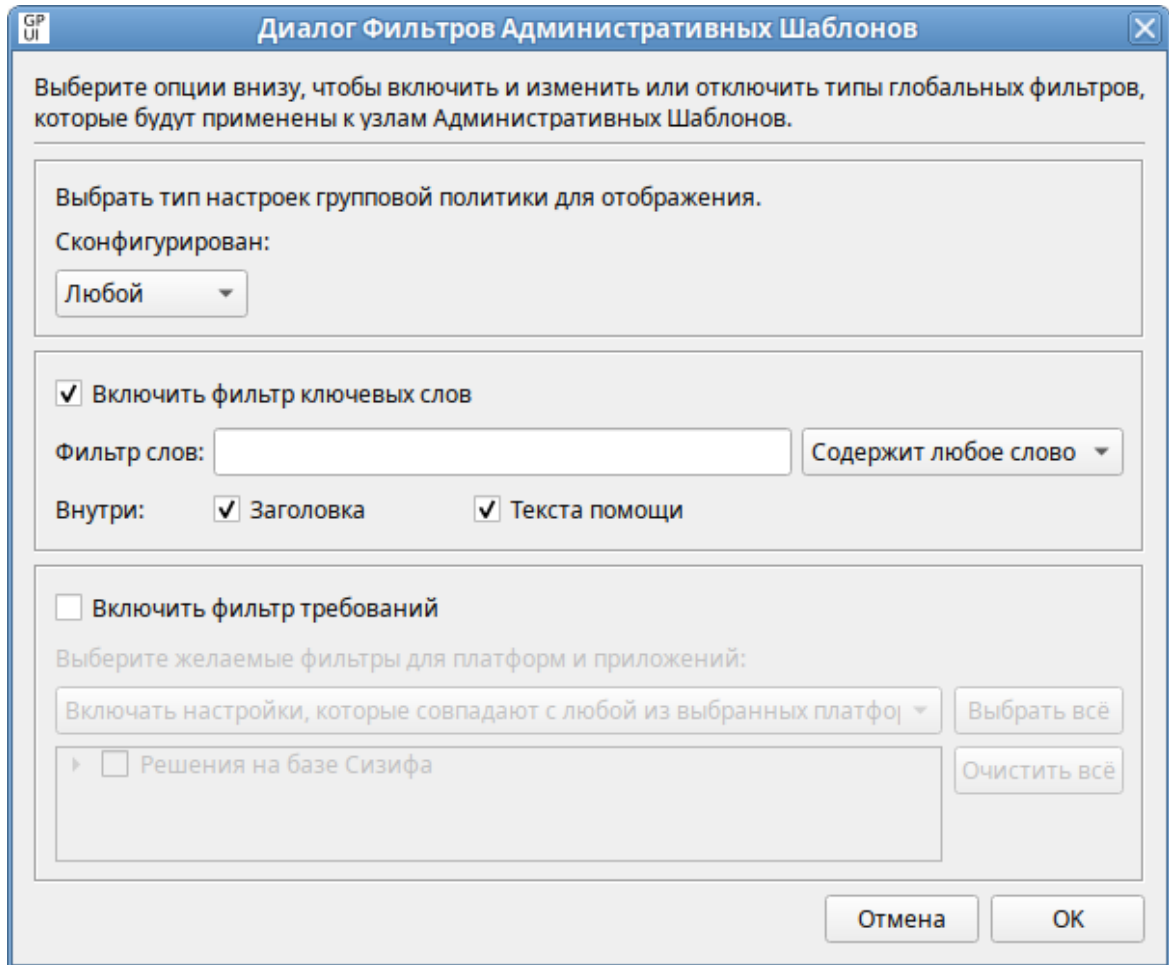


Рис. 364 – Отметка «Включить фильтр ключевых слов»

- 3) ввести одно или несколько ключевых слов в поле «Фильтр слов» и выбрать фильтр:
 - «Содержит любое слово» – фильтр содержит любое слово из поля «Фильтр слов»;
 - «Содержит все слова» – фильтр содержит все слова из поля «Фильтр слов»;
 - «Полностью совпадает» – фильтр содержит точное соответствие словам «Фильтр слов»;
- 4) установить соответствующие отметки в поле «Внутри»:
 - «Заголовка» – фильтр включает поиск в заголовке параметра политики;
 - «Текста помощи» – фильтр включает поиск в тексте помощи параметра политики;
- 5) нажать кнопку «ОК», чтобы сохранить параметры фильтра (рис. 365);

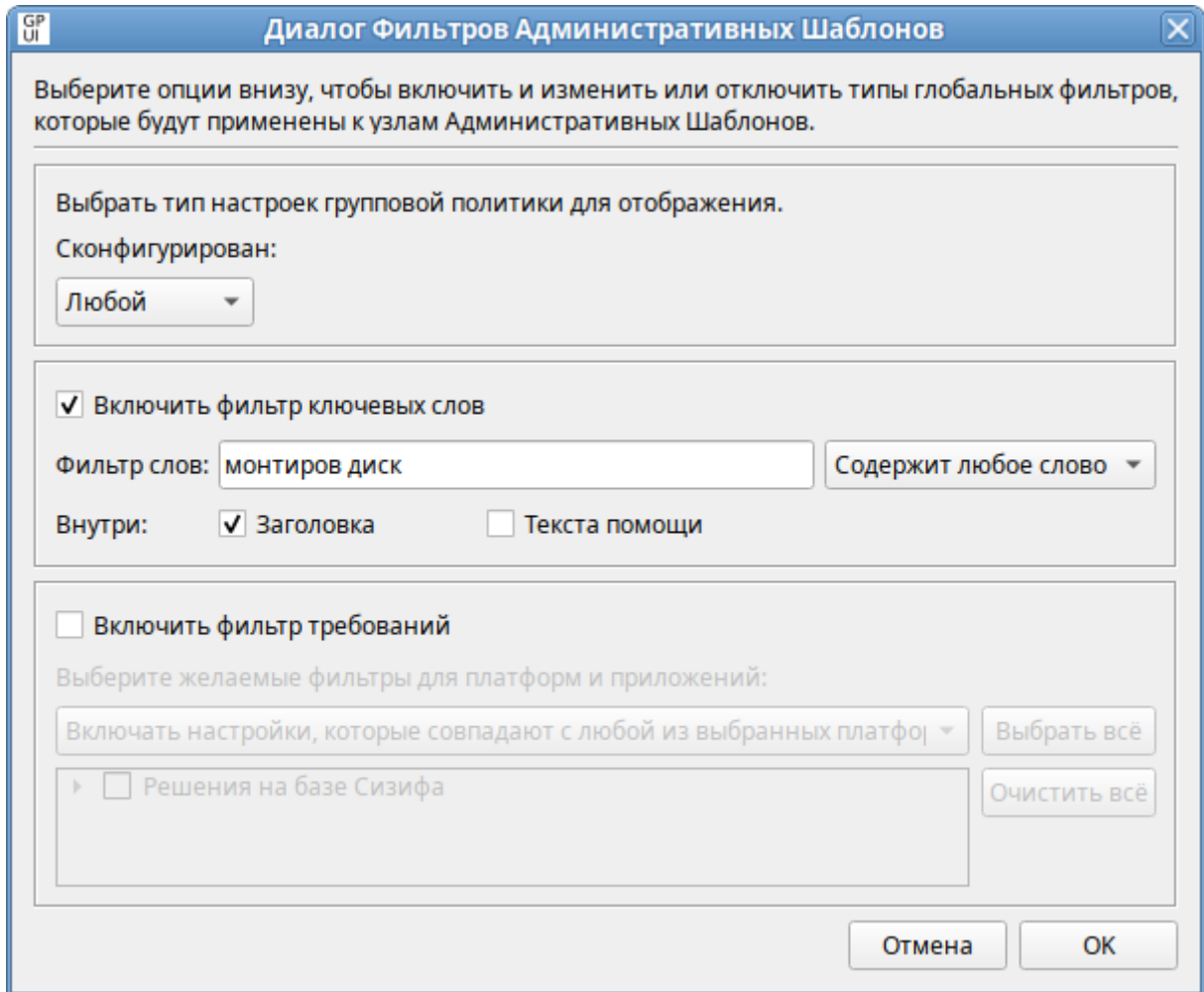


Рис. 365 – Настроенный фильтр ключевых слов

- б) чтобы применить фильтр в меню выбрать «Вид» → «Фильтр» → «Включить фильтр» (см. рис. 363).

Результат применения фильтра по ключевым словам (рис. 366).

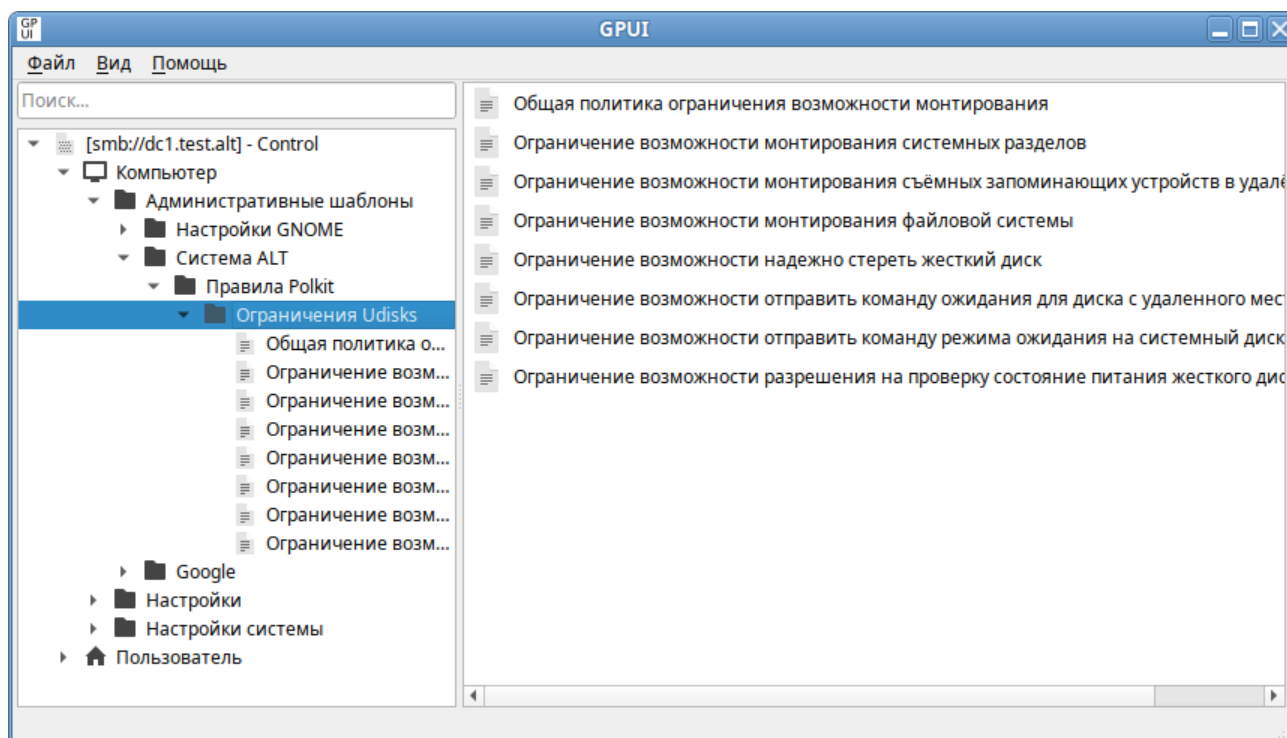


Рис. 366 – Результат применения фильтра по ключевым словам

10.4.6.3.2.3. Фильтр по требованиям

При помощи этого способа фильтрации, можно отобразить параметры, соответствующие всем выбранным платформам или отобразить параметры, соответствующие любой из выбранных платформ.

Для установки фильтра по требованиям:

- 1) в меню выбрать «Вид» → «Фильтр» → «Редактировать фильтр» (см. рис. 361);
- 2) в открывшемся окне установить отметку в поле «Включить фильтр ключевых требований»;
- 3) в списке «Выберите желаемые фильтры для платформы и приложений» выбрать фильтр:
 - включать настройки, которые совпадают с любой из выбранных платформ;
 - включить настройки, которые совпадают со всеми выбранными платформами;

- 4) выбрать необходимые платформы (рис. 367). Можно выбрать пункт «Решения на базе Сизифа», нажать кнопку «Выбрать все», чтобы выбрать все элементы в списке, или нажать кнопку «Очистить все», чтобы снять выделение всех элементов списка;

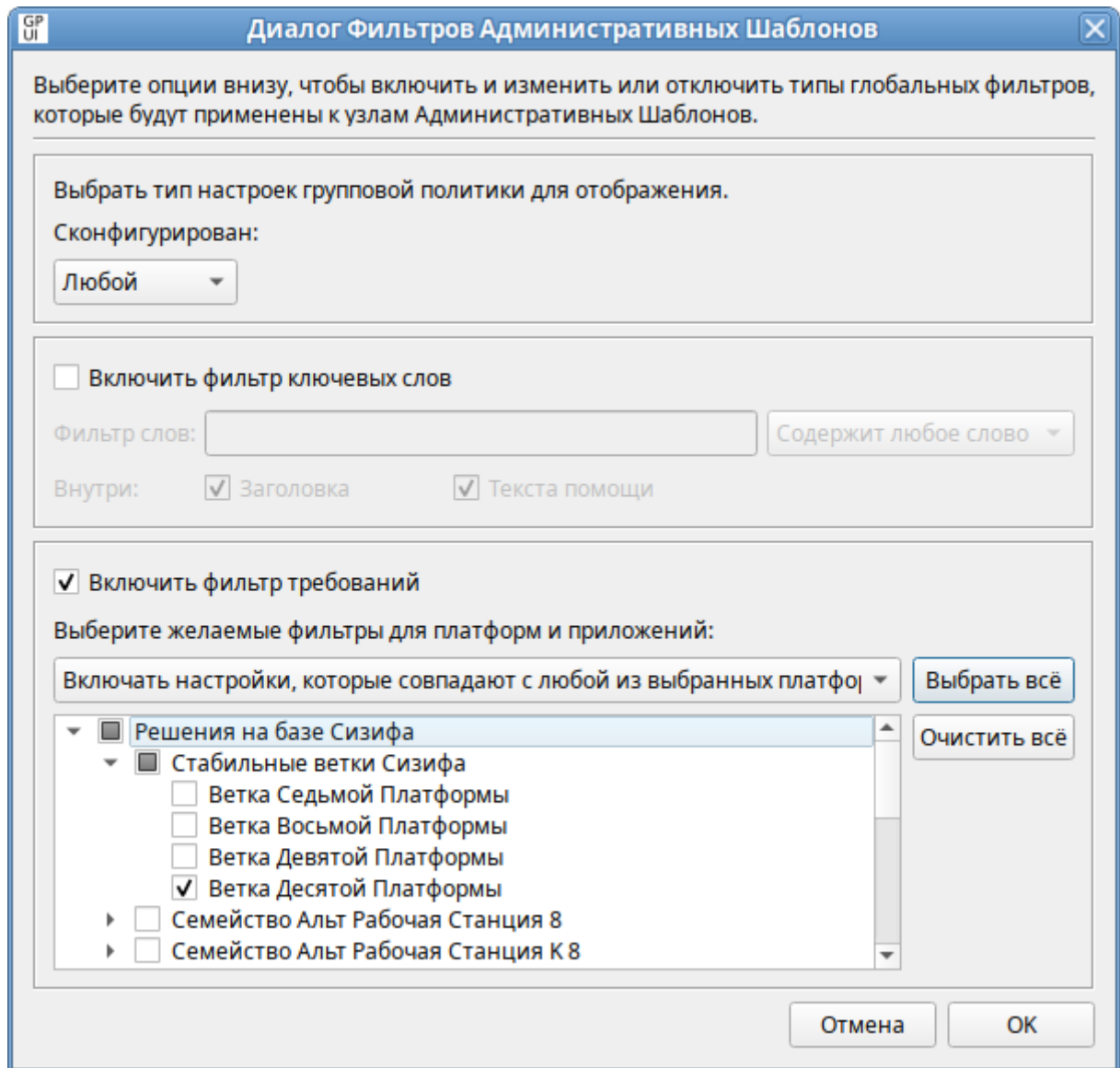


Рис. 367 – Настроенный фильтр по требованиям

- 5) нажать кнопку «ОК», чтобы сохранить параметры фильтра;
- 6) чтобы применить фильтр в меню выбрать «Вид» → «Фильтр» → «Включить фильтр» (рис. 363).

10.4.6.3.3. Работа с предпочтениями групповых политик

GPUИ позволяет настраивать следующие предпочтения:

- «Значки» – создание, редактирование или удаление ярлыков;

- «Окружение» – создание, редактирование или удаление переменных среды;
- «Папки» – создание, редактирование или удаление папок;
- «Реестр» – копирование параметров реестра и их применение к другим компьютерам, создание, замена или удаление параметров реестра (для машин Windows);
- «Сетевые папки» – создание, удаление (скрытие из общего доступа) или редактирование общих ресурсов;
- «Сетевые диски» – создание, редактирование или удаление сопоставленных дисков и настройка видимости всех дисков;
- «Файлы» – копирование, замена, удаление или изменение атрибутов файлов;
- «INI-файлы» – добавление, замена или удаление разделов/свойств файлов параметров настройки (INI) или информации об установке (INF).

Предпочтения можно настроить для пользователей и компьютеров (пункт «Настройки» соответственно в элементах «Компьютер» и «Пользователь») (рис. 368).

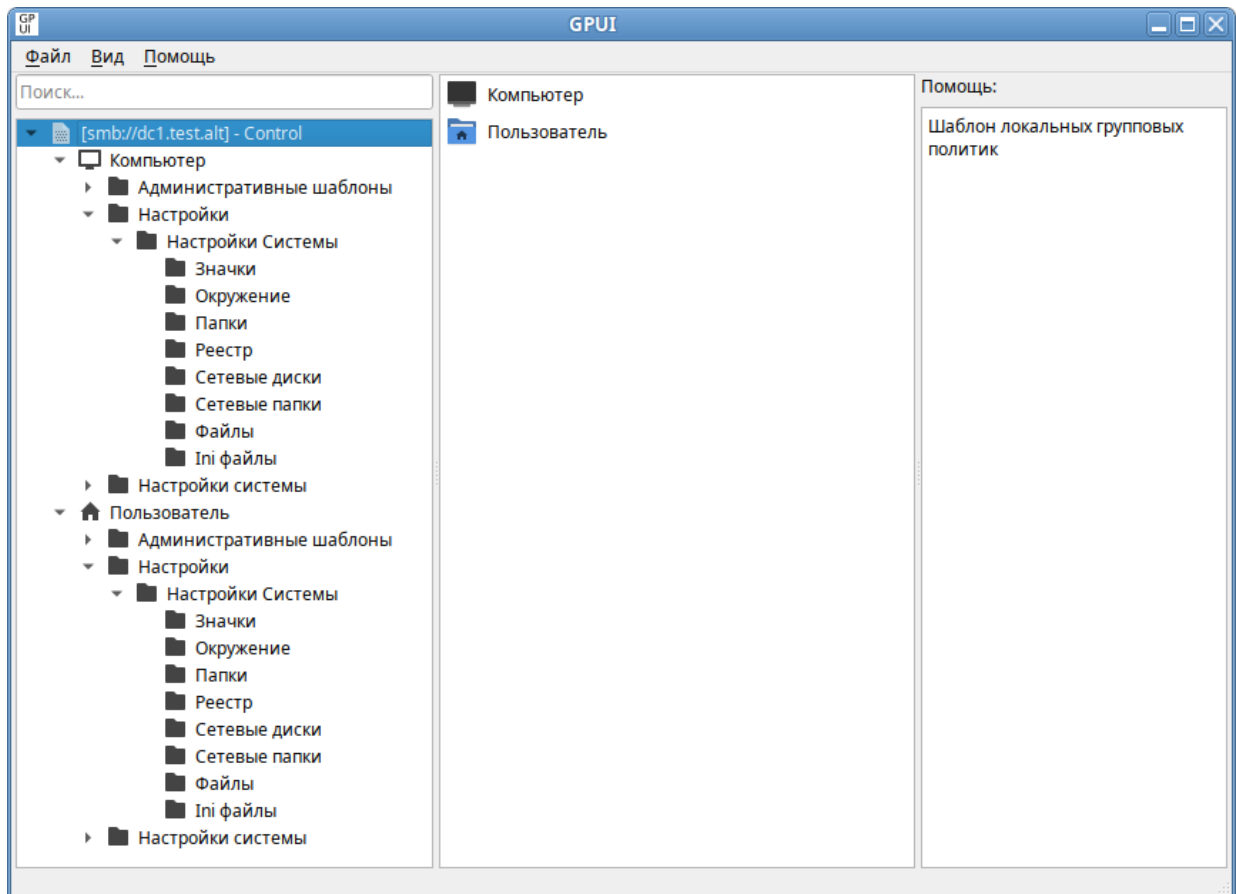


Рис. 368 – Управление предпочтениями

В каждом объекте групповой политики с каждым из расширений предпочтения можно создать несколько элементов предпочтения.

Для создания предпочтения нужно перейти в «Компьютер/Пользователь» → «Настройки» → «Настройки системы», выбрать соответствующее предпочтение, затем в контекстном меню свободной области выбрать пункт «Новый» → «Название_предпочтения».

Например, для создания нового предпочтения «Папки» нужно перейти в «Компьютер/Пользователь» → «Настройки» → «Настройки системы» → «Папки». В контекстном меню свободной области выбрать пункт «Новый» → «Папки» (рис. 369).

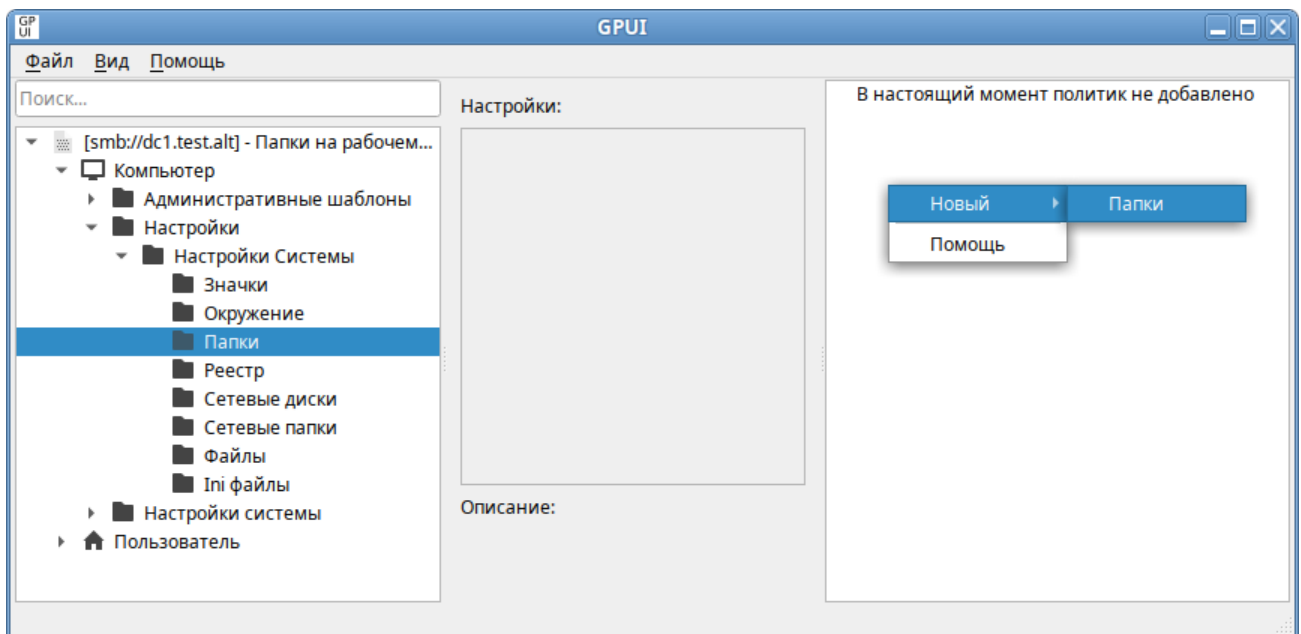


Рис. 369 – Создание новой политики «Папки»

Откроется диалоговое окно «Диалог настроек», где на вкладке «Основные настройки» можно задать параметры, характерные для соответствующего предпочтения (подробнее параметры настройки предпочтений рассмотрены в следующих разделах данного документа) (рис. 370).

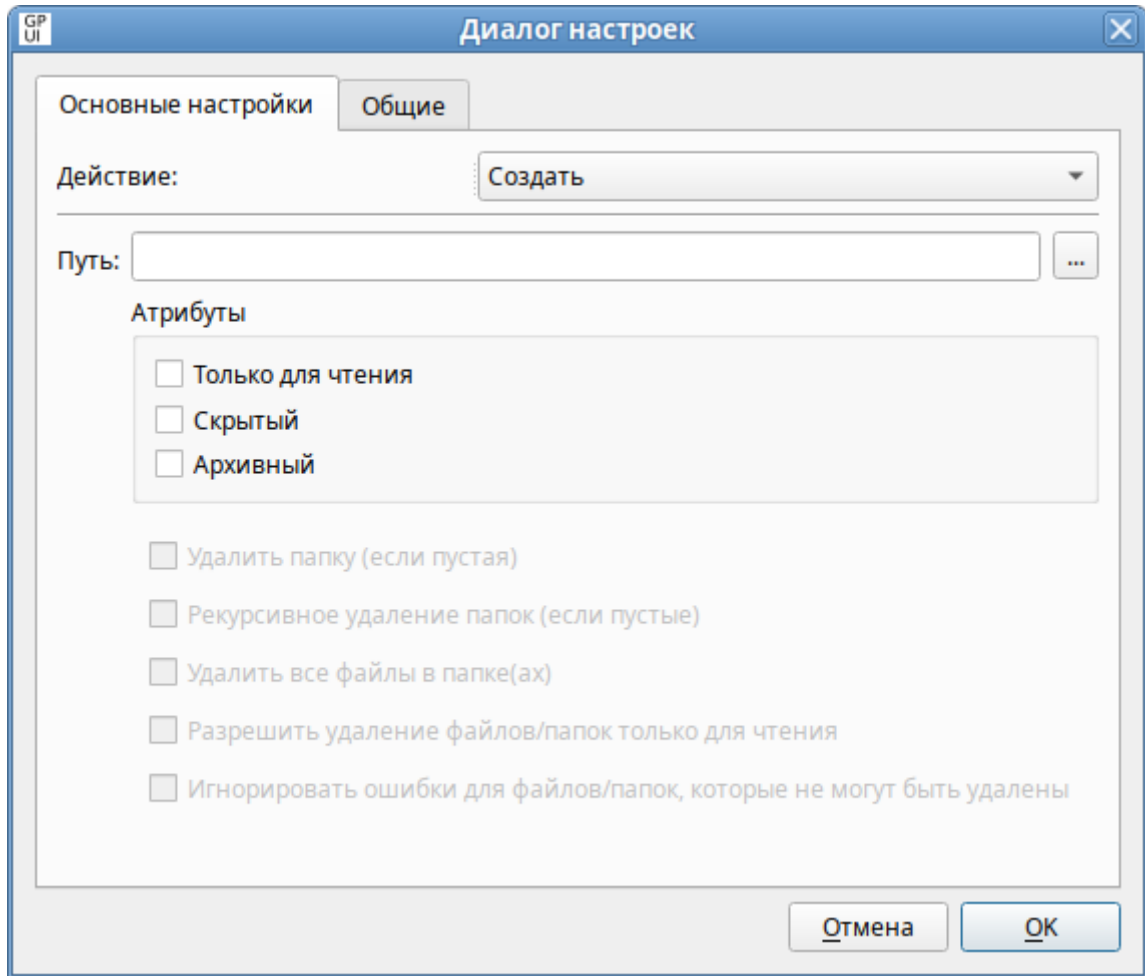


Рис. 370 – Вкладка «Основные настройки»

Вкладка «Общие» содержит настройки одинаковые для всех предпочтений:

- «Остановить обработку элементов в этом расширении при возникновении ошибки» – при сбое элемента предпочтений обработка других элементов предпочтений в этом расширении останавливается;
- «Выполнять в контексте безопасности текущего пользователя (опция пользовательских политик)»;
- «Удалить элемент, если больше не применим»;
- «Описание» (рис. 371).

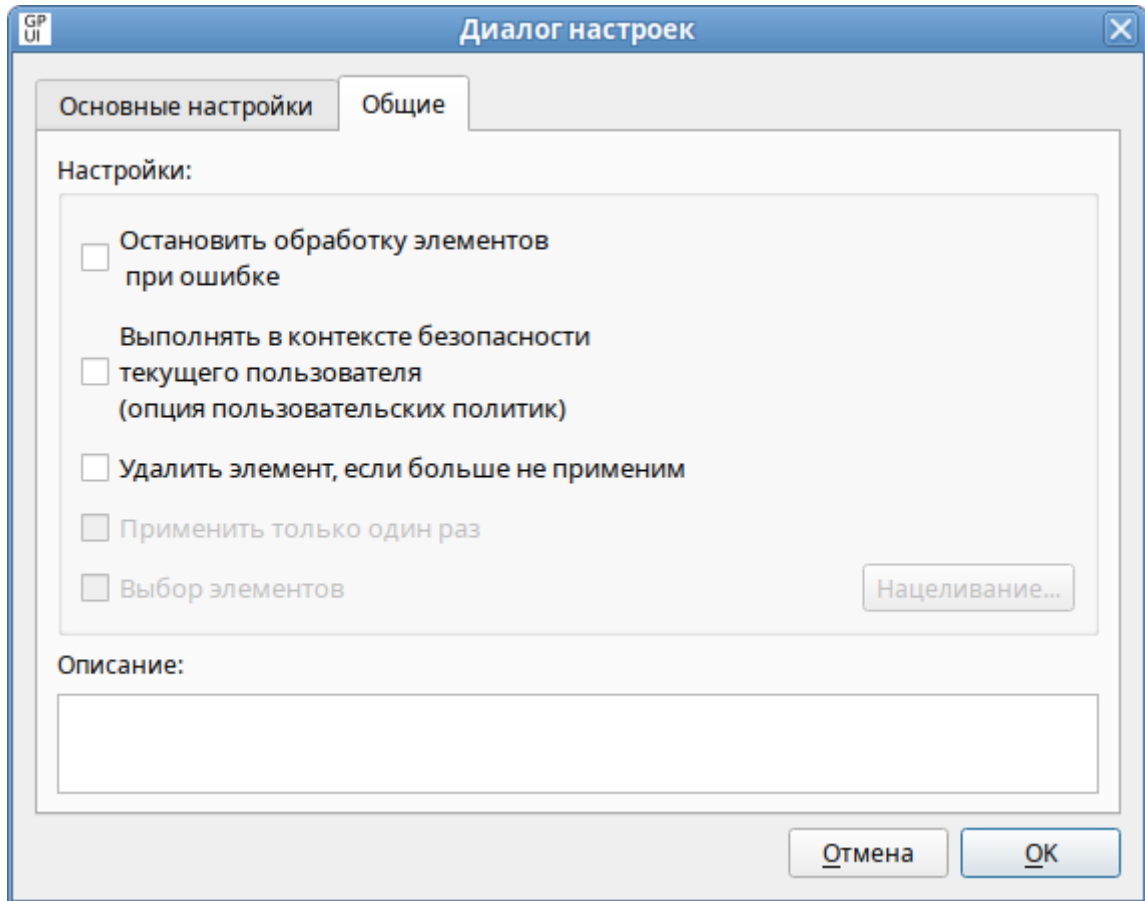


Рис. 371 – Вкладка «Общие»

Для редактирования элемента предпочтения следует дважды щелкнуть мышью по элементу (рис. 372) или в контекстном меню предпочтения выбрать пункт «Изменить элемент» (рис. 373).

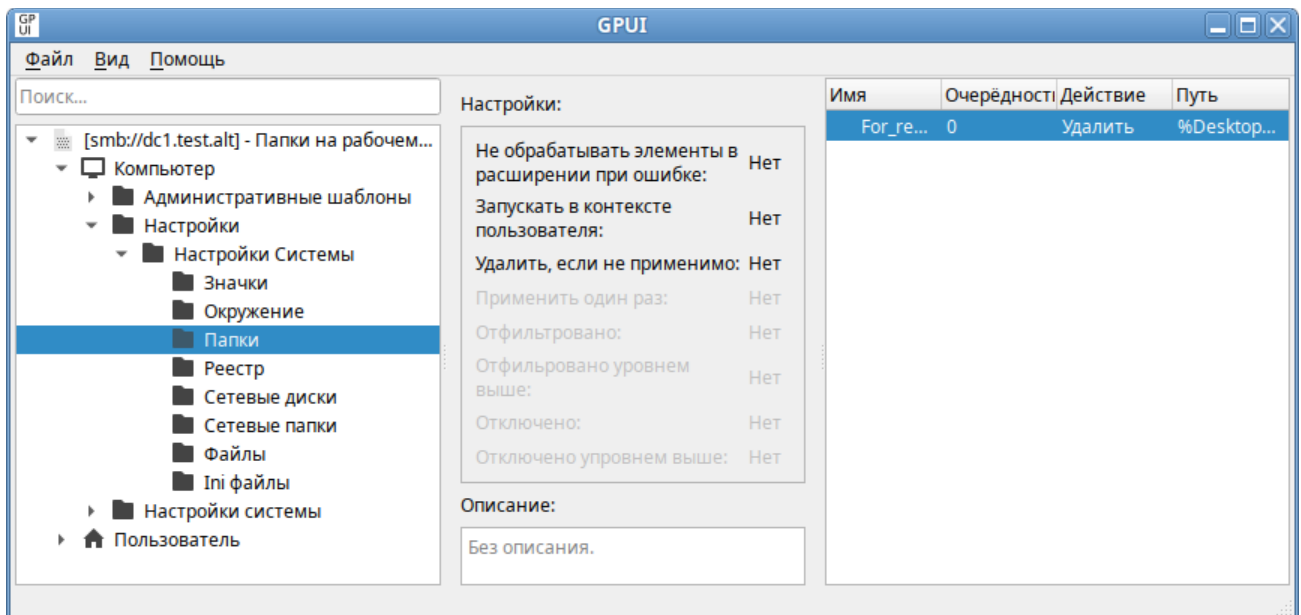


Рис. 372 – Элемент предпочтения

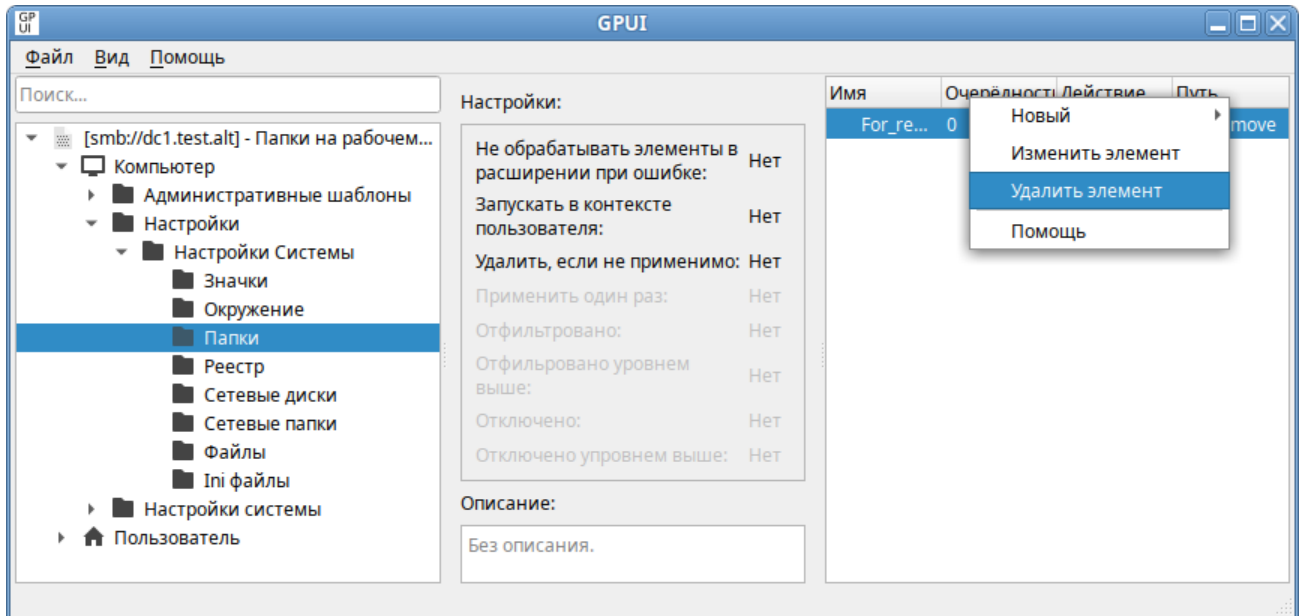


Рис. 373 – Контекстное меню элемента предпочтения

Откроется окно редактирования предпочтения (рис. 374).

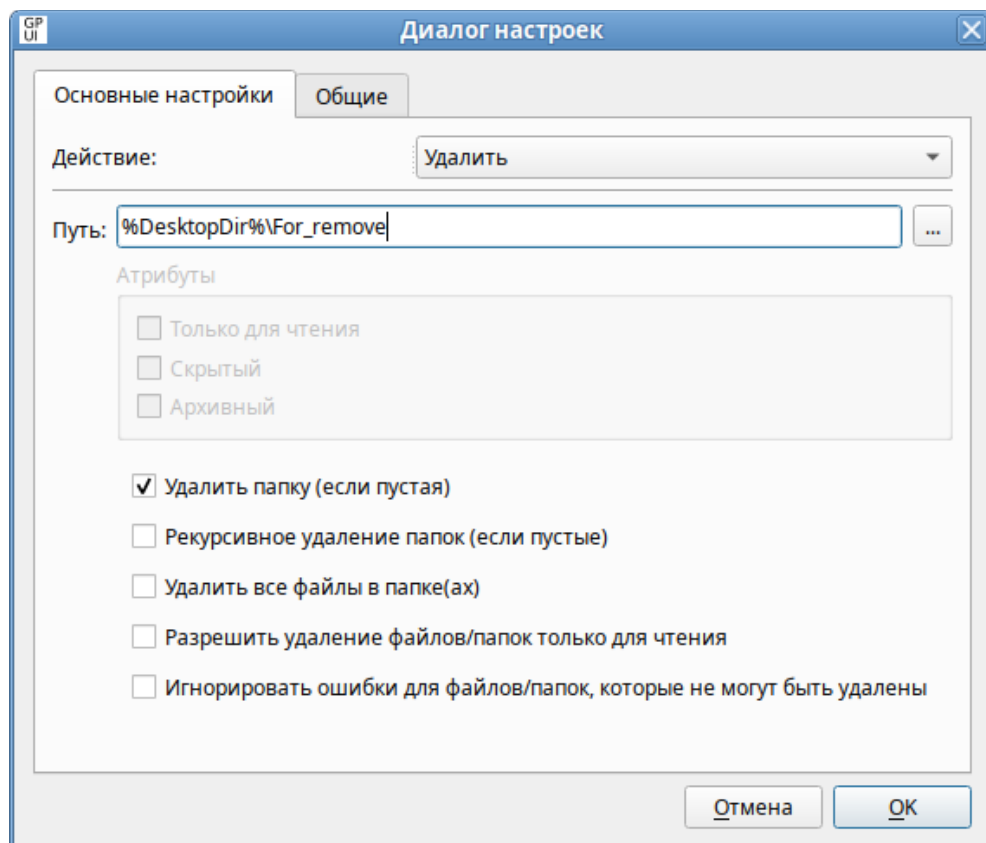


Рис. 374 – Редактирование предпочтения

Для удаления элемента следует в контекстном меню предпочтения выбрать пункт «Удалить элемент» (рис. 373).

10.4.6.3.4. Работа со скриптами

Работа со скриптами подробно описана в п. 10.4.6.6.

10.4.6.3.5. Смена языка

Для того чтобы изменить язык интерфейса, нужно в меню выбрать «Вид» → «Язык» (рис. 375).

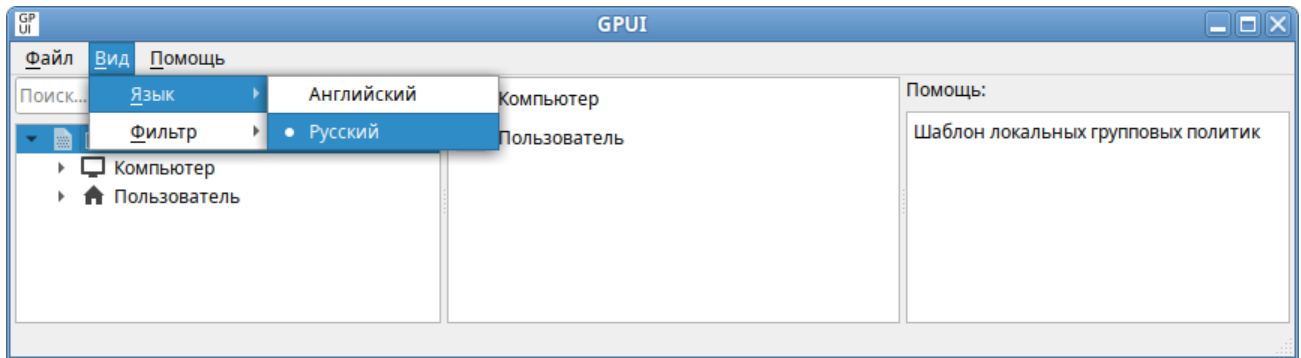


Рис. 375 – Выбор языка

10.4.6.4. Редактирование групповых политик

10.4.6.4.1. Включение или выключение различных служб (сервисов systemd)

Данные групповые политики позволяют управлять состоянием (включением или выключением) различных служб (сервисов systemd).

Для настройки политики следует перейти в «Компьютер» → «Административные шаблоны» → «Система ALT» → «Службы» → «Systemd» (рис. 376).

При выборе политики, откроется диалоговое окно настройки политики (рис. 377).

Можно не задавать настройку политики, включить или отключить:

- «Не сконфигурировано» – не изменять системное состояние службы;
- «Включено» – перевести службу во включенное состояние (выполнить команду `systemctl enable <служба>`);
- «Отключено» – перевести службу в состояние выключено (выполнить команду `systemctl disable <служба>`).

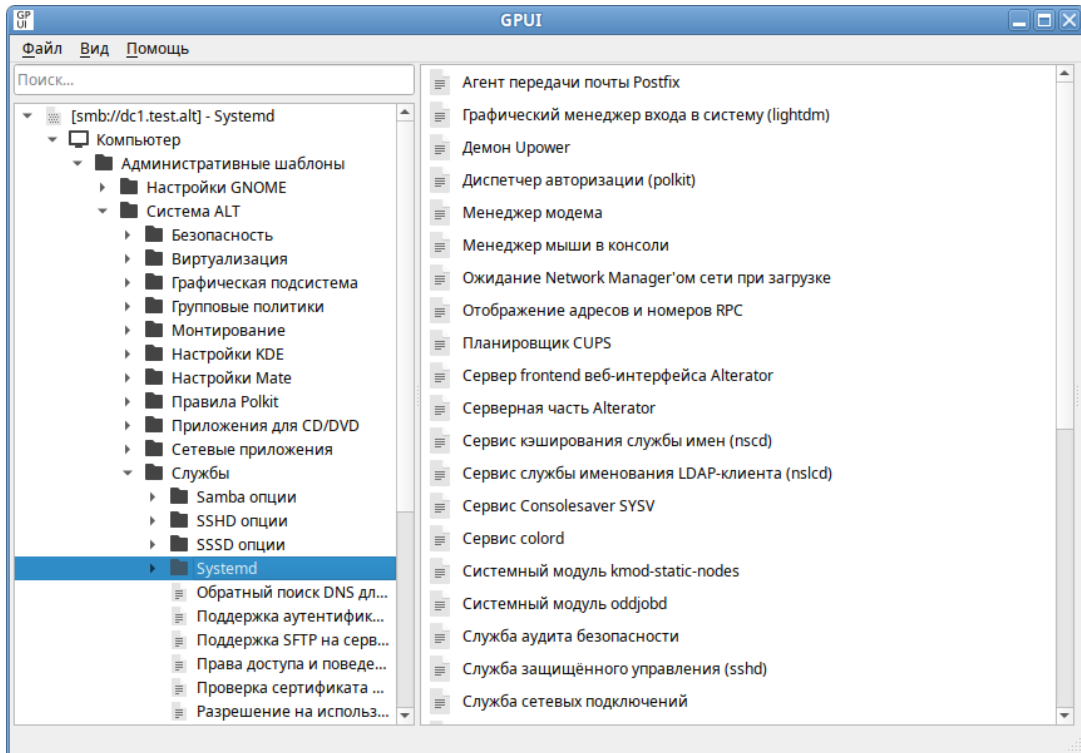


Рис. 376 – Список политик SystemdUnits

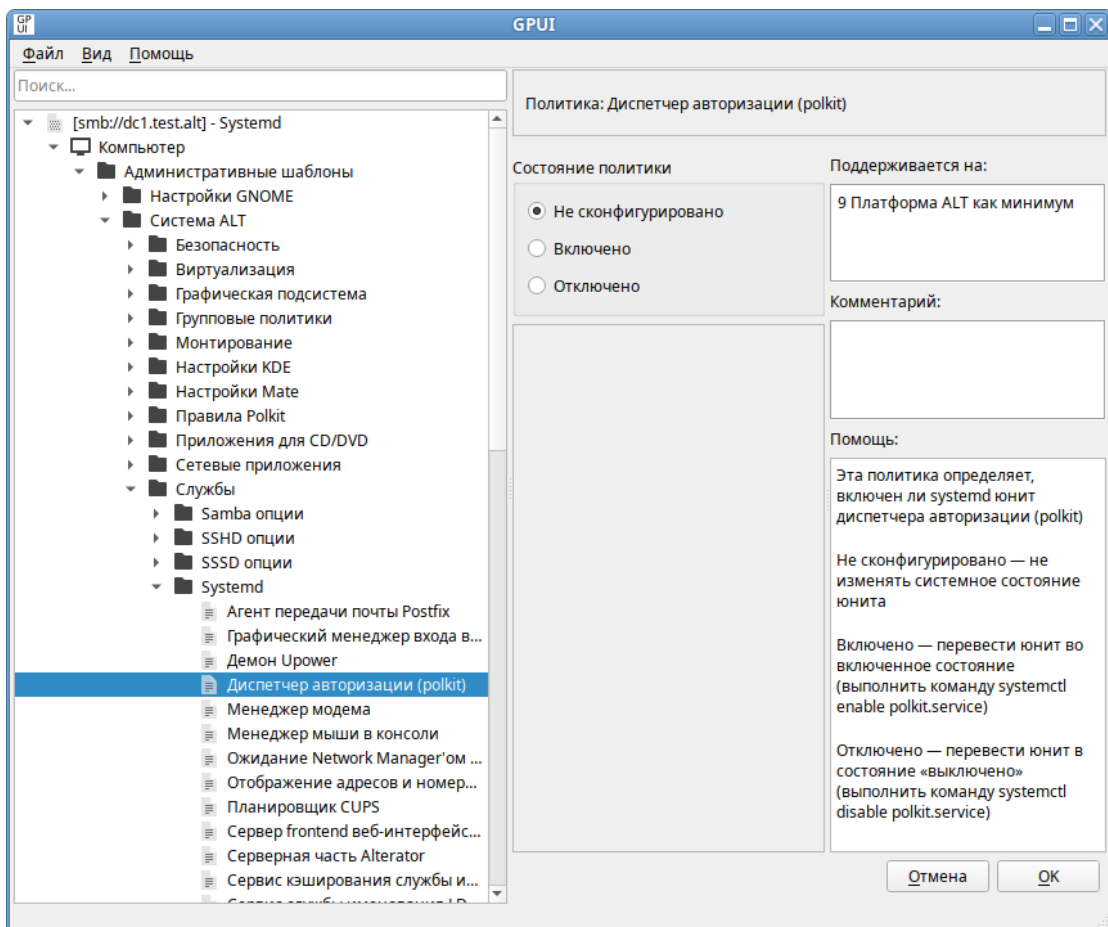


Рис. 377 – Диалоговое окно настройки политики

Список служб, состояние которых можно изменить, настроив соответствующую политику в GPUI, указан в таблице 29.

Т а б л и ц а 29 – Список служб, состояние которых можно изменить, настроив соответствующую политику в GPUI

Служба	Описание	Сервис systemd
Менеджер модема	Политика определяет, включен ли systemd юнит диспетчера модемов	ModemManager.service
Ожидание Network Manager'ом сети при загрузке	Политика определяет, включен ли systemd юнит «Network Manager Wait Online»	NetworkManager-wait-online.service
Управление службой Network Manager	Политика определяет, включен ли systemd юнит «Network Manager»	NetworkManager.service
Служба учетных записей (accounts-daemon)	Политика определяет, включен ли systemd юнит службы учетных записей (accounts-daemon)	accounts-daemon.service
Служба события ACPI	Политика определяет, включен ли systemd юнит системной службы событий ACPI	acpid.service
Сервер frontend веб-интерфейса Alterator	Политика определяет, включен ли systemd юнит веб-сервера frontend интерфейса Alterator	ahttpd.service
Серверная часть Alterator	Политика определяет, включен ли systemd юнит внутреннего сервера Alterator	alteratord.service
Служба аудита безопасности	Политика определяет, включен ли системный модуль службы аудита безопасности	auditd.service
Avahi mDNS/DNS-SD	Политика определяет, включен ли systemd юнит стека mDNS/DNS-SD Avahi	avahi-daemon.service
DNS-сервер BIND	Политика определяет, включен ли systemd юнит DNS-сервера (сервиса) BIND	bind.service
Chronyd (служба NTP)	Политика определяет, включен ли systemd юнит NTP клиента/сервера Chronyd	chronyd.service
Сервис colord	Политика определяет, включен ли systemd юнит colord (сервис для управления, установки и создания цветовых профилей)	colord.service
Сервис Consolesaver SYSV	Политика определяет, включен ли systemd юнит Consolesaver (этот пакет загружает конфигурацию энергосбережения консоли)	consolesaver.service
Cpufreq-simple сервис	Политика определяет, включен ли systemd юнит службы Cpufreq-simple (загружает модули ядра, которые требуются для масштабирования cpufreq)	cpufreq-simple.service
Служба Crond	Политика определяет, включен ли systemd юнит службы Cron	crond.service
Шина системных сообщений D-Bus	Политика определяет, включен ли systemd юнит шины системных сообщений D-Bus	dbus.service
Служба Dnsmasq	Политика определяет, включен ли systemd юнит службы Dnsmasq (облегченный DHCP и кэширующий DNS-сервер, а также TFTP-сервер для поддержки загрузки по сети)	dnsmasq.service

Окончание таблицы 29

Служба	Описание	Сервис systemd
Менеджер мыши в консоли	Политика определяет, включен ли systemd юнит диспетчера мыши консоли	gpm.service
Системный модуль kmod-static-nodes	Политика определяет, включен ли systemd юнит kmod-static-nodes (создает список статических узлов устройства для текущего ядра)	kmod-static-nodes.service
Kerberos 5 KDC	Политика определяет, включен ли systemd юнит Kerberos 5 KDC	krb5kdc.service
Графический менеджер входа в систему (lightdm)	Политика определяет, включен ли systemd юнит службы графического менеджера входа в систему	lightdm.service
Служба сетевых подключений	Политика определяет, включен ли systemd юнит службы сетевых подключений	network.service
Samba NMB сервис	Политика определяет, включен ли systemd юнит сервиса Samba NMB	nmb.service
Сервис кэширования службы имен (nscd)	Политика определяет, включен ли systemd юнит сервиса кэширования службы имен	nscd.service
Сервис службы именованя LDAP-клиента (nslcd)	Политика определяет, включен ли systemd юнит сервиса служб именованя клиента LDAP	nslcd.service
Системный модуль oddjobd	Политика определяет, включен ли systemd юнит oddjobd (используется для запуска привилегированных операций для непривилегированных процессов)	oddjobd.service
SYSV: интерфейс терминала смарт-карт	Политика определяет, включен ли systemd юнит Openct (SYSV: терминал смарт-карт)	openct.service
Планировщик CUPS	Политика определяет, включен ли systemd юнит Service CUPS (планировщик)	org.cups.cupsd.service
Служба PC/SC Smart Card	Политика определяет, включен ли systemd юнит службы поддержки PC/SC Smart Card	pcscd.service
Диспетчер авторизации (polkit)	Политика определяет, включен ли systemd юнит диспетчера авторизации (polkit)	polkit.service
Агент передачи почты Postfix	Политика определяет, включен ли systemd юнит агента передачи почты Postfix	postfix.service
Сервис отображения универсальных адресов и номеров программ RPC	Политика определяет, включен ли systemd юнит RPC bind	rpcbind.service
Samba SMB сервис	Политика определяет, включен ли systemd юнит сервиса Samba SMB	smb.service
Служба защищенного управления (sshd)	Политика определяет, включен ли systemd юнит демона сервера OpenSSH	sshd.service
Демон Upower	Политика определяет, включен ли systemd юнит Daemon Upower (управление питанием)	upower.service
Samba Winbind сервис	Политика определяет, включен ли systemd юнит Samba Winbind	winbind.service

10.4.6.4.2. Управление control framework

Через групповые политики реализовано управление настройками control.

control, использующийся в ОС Альт СП, механизм переключения между неким набором фиксированных состояний для задач, допускающих такой набор. Подсистема control используется для управления доступом к службам и позволяет переключать многие системные службы между заранее определенными состояниями.

Для настройки политики следует перейти в «Компьютер» → «Административные шаблоны» → «Система ALT». В этом разделе есть несколько подразделов, соответствующих категориям control (рис. 378).

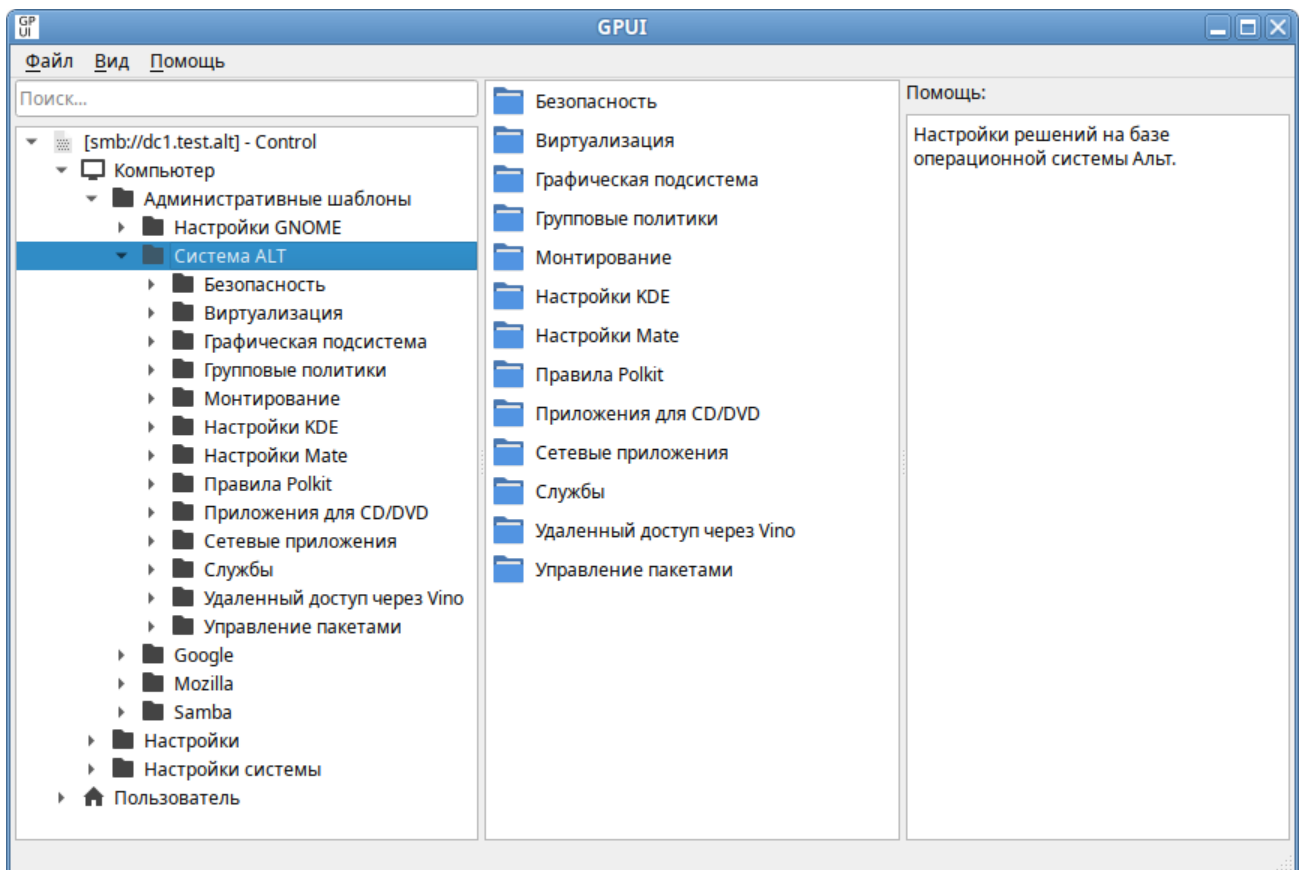


Рис. 378 – Политики настройки систем Альт

После выбора категории, в правом окне редактора отобразится список политик (рис. 379).

При выборе политики, откроется диалоговое окно настройки политики (рис. 380).

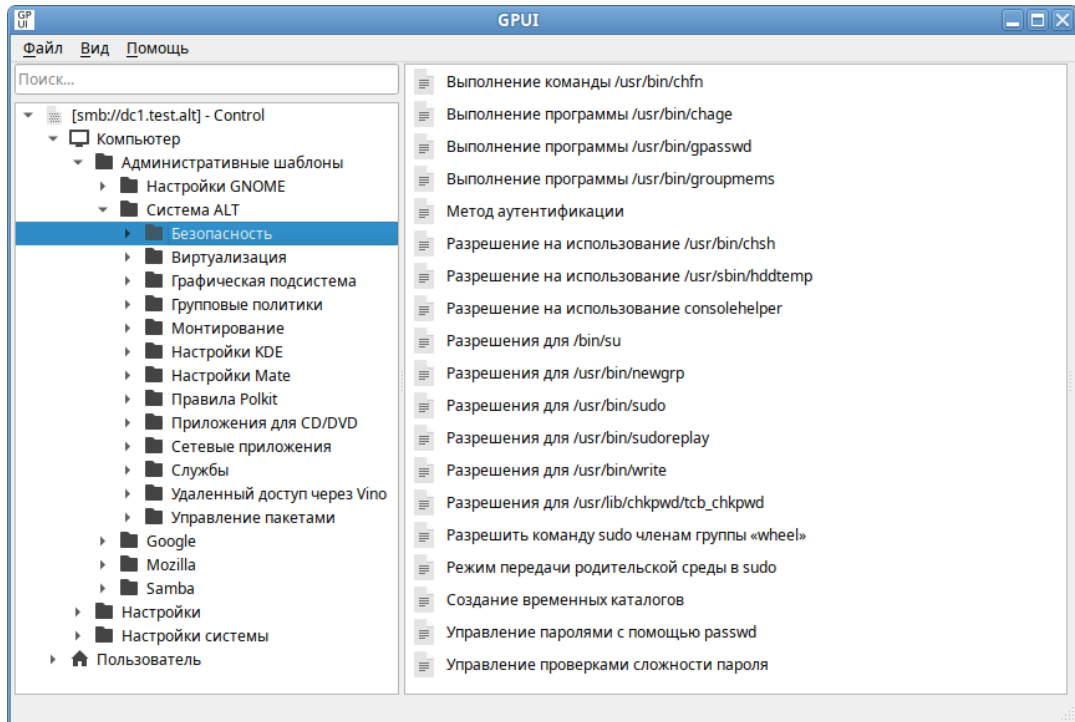


Рис. 379 – Список политик группы «Безопасность»

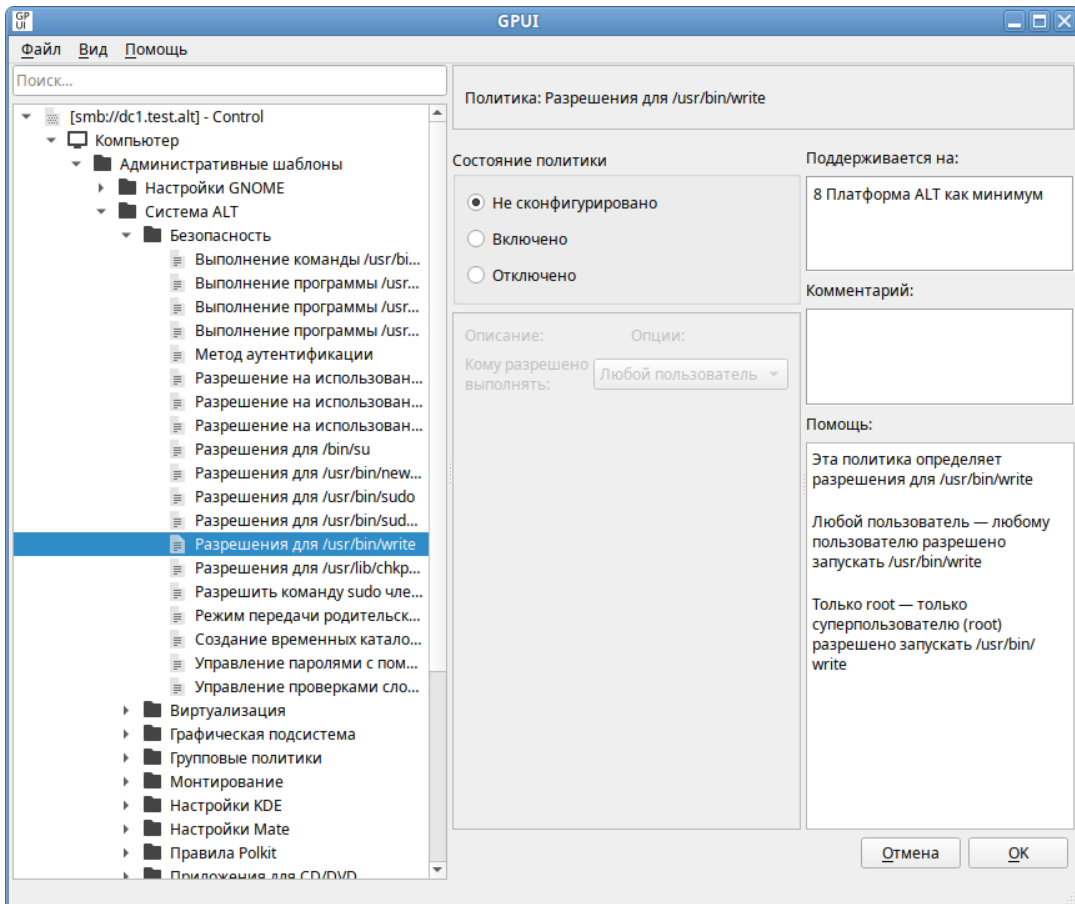


Рис. 380 – Диалоговое окно настройки политики

Можно не задавать настройку политики, включить или отключить. Если выбрать параметр «Включено», в разделе «Параметры» в выпадающем списке можно выбрать режим доступа для данного control (рис. 381).

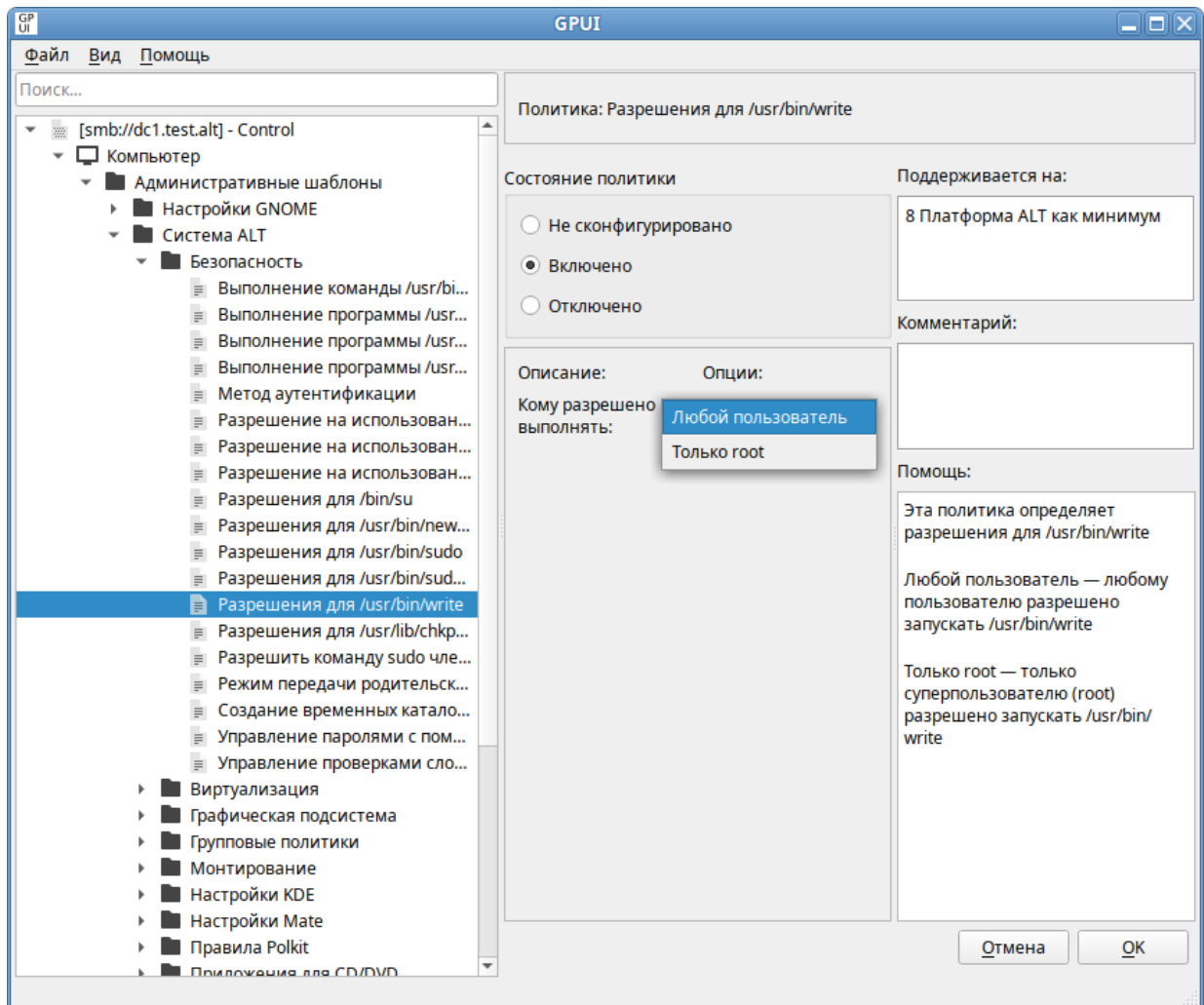


Рис. 381 – Выбор реeжима доступа для control

Все control в GPUI разделены на категории:

- «Безопасность» (см. таблицу 30);
- «Службы» (см. таблицу 31);
- «Сетевые приложения» (см. таблицу 32);
- «Приложения для CD/DVD» (см. таблицу 33);
- «Монтирование» (см. таблицу 34);
- «Виртуализация» (см. таблицу 35);
- «Графическая подсистема» (см. таблицу 36).

Примечание. Для поддержки общих сетевых ресурсов с помощью политик на клиенте должны быть выполнены следующие условия:

- установлен пакет `samba-usershares`;
- в файле `/etc/samba/smb.conf` в секции `[global]` подключен файл `/etc/samba/usershares.conf` (`include = /etc/samba/usershares.conf`).

Т а б л и ц а 30 – Категория «Безопасность»

Политика	Control	Описание	Режимы
Выполнение программы <code>/usr/bin/chage</code>	<code>chage</code>	Политика позволяет контролировать доступ для выполнения программы <code>/usr/bin/chage</code>	«Только root» – только суперпользователь (root) может выполнить <code>/usr/bin/chage</code> . «Любой пользователь» – любой пользователь может просмотреть, когда ему следует сменить свой пароль, используя команду <code>chage -l имя_пользователя</code>
Выполнение программы <code>/usr/bin/chfn</code>	<code>chfn</code>	Политика позволяет контролировать поведение и права доступа к команде <code>chfn</code> (<code>/usr/bin/chfn</code>). Команда <code>chfn</code> может изменить полное имя пользователя, номер кабинета, номера офисного и домашнего телефона для учетной записи пользователя. Обычный пользователь может изменять поля только для своей учетной записи, с учетом ограничений в <code>/etc/login.defs</code> (конфигурация по умолчанию не позволяет пользователям менять свое полное имя)	«Только root» – только суперпользователь (root) может выполнить <code>/usr/bin/chfn</code> . «Любой пользователь» – любой пользователь может использовать команду <code>/usr/bin/chfn</code>
Разрешение на использование Consolehelper	<code>consolehelper</code>	Определяет права доступа к инструменту <code>consolehelper</code> (<code>/usr/lib/consolehelper/priv/auth</code>), который позволяет пользователям консоли запускать системные программы, выполняя аутентификацию через PAM. Когда это возможно, аутентификация выполняется графически; в противном случае выполняется в текстовой консоли, с которой был запущен <code>consolehelper</code>	«Любой пользователь» – любой пользователь может использовать <code>consolehelper</code> . «Только wheel» – только члены группы «wheel» могут использовать команду <code>consolehelper</code> . «Только root» – только суперпользователь (root) может использовать <code>consolehelper</code>

Продолжение таблицы 30

Политика	Control	Описание	Режимы
Выполнение программы <code>/usr/bin/chsh</code>	<code>chsh</code>	Политика позволяет управлять правами доступа к команде <code>chsh</code> (<code>/usr/bin/chsh</code>). Команда <code>chsh</code> позволяет изменить командную оболочку (или интерпретатор командной строки), запускаемую по умолчанию при регистрации пользователя в текстовой консоли (по умолчанию используется <code>/bin/bash</code>). Обычный пользователь может изменить командную оболочку только для своей учетной записи (командная оболочка должна быть перечислена в файле <code>/etc/shells</code>). Суперпользователь может изменить настройки для любой учетной записи (могут быть указаны любые значения)	«Только root» – только суперпользователь (root) может выполнить <code>/usr/bin/chsh</code> . «Все пользователи» – любой пользователь может использовать команду <code>/usr/bin/chsh</code>
Выполнение программы <code>usr/bin/gpasswd</code>	<code>gpasswd</code>	Определяет права на запуск инструмента <code>/usr/bin/gpasswd</code>	«Любой пользователь» – любой пользователь может выполнить <code>/usr/bin/gpasswd</code> . «Только wheel» – только члены группы «wheel» могут выполнять <code>/usr/bin/gpasswd</code> . «Только root» – только суперпользователь (root) может выполнить <code>/usr/bin/gpasswd</code>
Создание временных каталогов	<code>ram_mktemp</code>	Определяет, следует ли создавать отдельные временные каталоги для пользователей	«Отключено» – отключить создание отдельных временных каталогов для пользователей. «Включено» – включить создание отдельных временных каталогов для пользователей

Продолжение таблицы 30

Политика	Control	Описание	Режимы
Выполнение программы <code>usr/bin/groupmems</code>	<code>groupmems</code>	Определяет права на выполнение программы <code>/usr/bin/groupmems</code>	«Любой пользователь» – любой пользователь может выполнить <code>/usr/bin/groupmems</code> . «Только wheel» – только члены группы «wheel» могут выполнять команду <code>/usr/bin/groupmems</code> . «Только root» – только суперпользователь (root) может выполнить <code>/usr/bin/groupmems</code>
Выполнение программы <code>usr/sbin/hddtemp</code>	<code>groupmems</code>	Разрешение на использование инструмента <code>usr/sbin/hddtemp</code> – отслеживание температуры жесткого диска	«Любой пользователь» – любой пользователь может выполнить <code>usr/sbin/hddtemp</code> . «Только wheel» – только члены группы «wheel» могут выполнять <code>usr/sbin/hddtemp</code> . «Только root» – только суперпользователь (root) может выполнить <code>usr/sbin/hddtemp</code>
Разрешения для <code>usr/bin/newgrp</code>	<code>newgrp</code>	Разрешение на использование инструмента <code>/usr/bin/newgrp</code>	«Любой пользователь» – любой пользователь может выполнить <code>/usr/bin/newgrp</code> . «Только wheel» – только члены группы «wheel» могут выполнять <code>/usr/bin/newgrp</code> . «Только root» – только суперпользователь (root) может выполнить <code>/usr/bin/newgrp</code>

Продолжение таблицы 30

Политика	Control	Описание	Режимы
Управление паролями с помощью passwd	Passwd	Определяет политику управления паролями с помощью команды /usr/bin/passwd	«ТСВ» – любой пользователь может изменить свой пароль, используя /usr/bin/passwd, когда включена схема tcb. «Традиционный (схема tcb отключена)» – любой пользователь может изменить свой пароль, используя /usr/bin/passwd, когда схема tcb отключена. «Только root» – только суперпользователь (root) имеет право изменять пароли пользователей
Управление проверками сложности пароля	passwdqc-enforce	Политика управляет паролями для достаточной надежности пароля	«Все» – включить проверку сложности пароля для всех пользователей. «Только для пользователей» – включить проверку сложности пароля для всех пользователей, кроме суперпользователей
Разрешения для /bin/su	su	Определяет разрешения для /bin/su	«Любой пользователь» – любой пользователь может запускать /bin/su. «Все пользователи, кроме root» – любой пользователь может запускать /bin/su, но только пользователи группы «wheel» могут повышать привилегии суперпользователя. «Только wheel» – только пользователи из группы «wheel» могут запускать /bin/su. «Только root» – только суперпользователь (root) может запускать /bin/su

Продолжение таблицы 30

Политика	Control	Описание	Режимы
Разрешения для /usr/bin/sudo	sudo	Определяет разрешения для /usr/bin/sudo	«Любой пользователь» – любой пользователь может запускать /usr/bin/sudo. «Только wheel» – только пользователи из группы «wheel» могут запускать /usr/bin/sudo. «Только root» – только суперпользователь (root) может запускать /usr/bin/sudo
Режим передачи родительской среды в sudo	sudoers	Определяет, передаются ли переменные среды в sudo	«Строгий» – не передавать переменные окружения дочернему процессу. «Слабый» – передать переменные окружения дочернему процессу
Разрешения для /usr/bin/sudo replay	sudoreplay	Определяет разрешения для /usr/bin/sudo replay	«Любой пользователь» – любой пользователь может запускать /usr/bin/sudo replay. «Только wheel» – только пользователи из группы «wheel» могут запускать /usr/bin/sudo replay. «Только root» – только суперпользователь (root) может запускать /usr/bin/sudoreplay
Разрешить команду sudo членам группы «wheel»	sudowheel	Эта политика разрешает или запрещает членам группы «wheel» применять команду sudo. Если политика включена, пользователи, входящие в группу «wheel» могут повысить системные привилегии через команду sudo. Если политика не настроена или отключена, пользователи, входящие в группу «wheel» не смогут применить команду sudo	«Отключено» – пользователи группы «wheel» не могут повысить привилегии через команду sudo. «Включено» – пользователи группы «wheel» могут повысить привилегии через команду sudo

Окончание таблицы 30

Политика	Control	Описание	Режимы
Метод аутентификации	system-auth	Определяет метод аутентификации пользователя	«Winbind» – использовать Winbind для аутентификации. «SSSD» – использовать метод проверки подлинности демона System Security Services
Разрешения для /usr/lib/chkpwd /tcb_chkpwd	tcb_chkpwd	Определяет разрешения для привилегированного помощника /usr/lib/chkpwd/tcb_chkpwd	«Любой пользователь с отключенным tcb» – любой пользователь может быть аутентифицирован с использованием привилегированного помощника /usr/lib/chkpwd/tcb_chkpwd когда отключена схема tcb. «Любой пользователь с включенным tcb» – любой пользователь может аутентифицироваться с помощью привилегированного помощника /usr/lib/chkpwd/tcb_chkpwd если включена схема tcb. «Только root» – только суперпользователь (root) может быть аутентифицирован с помощью /usr/lib/chkpwd/tcb_chkpwd
Разрешения для /usr/bin/write	write	Определяет разрешения для /usr/bin/write	«Любой пользователь» – любой пользователь может запускать /usr/bin/write. «Только root» – только суперпользователь (root) может запускать /usr/bin/write

Т а б л и ц а 31 – Категория «Службы»

Политика	Control	Описание	Режимы
Права доступа и поведение очереди заданий <code>/usr/bin/at</code>	at	Политика позволяет контролировать поведение и права доступа для запуска очереди заданий (права доступа для запуска <code>/usr/bin/at</code>)	«Все пользователи» – всем пользователям разрешено запускать <code>/usr/bin/at</code> . «Только root» – только суперпользователь (root) может запускать <code>/usr/bin/at</code> . «Режим совместимости» – режим «atdaemon» (не должен использоваться)
Режим демона NTP Chrony	chrony	Политика определяет режим работы (конфигурацию) демона Chrony, который реализует функции сетевого протокола времени	«Сервер» – в файл конфигурации будет добавлена директива «allow all». «Клиент» – директива «allow» в файле конфигурации демона будет закомментирована
Разрешение на использование crontab	crontab	Политика определяет права доступа к инструменту crontab (<code>/usr/bin/crontab</code>)	«Любой пользователь» – любой пользователь может использовать <code>/usr/bin/crontab</code> . «Только root» – только суперпользователь (root) может использовать <code>/usr/bin/crontab</code>
Режим CUPS	cups	Политика определяет поведение CUPS	«Внешний интерфейс IPP» – внешний интерфейс IPP доступен для пользователя. «Только локальные утилиты» – только локальные утилиты могут работать с CUPS
Обратный поиск DNS для запросов OpenLDAP	ldap-reverse-dns-lookup	Политика определяет, разрешен ли обратный поиск DNS для запросов OpenLDAP	«Разрешить» – выполнять обратный поиск DNS для запросов OpenLDAP. «Не разрешать» – не выполнять обратный поиск DNS для запросов OpenLDAP. «По умолчанию» – выполнять обратный поиск DNS для запросов OpenLDAP

Продолжение таблицы 31

Политика	Control	Описание	Режимы
Проверка сертификата при установлении соединений TLS OpenLDAP	ldap-tls-cert-check	Политика определяет режим проверки сертификата при установке TLS соединений OpenLDAP	«По умолчанию» – установить соединение только с правильным сертификатом. «Разрешить» – установить соединение, даже если сертификат отсутствует или неверный. «Пробовать» – установить соединение, если нет или с действующим сертификатом. «Требовать» – установить соединение только с правильным сертификатом. «Никогда» – не выполнять никаких проверок
Режим работы Postfix MTA	postfix	Политика определяет режим работы MTA Postfix (почтовый транспортный агент)	«Локальный (отключен)» – Postfix MTA отключен. «Сервер (фильтры отключены)» – Postfix MTA включен без почтовых фильтров. «Фильтр» – Postfix MTA включен с почтовыми фильтрами
Разрешения для /usr/bin/postqueue	postqueue	Определяет разрешения для /usr/bin/postqueue	«Любой пользователь» – любому пользователю разрешено запускать /usr/bin/postqueue. «Группа mailadm» – пользователям из группы «mailadm» разрешено запускать /usr/bin/postqueue. «Только root» – только суперпользователю (root) разрешено запускать /usr/bin/postqueue
Режим работы Rpcbind	rpcbind	Политика определяет режим работы rpcbind (/sbin/rpcbind)	«Сервер» – rpcbind будет прослушивать входящие соединения из сети. «Локальный» – rpcbind будет принимать только локальные запросы
Поддержка SFTP на сервере OpenSSH	sftp	Политика определяет поддержку SFTP на сервере OpenSSH	«Включено» – включить поддержку SFTP на сервере OpenSSH. «Отключено» – отключить поддержку SFTP на сервере OpenSSH

Продолжение таблицы 31

Политика	Control	Описание	Режимы
Поддержка аутентификации OpenSSH-клиентов через GSSAPI	ssh-gssapi-auth	Эта политика определяет функциональные возможности поддержки аутентификации OpenSSH-клиентов через GSSAPI	«Включено» – поддержка аутентификации через GSSAPI для OpenSSH-клиентов включена. «Отключено» – поддержка аутентификации через GSSAPI для OpenSSH-клиентов отключена
Samba опции			
Гостевой доступ к общим каталогам	smb-conf-usershare-allow-guests	Политика управляет возможностью предоставления гостевого доступа общему ресурсу. Данная политика управляет параметром <code>usershare allow guests</code> в файле <code>/etc/samba/usershares.conf</code> .	«Включено» – разрешить предоставление гостевого доступа к общему ресурсу; разрешить создание общих каталогов с параметром доступа без авторизации (<code>usershare allow guests = yes</code>). «Отключено» – запретить предоставление гостевого доступа к общему ресурсу; запретить создание общих каталогов с параметром доступа без авторизации (<code>usershare allow guests = no</code>)
Доступ к общим каталогам других пользователей	smb-conf-usershare-owner-only	Политика управляет правом пользователя на предоставление общего доступа или доступ к каталогу, если пользователь не является владельцем этого каталога. Данная политика управляет параметром <code>usershare owner only</code> в файле <code>/etc/samba/usershares.conf</code> .	«Включено» – запретить предоставление общего доступа не владельцу каталога; запретить доступ к общим каталогам пользователей, без проверки владельца каталога (<code>usershare owner only = yes</code>). «Отключено» – разрешить предоставление общего доступа не владельцу каталога; разрешить доступ к общим каталогам пользователей, без проверки владельца каталога (<code>usershare owner only = no</code>)

Продолжение таблицы 31

Политика	Control	Описание	Режимы
Запрет на создание общих каталогов в системных каталогах	smb-conf-usershare-deny-list	<p>Данная политика управляет параметром <code>usershare prefix deny list</code> в файле <code>/etc/samba/usershares.conf</code> – открывая или закрывая комментарием этот параметр.</p> <p>Параметр <code>usershare prefix deny list</code> определяет каталоги в корневом каталоге (<code>/</code>), в которых пользователю запрещено создавать общие каталоги. Если абсолютный путь к общему каталогу пользователя начинается с одного из перечисленных каталогов, то доступ к нему будет запрещен. Таким образом ограничивается список каталогов, в которых возможно создавать общие пользовательские каталоги. По умолчанию в параметре <code>usershare prefix deny list</code> заданы каталоги: <code>/etc, /dev, /sys, /proc</code>.</p> <p>Если настроен список запрещенных каталогов <code>usershare prefix deny list</code>, и список разрешенных каталогов <code>usershare prefix allow list</code>, сначала обрабатывается список запрета, а затем уже список разрешений.</p>	<p>«Включено» – включить список запрещенных каталогов (параметр <code>usershare prefix deny list</code> будет раскомментирован).</p> <p>«Отключено» – отключить список запрещенных каталогов (параметр <code>usershare prefix deny list</code> будет закоментирован)</p>

Продолжение таблицы 31

Политика	Control	Описание	Режимы
Разрешение на создание общих каталогов в системных каталогах	smb-conf-usershare-allow-list	<p>Данная политика управляет параметром <code>usershare prefix allow list</code> в файле <code>/etc/samba/usershares.conf</code> – открывая или закрывая комментарием этот параметр.</p> <p>Параметр <code>usershare prefix allow list</code> определяет каталоги в корневом каталоге (<code>/</code>), в которых пользователю разрешено создавать общие каталоги. Если абсолютный путь к общему каталогу пользователя не начинается с одного из перечисленных каталогов, то доступ к нему будет запрещен. Таким образом ограничивается список каталогов, в которых возможно создавать общие пользовательские каталоги. По умолчанию в параметре <code>usershare prefix allow list</code> заданы каталоги: <code>/home, /srv, /mnt, /media, /var</code>.</p> <p>Если настроен список запрещенных каталогов <code>usershare prefix deny list</code>, и список разрешенных каталогов <code>usershare prefix allow list</code>, сначала обрабатывается список запрета, а затем уже список разрешений.</p>	<p>«Включено» – включить список разрешенных каталогов (параметр <code>usershare prefix allow list</code> будет раскомментирован).</p> <p>«Отключено» – отключить список разрешенных каталогов (параметр <code>usershare prefix allow list</code> будет закомментирован)</p>

Продолжение таблицы 31

Политика	Control	Описание	Режимы
Доступ членам группы «sambashare» к управлению общими каталогами	role-sambashare	Политика управляет разрешением членам группы «sambashare» управлять общими каталогами. Конфигурации пользовательских общих ресурсов расположены в каталоге /var/lib/samba/usershares, права на запись в котором имеют члены группы «usershares». Данная политика позволяет расширить привилегии членов группы «sambashare», добавляя их в группу «usershares».	«Включено» – разрешить членам группы «sambashare» управлять общими каталогами. «Отключено» – запретить членам группы «sambashare» управлять общими каталогами
Доступ членам группы «users» к управлению общими каталогами	role-usershares	Политика управляет разрешением членам группы «users» управлять общими каталогами. Конфигурации пользовательских общих ресурсов расположены в каталоге /var/lib/samba/usershares, права на запись в котором имеют члены группы «usershares». Данная политика позволяет расширить привилегии членов группы «users», добавляя их в группу «usershares».	«Включено» – разрешить членам группы «users» управлять общими каталогами. «Отключено» – запретить членам группы «users» управлять общими каталогами. Данный параметр также влияет на разрешение управления общими каталогами через настройку предпочтений
Разрешение на создание пользовательских общих каталогов	smb-conf-usershare	Политика управляет возможностью создания пользовательских общих каталогов на компьютере.	«Включено» – включить возможность создания и использования общих каталогов пользователей (usershare max shares = 100).

Продолжение таблицы 31

Политика	Control	Описание	Режимы
		Данная политика управляет параметром <code>usershare max shares</code> в файле <code>/etc/samba/usershare s.conf</code> , который устанавливает предельное число общих каталогов.	«Отключено» – отключить возможность создания и использования общих каталогов пользователей (<code>usershare max shares = 0</code>)
SSHD опции			
Контроль доступа по группам к серверу OpenSSH	<code>ssh-gssapi-auth</code>	Эта политика включает в службе удаленного доступа OpenSSH контроль доступа по списку разрешенных групп	«Включено» – контроль доступа по группам для службы удаленного доступа OpenSSH включен. «Отключено» – контроль доступа по группам для службы удаленного доступа OpenSSH отключен
Группы для контроля доступа к серверу OpenSSH	<code>sshd-allow-groups-list</code>	Эта политика определяет, какие группы входят в список разрешенных для службы удаленного доступа к серверу OpenSSH	«Все пользователи» – разрешить доступ к серверу OpenSSH для групп «wheel» и «users». «Группы wheel и remote» – разрешить доступ к серверу OpenSSH для групп администраторов и пользователей удаленного доступа («wheel» и «remote») «Только wheel» – разрешить доступ к серверу OpenSSH только для группы администраторов («wheel») «Только remote» – разрешить доступ к серверу OpenSSH только для группы «remote»
Поддержка GSSAPI-аутентификации на сервере OpenSSH	<code>sshd-gssapi-auth</code>	Эта политика включает поддержку аутентификации с использованием GSSAPI на сервере OpenSSH	«Включено» – поддержка GSSAPI на сервере OpenSSH включена. «Отключено» – поддержка GSSAPI на сервере OpenSSH отключена

Продолжение таблицы 31

Политика	Control	Описание	Режимы
Аутентификация по паролю на сервере OpenSSH	sshd-password-auth	Эта политика включает поддержку аутентификации по паролю на сервере OpenSSH	«Включено» – поддержка аутентификации по паролю на сервере OpenSSH включена. «Отключено» – поддержка аутентификации по паролю на сервере OpenSSH отключена
Аутентификация суперпользователя на сервере OpenSSH	sshd-permit-root-login	Эта политика определяет режимы аутентификации для суперпользователя (root) на сервере OpenSSH	«Только без пароля» – суперпользователю разрешена только беспарольная аутентификация на сервере OpenSSH. «Разрешено» – суперпользователю разрешена аутентификация на сервере OpenSSH. «Запрещено» – суперпользователю запрещена аутентификация на сервере OpenSSH. «По умолчанию» – сбросить режим аутентификации для суперпользователя на значение по умолчанию в пакете
SSSD опции			
Игнорирование политик при недоступности GPT	sssd-ad-gpo-ignore-unreadable	Эта настройка определяет будут ли проигнорированы правила управления доступом в SSSD основанные на групповых политиках, если недоступен какой-либо шаблон (GPT) объекта групповой политики (GPO)	«Включить» – игнорировать правила управления доступом через групповые политики, если шаблоны групповых политик не доступны для SSSD. «Отключить» – запретить доступ пользователям SSSD AD, которым назначены групповые политики, если шаблоны групповых политик не доступны. «По умолчанию» – настройка игнорирования политик, при недоступности шаблонов групповых политик сброшена на значение по умолчанию в пакете

Продолжение таблицы 31

Политика	Control	Описание	Режимы
Контроль доступа в SSSD через групповые политики	sssd-ad-gpo-access-control	Эта политика определяет в каком режиме будет осуществляться контроль доступа в SSSD основанный на групповых политиках Active Directory (GPO)	<p>«Принудительный режим» – правила управления доступом в SSSD основанные на GPO выполняются, ведется логирование.</p> <p>«Разрешающий режим» – правила управления доступом в SSSD основанные на GPO не выполняются, ведется только логирование. Такой режим требуется администратору, чтобы оценить, как срабатывают новые правила.</p> <p>«Отключить» – правила управления доступом в SSSD основанные на GPO не логируются и не выполняются.</p> <p>«По умолчанию» – настройка контроля доступа в SSSD основанное на GPO сброшено на значение по умолчанию в пакете</p>
Кэширование учетных данных пользователей	sssd-cache-credentials	Эта политика определяет, будут ли учетные данные удаленных пользователей сохраняться в локальном кеше SSSD	<p>«Включить» – сохранение в локальном кеше SSSD учетных данных пользователей включено.</p> <p>«Отключить» – сохранение в локальном кеше SSSD учетных данных пользователей отключено.</p> <p>«По умолчанию» – настройка сохранения в локальном кеше SSSD учетных данных пользователей сброшена на значение по умолчанию в пакете</p>

Окончание таблицы 31

Политика	Control	Описание	Режимы
Режим привилегий службы SSSD	sssd-drop-privileges	Эта политика позволяет сбросить права службы SSSD, чтобы избежать работы от имени суперпользователя (root)	«Привилегированный» – служба SSSD запущена от имени привилегированного суперпользователя (root). «Непривилегированный» – служба SSSD запущена от имени непривилегированного пользователя (_sssd). «По умолчанию» – режим привилегий службы SSSD задан по умолчанию в пакете
Обновление DNS-записей прямой зоны	sssd-dyndns-update	Эта политика позволяет включить или отключить автоматическое обновление DNS-записей (защищенных с помощью GSS-TSIG) с IP-адресом клиента через SSSD	«Включить» – автоматическое обновление DNS-записи клиента через SSSD включено. «Отключить» – автоматическое обновление DNS-записи клиента через SSSD отключено. «По умолчанию» – настройка автоматического обновления DNS-записи клиента через SSSD задана по умолчанию в пакете
Обновление DNS-записей обратной зоны	sssd-dyndns-update-ptr	Данная политика определяет, будет ли обновляться клиентская PTR-запись (защищенная с помощью GSS-TSIG). Эта политика работает, только если включено «Обновление DNS-записей прямой зоны»	«Включить» – автоматическое обновление DNS-записи обратной зоны через SSSD включено. «Отключить» – автоматическое обновление DNS-записи обратной зоны через SSSD отключено. «По умолчанию» – настройка автоматического обновления DNS-записи обратной зоны задана по умолчанию в пакете

Т а б л и ц а 32 – Категория «Сетевые приложения»

Политика	Control	Описание	Режимы
Разрешение на использование <code>/usr/bin/mtr</code>	mtr	Разрешение на использование сетевого инструмента <code>/usr/bin/mtr</code>	«Любой пользователь» – любой пользователь может выполнить <code>/usr/bin/mtr</code> . «Группа netadmin» – только члены группы «netadmin» могут выполнять <code>/usr/bin/mtr</code> . «Только root» – только суперпользователь (root) может выполнить <code>/usr/bin/mtr</code>
Разрешения для <code>/usr/bin/ping</code>	ping	Эта политика определяет разрешения для <code>/usr/bin/ping</code>	«Любой пользователь» – любой пользователь может запускать <code>/usr/bin/ping</code> . «Группа netadmin» – пользователям из группы «netadmin» разрешено запускать <code>/usr/bin/ping</code> . «Только root» – только суперпользователь (root) может запускать <code>/usr/bin/ping</code> . «Любой пользователь (в контейнерах)» – любой пользователь может запускать <code>/usr/bin/ping</code> (в контейнерах). «Группа netadmin (в контейнерах)» – пользователям из группы «netadmin» разрешено запускать <code>/usr/bin/ping</code> (в контейнерах)
Разрешения для <code>/usr/sbin/pppd</code>	ppp	Эта политика определяет разрешения для <code>/usr/sbin/pppd</code>	«Только root» – только суперпользователю (root) разрешено запускать <code>/usr/sbin/pppd</code> . «Традиционный» – любой пользователь имеет право запустить <code>/usr/sbin/pppd</code> без повышения привилегий. «Группа uusr» – пользователям из группы «uusr» имеют право запускать <code>/usr/sbin/pppd</code> с правами суперпользователя. «Любой пользователь» – любой пользователь имеет право запускать <code>/usr/sbin/pppd</code> с правами суперпользователя
Разрешения для wireshark-capture (<code>dumpcap</code>)	wireshark-capture	Эта политика определяет функциональные возможности (режимы) разрешения для захвата wireshark (<code>/usr/bin/dumpcap</code>)	«Любой пользователь» – любой пользователь имеет право запустить <code>/usr/bin/dumpcap</code> , захват трафика включен. «Любой пользователь, без захвата трафика» – любой пользователь имеет право запустить <code>/usr/bin/dumpcap</code> , захват трафика отключен. «Группа netadmin» – пользователям из группы «netadmin» имеют право запускать <code>/usr/bin/dumpcap</code> . «Только root» – только суперпользователь (root) может запускать <code>/usr/bin/dumpcap</code>

Т а б л и ц а 33 – Категория «Приложения для CD/DVD»

Политика	Control	Описание	Режимы
Разрешение на использование /usr/bin/dvd-ram-control	dvd-ram-control	Эта политика определяет права доступа к /usr/bin/dvd-ram-control	«Только cdwriter» – только члены группы «cdwriter» могут выполнять /usr/bin/dvd-ram-control. «Только root» – только суперпользователь (root) может выполнять /usr/bin/dvd-ram-control. «Режим совместимости» – режим совместимости, не должен использоваться
Разрешения на использование /usr/bin/dvd+rw-booktype	dvd+rw-booktype	Эта политика определяет права доступа к /usr/bin/dvd+rw-booktype	«Только cdwriter» – только члены группы «cdwriter» могут выполнять /usr/bin/dvd+rw-booktype. «Только root» – только суперпользователь (root) может выполнять /usr/bin/dvd+rw-booktype. «Режим совместимости» – режим совместимости, не должен использоваться
Разрешения на использование /usr/bin/dvd+rw-format	dvd+rw-format	Эта политика определяет права доступа к /usr/bin/dvd+rw-format	«Только cdwriter» – только члены группы «cdwriter» могут выполнять /usr/bin/dvd+rw-format. «Только root» – только суперпользователь (root) может выполнять /usr/bin/dvd+rw-format. «Режим совместимости» – режим совместимости, не должен использоваться
Разрешения на использование /usr/bin/dvd+rw-mediainfo	dvd+rw-mediainfo	Эта политика определяет права доступа к /usr/bin/dvd+rw-mediainfo	«Только cdwriter» – только члены группы «cdwriter» могут выполнять /usr/bin/dvd+rw-mediainfo. «Только root» – только суперпользователь (root) может выполнять /usr/bin/dvd+rw-mediainfo. «Режим совместимости» – режим совместимости, не должен использоваться
Разрешения на использование /usr/bin/growisofs	growisofs	Эта политика определяет права на использование инструмента /usr/bin/growisofs	«Только cdwriter» – только члены группы «cdwriter» могут выполнять /usr/bin/growisofs. «Только root» – только суперпользователь (root) может выполнять /usr/bin/growisofs. «Режим совместимости» – режим совместимости, не должен использоваться

Т а б л и ц а 34 – Категория «Монтирование»

Политика	Control	Описание	Режимы
Доступ к инструментам FUSE	fusermount	Эта политика определяет права доступа для монтирования файловой системы FUSE (выполнение программ /usr/bin/fusermount и /usr/bin/fusermount3)	«Любой пользователь» – любой пользователь может выполнить /usr/bin/fusermount и /usr/bin/fusermount3. «Только fuse» – только члены группы «fuse» могут выполнять /usr/bin/fusermount и /usr/bin/fusermount3. «Только wheel» – только члены группы «wheel» могут выполнять /usr/bin/fusermount и /usr/bin/fusermount3. «Только root» – только суперпользователь (root) может выполнить /usr/bin/fusermount и /usr/bin/fusermount3
Разрешения для /bin/mount и /bin/umount	mount	Эта политика определяет разрешения для /bin/mount и /bin/umount	«Любой пользователь» – любому пользователю разрешено запускать /bin/mount и /bin/umount. «Группа wheel» – пользователям из группы «wheel» разрешено запускать /bin/mount и /bin/umount. «Непривилегированный пользователь» – любой пользователь может запускать /bin/mount и /bin/umount для непривилегированных действий (не от имени root). «Только root» – только суперпользователь (root) может запускать /bin/mount и /bin/umount
Разрешения для /sbin/mount.nfs	nfsmount	Эта политика определяет разрешения для /sbin/mount.nfs	«Любой пользователь» – любому пользователю разрешено запускать /sbin/mount.nfs «Только wheel» – пользователям из группы «wheel» разрешено запускать /sbin/mount.nfs «Только root» – только суперпользователю (root) может запускать /sbin/mount.nfs
Правила подключения USB-накопителей	udisks2	Эта политика определяет правила подключения USB-накопителей	«По умолчанию» – подключить накопитель индивидуально (/run/media/\$user/) для каждого пользователя. «Общий» – подключить накопитель к общедоступной точке (/media/)

Т а б л и ц а 35 – Категория «Виртуализация»

Политика	Control	Описание	Режимы
Разрешения для VirtualBox	virtualbox	Эта политика определяет разрешения для VirtualBox	«Любой пользователь» – любому пользователю разрешено использовать VirtualBox. «Группа vboxusers» – пользователям из группы «vboxusers» разрешено использовать VirtualBox. «Только root» – только суперпользователю (root) разрешено использовать VirtualBox

Т а б л и ц а 36 – Категория «Графическая подсистема»

Политика	Control	Описание	Режимы
Список пользователей в greeter (LightDM)	lightdm-greeter-hide-users	Эта политика определяет, будет ли показан список всех пользователей при входе в систему с помощью LightDM (в greeter – на экране приветствия/входа в систему LightDM) или нет	«Показать» – показать список доступных пользователей в greeter. «Скрыть» – не перечислять всех пользователей в greeter
Стандартные каталоги в home	xdg-user-dirs	Эта политика определяет, работает ли функция стандартных каталогов (Документы, Загрузки, Изображения и т. д.) xdg-user-dirs в домашнем каталоге (home) пользователя	«Отключено» – функция сохранения списка пользовательских каталогов отключена. «Группа vboxusers» – функция сохранения списка пользовательских каталогов включена
Разрешения для Xorg	xorg-server	Эта политика определяет разрешения для Xorg (/usr/bin/Xorg)	«Любой пользователь» – всем разрешено запускать /usr/bin/Xorg. «Группа xgr» – пользователям группы «xgr» разрешено запускать /usr/bin/Xorg. «Только root» – только суперпользователь (root) может запускать /usr/bin/Xorg

10.4.6.4.3. Управление настройками службы Polkit

Через групповые политики реализовано управление настройками службы Polkit (PolicyKit).

В настоящий момент реализованы следующие настройки:

- ограничения службы Login – формирование правил PolKit для управления службой Login;
- ограничения службы Machine – формирование правил PolKit для управления службой Machine;

- ограничения Udisks2 – формирование правил PolKit для монтирования файловых систем (демон udisk2);
- ограничения PackageKit – формирование правил PolKit для установки, удаления, обновления пакетов;
- ограничения Realmd – формирование правил PolKit для управления службой Realmd;
- ограничения NetworkManager – формирование правил PolKit для операций с сетевыми подключениями и настройкой сетевых интерфейсов;
- ограничения ModemManager – формирование правил PolKit для операций с ModemManager (взаимодействие с модемом или мобильным телефоном);
- ограничения для работы с токенами и смарт-картами – формирование правил PolKit для работы с токенами и смарт-картами.

Для настройки политики следует перейти в «Компьютер»/«Пользователь» → «Административные шаблоны» → «Система ALT» → «Правила Polkit». В этом разделе есть несколько подразделов (рис. 382).

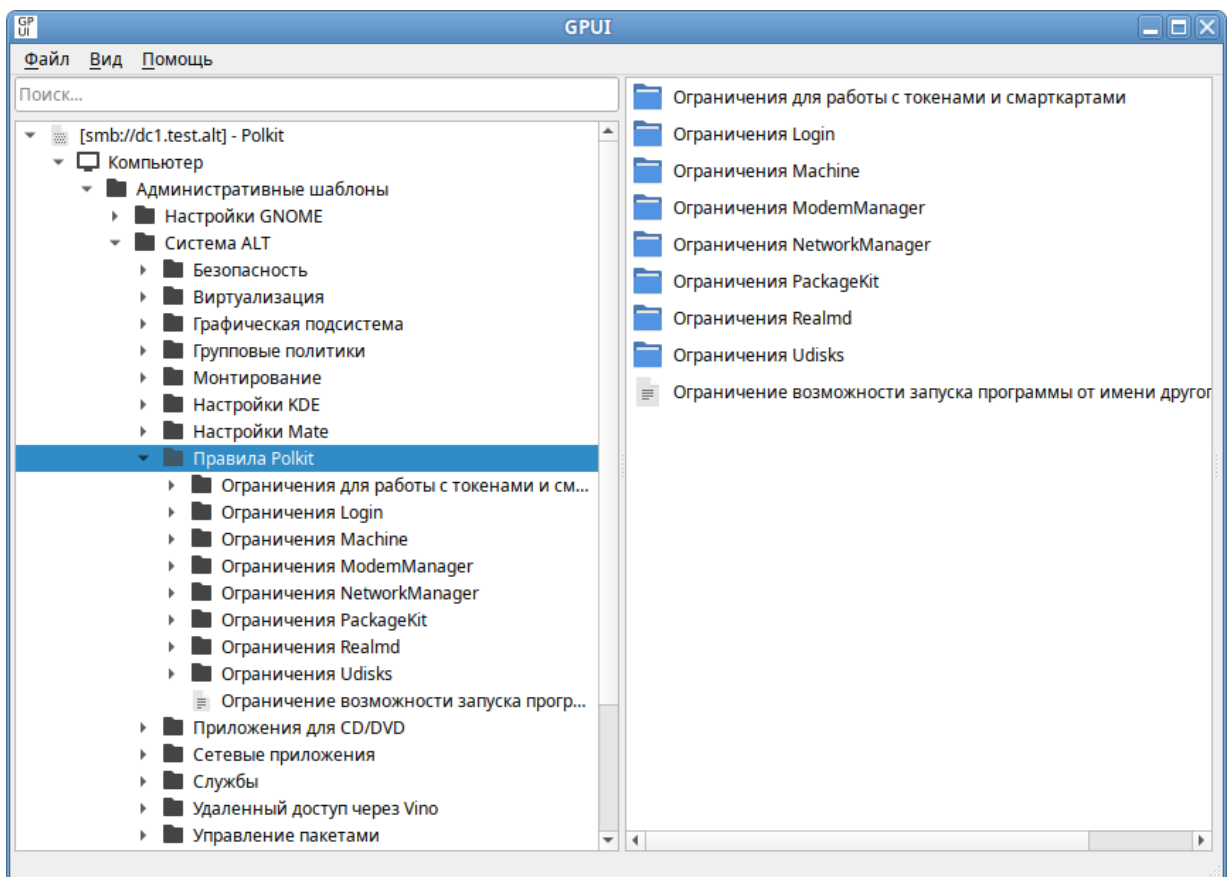


Рис. 382 – Список разделов Polkit

При выборе раздела, в правом окне редактора отобразится список политик (рис. 383).

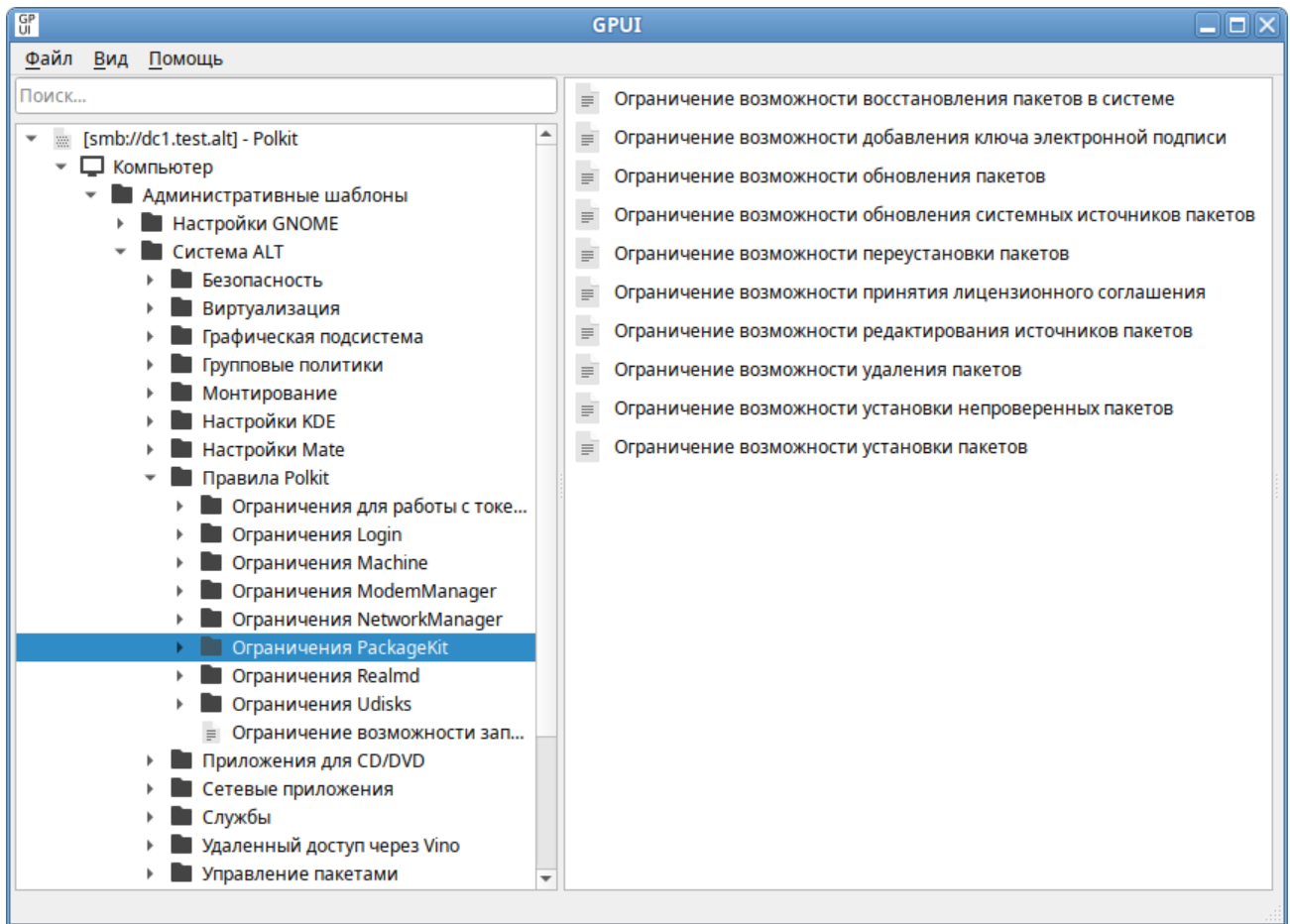


Рис. 383 – Список политик PackageKit

При выборе политики, откроется диалоговое окно настройки политики (рис. 384).

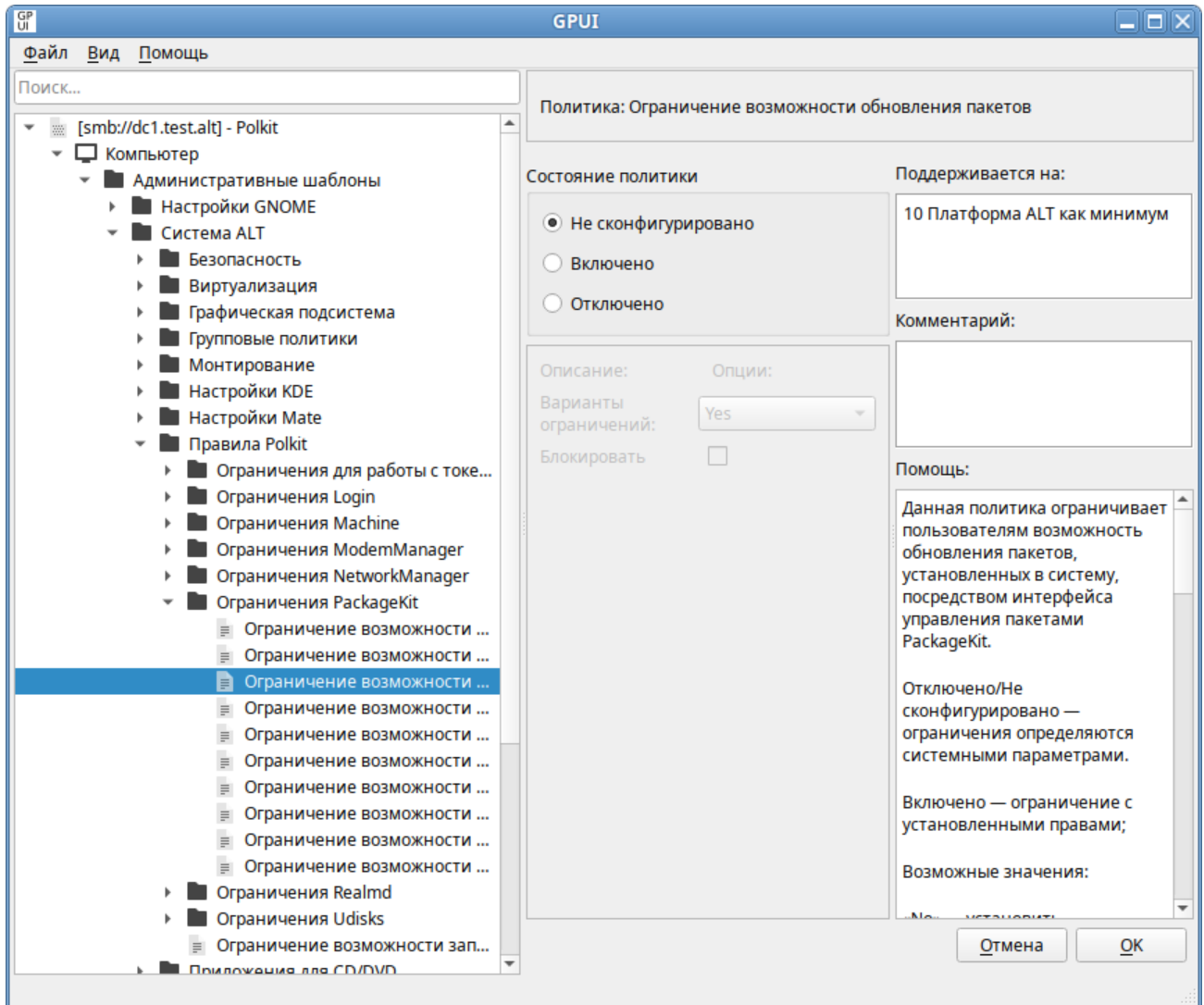


Рис. 384 – Диалоговое окно настройки ограничения Polkit

Можно не задавать настройку политики, включить или отключить. Если политика находится в состоянии «Отключено»/«Не сконфигурировано» разрешения определяются системными параметрами (по умолчанию – «Auth_admin»). Если выбрать параметр «Включено», в разделе «Опции» в выпадающем списке можно выбрать вариант ограничения для данного разрешения (рис. 385).

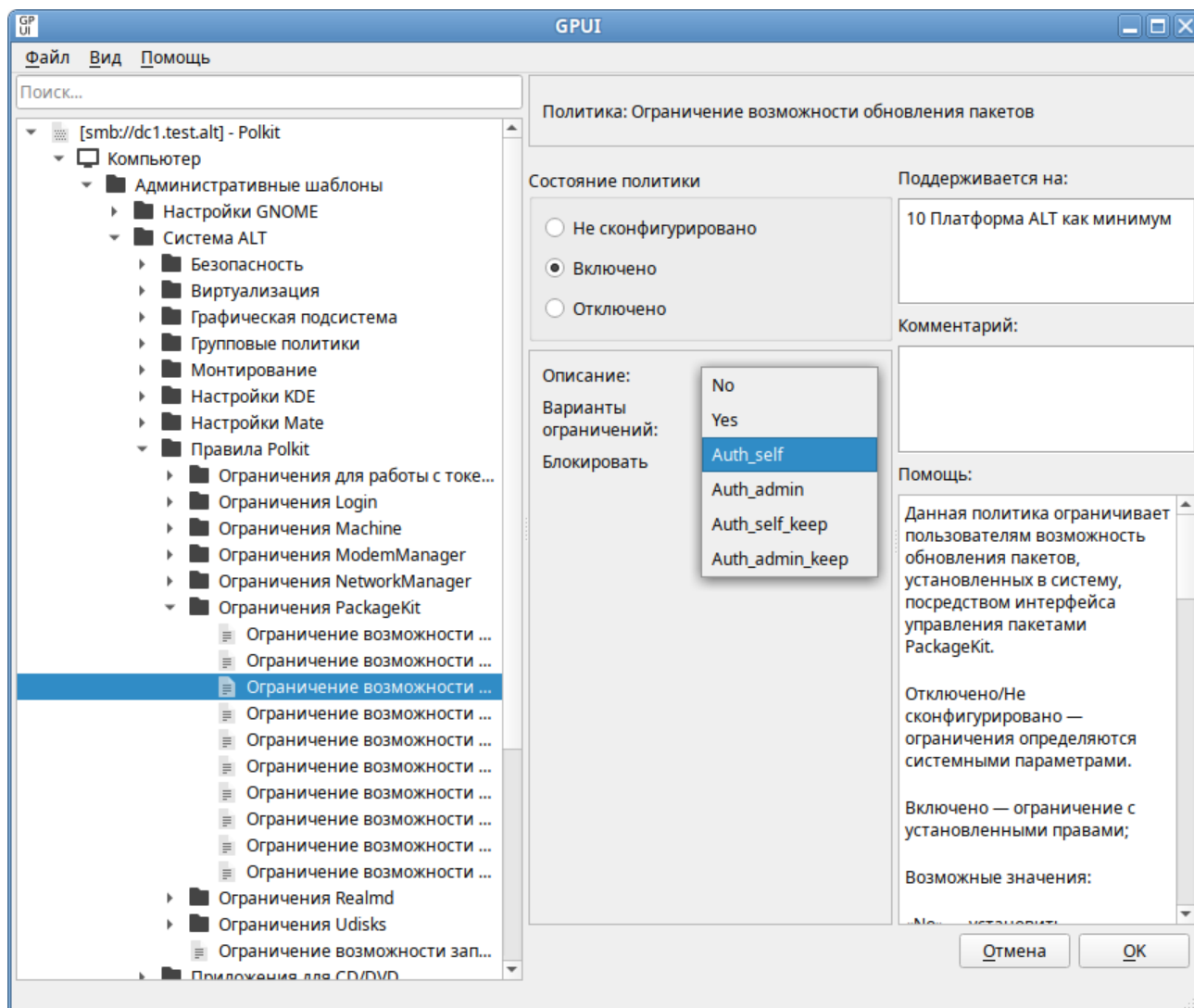


Рис. 385 – Настройка ограничения Polkit

Если выбран параметр «Включено», для каждой из этих политик доступны следующие разрешения:

- «No» – установить ограничение с запретом действия (пользователю не разрешено выполнять действие);
- «Yes» – снять ограничение (пользователь может выполнять действие без какой-либо аутентификации);
- «Auth_self» – пользователь должен ввести свой пароль для аутентификации.

Следует обратить внимание, что этого уровня ограничения недостаточно для большинства применений в многопользовательских системах, обычно рекомендуется ограничение «Auth_admin»;

- «Auth_admin» – пользователь должен ввести пароль администратора при каждом запросе. Требуется аутентификация пользователя с правами администратора;
- «Auth_self_keep» – подобно «Auth_self», но авторизация сохраняется в течение короткого периода времени (например, пять минут). Следует обратить внимание, что этого ограничения недостаточно для большинства применений в многопользовательских системах, обычно рекомендуется ограничение «Auth_admin_keep»;
- «Auth_admin_keep» – аналогично «Auth_admin», но авторизация сохраняется в течение короткого периода времени (например, пять минут).

Примечание. Администратор – в ОС Альт СП определен в правиле `/etc/polkit-1/rules.d/50-default.rules`:

```
polkit.addAdminRule(function(action, subject) {
    return ["unix-group:wheel"];
});
```

По умолчанию запрашивается пароль пользователя, находящегося в группе `wheel`.

Для машинной политики создается файл правил `49-alt_group_policy_permissions.rules`, для пользовательской политики – `48-alt_group_policy_permissions_user.<USERNAME>.rules`. Правила для пользовательской политики обрабатываются до правил для машинной политики. У машинных политик имеются блокировки (параметр «Блокировать»), при установке которых машинные политики становятся приоритетнее пользовательских (создается файл правил `47-alt_group_policy_permissions.rules`).

Все настройки политики управления политиками Polkit хранятся в файлах `{GUID GPT}/Machine/Registry.pol` и `{GUID GPT}/User/Registry.pol`.

Пример файла `Registry.pol`:

```
PReg
[Software\BaseALT\Policies\PolkitLocks;org.freedesktop.udisks2.filesystem-mount;;;]
[Software\BaseALT\Policies\Polkit;org.freedesktop.udisks2.filesystem-mount;;;No]
```

```
[Software\BaseALT\Policies\Polkit;org.freedesktop.packagekit.system-
update;;;Auth_self]
[Software\BaseALT\Policies\PolkitLocks;org.freedesktop.NetworkManager.
network-control;;;]
[Software\BaseALT\Policies\Polkit;org.freedesktop.NetworkManager.netwo
rk-control;;;Yes]
```

10.4.6.4.3.1. Ограничения для работы с токенами и смарт-картами

Список политик, настраивающих ограничения для работы с токенами и смарт-картами приведены в таблице 37.

Т а б л и ц а 37 – Ограничения для работы с токенами и смарт-картами

Политика	Описание	Правило Polkitd
Ограничение возможности доступа к демону PC/SC	Данная политика управляет ограничением возможности доступа к демону PC/SC и регулирует работу с токенами	org.debian.pcsclite.access_pcsclite
Ограничение возможности к смарт-картам	Данная политика управляет ограничением возможности доступа к смарт-картам	org.debian.pcsclite.access_card

10.4.6.4.3.2. Ограничения службы Login

Список политик, настраивающих ограничения службы Login приведены в таблице 38.

Т а б л и ц а 38 – Ограничения службы Login

Политика	Описание	Правило Polkitd
Ограничение возможности блокировки или разблокировки экрана активных сеансов	Политика ограничивает возможность блокировки или разблокировки экрана активных сеансов	org.freedesktop.login1.lock-sessions
Ограничение возможности выключения питания системы	Политика ограничивает возможность выключения питания системы	org.freedesktop.login1.power-off
Ограничение возможности выключения системы, когда приложение запрещает это действие	Политика ограничивает возможность выключения системы, когда приложение запрещает это действие	org.freedesktop.login1.power-off-ignore-inhibit
Ограничение возможности выключения системы, при наличии активных сеансов других пользователей	Политика ограничивает возможность выключения системы, при наличии активных сеансов других пользователей	org.freedesktop.login1.power-off-multiple-sessions

Продолжение таблицы 38

Политика	Описание	Правило Polkitd
Ограничение возможности изменения сеанса виртуального терминала	Политика управляет ограничением возможности изменить сеанс виртуального терминала	org.freedesktop.login1.chvt
Ограничение возможности остановки системы	Политика ограничивает возможность остановки системы	org.freedesktop.login1.halt
Ограничение возможности остановки системы, когда приложение запрещает это действие	Политика ограничивает возможность остановки системы, пока приложение запрещает это действие	org.freedesktop.login1.halt- ignore-inhibit
Ограничение возможности остановки системы, при наличии активных сеансов других пользователей	Политика ограничивает возможность остановки системы, при наличии активных сеансов других пользователей	org.freedesktop.login1.halt- multiple-sessions
Ограничение возможности очистки устройства в месте привязки (изменение способа подключения устройств к рабочим местам)	Политика управляет ограничением возможности очистки устройства в месте привязки (изменение способа подключения устройств к рабочим местам)	org.freedesktop.login1.flush- devices
Ограничение возможности перевода системы в спящий режим	Политика ограничивает возможность перевода системы в спящий режим	org.freedesktop.login1.hibern- ate
Ограничение возможности перевода системы в спящий режим, пока приложение препятствует этому	Политика ограничивает возможность перевода системы в спящий режим, пока приложение препятствует этому	org.freedesktop.login1.hibern- ate- ignore-inhibit
Ограничение возможности перевода системы в спящий режим, при наличии активных сеансов других пользователей	Политика ограничивает возможность перевода системы в спящий режим, при наличии активных сеансов других пользователей	org.freedesktop.login1.hibern- ate- multiple-sessions
Ограничение возможности перезагрузки системы	Политика ограничивает возможность перезагрузки системы	org.freedesktop.login1.reboot
Ограничение возможности перезагрузки системы, когда приложение препятствует этому действию	Политика ограничивает возможность перезагрузки системы, когда приложение препятствует этому действию	org.freedesktop.login1.reboot- ignore-inhibit
Ограничение возможности перезагрузки системы, при наличии активных сеансов других пользователей	Политика ограничивает возможность перезагрузки системы, при наличии активных сеансов других пользователей	org.freedesktop.login1.reboot- multiple-sessions
Ограничение возможности приложениям блокировать выключение системы	Политика ограничивает возможность приложениям блокировать выключение системы	org.freedesktop.login1.inhibit- block-shutdown

Продолжение таблицы 38

Политика	Описание	Правило Polkitd
Ограничение возможности приложениям запрещать автоматическое приостановление работы системы	Политика ограничивает возможность приложениям запрещать автоматическое приостановление работы системы	org.freedesktop.login1.inhibit-block-idle
Ограничение возможности приложениям запрещать низкоуровневую обработку аппаратного ключа гибернации (энергосбережения) системы	Политика ограничивает возможность приложениям запрещать низкоуровневую обработку аппаратного ключа гибернации (энергосбережения) системы	org.freedesktop.login1.inhibit-handle-hibernate-key
Ограничение возможности приложениям запрещать низкоуровневую обработку аппаратного переключателя крышки (устройства)	Политика ограничивает возможность приложениям запрещать низкоуровневую обработку аппаратного переключателя крышки (устройства)	org.freedesktop.login1.inhibit-handle-lid-switch
Ограничение возможности приложениям запрещать низкоуровневую обработку аппаратной клавиши перезагрузки системы	Политика ограничивает возможность приложениям запрещать низкоуровневую обработку аппаратной клавиши перезагрузки системы	org.freedesktop.login1.inhibit-handle-reboot-key
Ограничение возможности приложениям запрещать низкоуровневую обработку аппаратной клавиши питания системы	Политика ограничивает возможность приложениям запрещать низкоуровневую обработку аппаратной клавиши питания системы	org.freedesktop.login1.inhibit-handle-power-key
Ограничение возможности приложениям запрещать низкоуровневую обработку аппаратной клавиши приостановки системы	Политика ограничивает возможность приложениям запрещать низкоуровневую обработку аппаратной клавиши приостановки системы	org.freedesktop.login1.inhibit-handle-suspend-key
Ограничение возможности приложениям запрещать системный сон	Политика ограничивает возможность приложениям запрещать системный сон	org.freedesktop.login1.inhibit-block-sleep
Ограничение возможности приложениям откладывать выключение системы	Политика ограничивает возможность приложениям откладывать выключение системы	org.freedesktop.login1.inhibit-delay-shutdown
Ограничение возможности приложениям откладывать переход в спящий режим	Политика ограничивает возможность приложениям откладывать переход в спящий режим	org.freedesktop.login1.inhibit-delay-sleep
Ограничение возможности приостановки работы системы	Политика ограничивает возможность приостановки работы системы	org.freedesktop.login1.suspend
Ограничение возможности приостановки работы системы, пока приложение препятствует этому действию	Политика ограничивает возможность приостановки работы системы, пока приложение препятствует этому действию	org.freedesktop.login1.suspend-ignore-inhibit

Окончание таблицы 38

Политика	Описание	Правило Polkitd
Ограничение возможности приостановки работы системы, при наличии активных сеансов других пользователей	Политика ограничивает возможность приостановки работы системы, при наличии активных сеансов других пользователей	org.freedesktop.login1.suspend-multiple-sessions
Ограничение возможности присоединения устройств к рабочим местам	Политика управляет ограничением возможности присоединить устройства к рабочим местам	org.freedesktop.login1.attach-device
Ограничение возможности разрешения незалогиненному пользователю запускать программы	Политика ограничивает возможность разрешения незалогиненному пользователю запускать программы	org.freedesktop.login1.set-self-linger
Ограничение возможности разрешения незалогиненным пользователям запускать программы	Политика ограничивает возможность разрешения незалогиненным пользователям запускать программы	org.freedesktop.login1.set-user-linger
Ограничение возможности указания загрузчику системы на загрузку в определенную запись загрузчика	Политика ограничивает возможность указания загрузчику системы на загрузку в определенную запись загрузчика	org.freedesktop.login1.set-reboot-to-boot-loader-entry
Ограничение возможности указания загрузчику системы на необходимость загрузки в меню загрузчика	Политика ограничивает возможность указания загрузчику системы на необходимость загрузки в меню загрузчика	org.freedesktop.login1.set-reboot-to-boot-loader-menu
Ограничение возможности указания микропрограмме системы на необходимость перезагрузки в интерфейс настройки микропрограммы	Политика ограничивает возможность указания микропрограмме системы на необходимость перезагрузки в интерфейс настройки микропрограммы	org.freedesktop.login1.set-reboot-to-firmware-setup
Ограничение возможности управления активными сеансами, пользователями и местами	Политика ограничивает возможность управления активными сеансами, пользователями и местами	org.freedesktop.login1.manage
Ограничение возможности установки «причины» перезагрузки в ядре	Политика ограничивает возможность установить «причины» перезагрузки в ядре	org.freedesktop.login1.set-reboot-parameter
Ограничение возможности установки сообщения на стене (сообщение, которое будет отправлено на все терминалы)	Политика ограничивает возможность установки сообщения на стене (сообщение, которое будет отправлено на все терминалы)	org.freedesktop.login1.set-wall-message

10.4.6.4.3.3. Ограничения службы Machine

Список политик, настраивающих ограничения службы Machine приведены в таблице 39.

Т а б л и ц а 39 – Ограничения службы Machine

Политика	Описание	Правило Polkitd
Ограничение возможности авторизации в локальном контейнере	Политика управляет ограничением возможности авторизации в локальном контейнере	org.freedesktop.machine1.login
Ограничение возможности авторизации на локальном хосте	Политика управляет ограничением возможности авторизации на локальном хосте	org.freedesktop.machine1.host-login
Ограничение возможности получения интерпретатора командной строки (командной оболочки) в локальном контейнере	Политика управляет ограничением возможности получения интерпретатора командной строки (командной оболочки) в локальном контейнере	org.freedesktop.machine1.shell
Ограничение возможности получения интерпретатора командной строки (командной оболочки) на локальном хосте	Политика управляет ограничением возможности получения интерпретатора командной строки (командной оболочки) на локальном хосте	org.freedesktop.machine1.host-shell
Ограничение возможности получения псевдотерминала (TTY) в локальном контейнере	Политика управляет ограничением возможности получения псевдотерминала (TTY) в локальном контейнере	org.freedesktop.machine1.open-pty
Ограничение возможности получения псевдотерминала (TTY) на локальном хосте	Политика управляет ограничением возможности получения псевдотерминала (TTY) на локальном хосте	org.freedesktop.machine1.host-open-pty
Ограничение возможности управления локальными виртуальными машинами и контейнерами	Политика управляет ограничением возможности управления локальными виртуальными машинами и контейнерами	org.freedesktop.machine1.manage-machines
Ограничение возможности управления локальными виртуальными машинами и образами контейнеров	Политика управляет ограничением возможности управления локальными виртуальными машинами и образами контейнеров	org.freedesktop.machine1.manage-images

10.4.6.4.3.4. Ограничения службы NetworkManager

Список политик, настраивающих ограничения службы NetworkManager приведены в таблице 40.

Т а б л и ц а 40 – Ограничения службы NetworkManager

Политика	Описание	Правило Polkitd
Ограничение возможности включения или отключения сети	Политика управляет ограничением возможности включения или отключения сетевого взаимодействия системы. Если сетевое взаимодействие отключено, все управляемые интерфейсы отсоединяются и деактивируются. Если сетевое взаимодействие включено, все управляемые интерфейсы доступны для активации	org.freedesktop.NetworkManager.enable-disable-network
Ограничение возможности включения или отключения статистики	Политика управляет ограничением возможности включения или отключения счетчика статистики устройства	org.freedesktop.NetworkManager.enable-disable-statistics
Ограничение возможности включения или отключения устройств Wi-Fi	Данная политика управляет ограничением возможности включения или отключения устройств Wi-Fi	org.freedesktop.NetworkManager.enable-disable-wifi
Ограничение возможности включения или отключения устройств WiMAX	Данная политика управляет ограничением возможности включения или отключения мобильных широкополосных устройств WiMAX	org.freedesktop.NetworkManager.enable-disable-wimax
Ограничение возможности включения или отключения WWAN-устройств	Политика управляет ограничением возможности включения или отключения WWAN-устройств	org.freedesktop.NetworkManager.enable-disable-wwan
Ограничение возможности изменения общих настроек DNS	Политика управляет ограничением возможности изменения общей конфигурации DNS	org.freedesktop.NetworkManager.settings.modify.global-dns
Ограничение возможности изменения персональных сетевых настроек	Данная политика управляет ограничением возможности изменения личных сетевых соединений	org.freedesktop.NetworkManager.settings.modify.own
Ограничение возможности изменения постоянного имени хоста	Данная политика управляет ограничением возможности изменения постоянного имени системы	org.freedesktop.NetworkManager.settings.modify.hostname
Ограничение возможности изменения сетевых подключений для всех пользователей	Политика управляет ограничением возможности изменения системных сетевых настроек для всех пользователей	org.freedesktop.NetworkManager.settings.modify.system
Разрешение изменения системных настроек для сети	Политика управляет ограничением возможности изменения системных сетевых настроек	org.freedesktop.NetworkManager.network-control
Ограничение возможности изменения состояния сна NetworkManager	Данная политика управляет ограничением возможности на перевод NetworkManager в спящий режим или пробуждение из спящего режима (должна использоваться только для управления питанием системы)	org.freedesktop.NetworkManager.sleep-wake

Окончание таблицы 40

Политика	Описание	Правило Polkitd
Ограничение возможности отката конфигурации сетевых интерфейсов к контрольной точке	Политика управляет ограничением возможности создания контрольной точки сетевых интерфейсов или откату к ней	org.freedesktop.NetworkManager.checkpoint-rollback
Ограничение возможности перезагрузки NetworkManager	Политика управляет ограничением возможности перезагрузки конфигурации NetworkManager	org.freedesktop.NetworkManager.reload
Ограничение возможности проверки подключения сети	Политика управляет ограничением возможности включения или отключения проверки подключения к сети	org.freedesktop.NetworkManager.enable-disable-connectivity-check
Ограничение возможности сканирования Wi-Fi сетей	Данная политика управляет ограничением возможности сканирования Wi-Fi сетей	org.freedesktop.NetworkManager.wifi.scan
Ограничение возможности совместных подключений через защищенную сеть Wi-Fi	Политика управляет ограничением возможности совместного подключения через защищенную сеть Wi-Fi	org.freedesktop.NetworkManager.wifi.share.protected
Ограничение возможности совместных подключений через открытую сеть Wi-Fi	Политика управляет ограничением возможности совместного подключения через открытую сеть Wi-Fi	org.freedesktop.NetworkManager.wifi.share.open

Разрешения NetworkManager для текущего пользователя можно просмотреть, выполнив команду:

```
$ nmcli general permissions
```

```
PERMISSION
```

```
VALUE
```

```
org.freedesktop.NetworkManager.checkpoint-rollback      auth
org.freedesktop.NetworkManager.enable-disable-connectivity-check  нет
org.freedesktop.NetworkManager.enable-disable-network      auth
org.freedesktop.NetworkManager.enable-disable-statistics    auth
org.freedesktop.NetworkManager.enable-disable-wifi          да
org.freedesktop.NetworkManager.enable-disable-wimax         да
org.freedesktop.NetworkManager.enable-disable-wwan          да
org.freedesktop.NetworkManager.network-control             да
org.freedesktop.NetworkManager.reload                      auth
org.freedesktop.NetworkManager.settings.modify.global-dns   нет
org.freedesktop.NetworkManager.settings.modify.hostname     auth
org.freedesktop.NetworkManager.settings.modify.own          auth
org.freedesktop.NetworkManager.settings.modify.system        да
org.freedesktop.NetworkManager.sleep-wake                   да
org.freedesktop.NetworkManager.wifi.scan                    да
org.freedesktop.NetworkManager.wifi.share.open              да
org.freedesktop.NetworkManager.wifi.share.protected         да
```

10.4.6.4.3.5. Ограничения службы ModemManager

Список политик, настраивающих ограничения службы ModemManager приведены в таблице 41.

Т а б л и ц а 41 – Ограничения службы ModemManager

Политика	Описание	Правило Polkitd
Ограничение возможности блокировки и управления мобильным широкополосным устройством	Политика ограничивает возможность изменения конфигурации мобильного широкополосного устройства	org.freedesktop.ModemManager1.Device.Control
Ограничение возможности добавления, изменения или удаления контактов устройства	Политика управляет ограничением возможности добавления, изменения и удаления контактов мобильного широкополосного доступа	org.freedesktop.ModemManager1.Contacts
Ограничение возможности запросов и использования сетевой информации и услуг	Политика ограничивает возможность запрашивать или использовать сетевую информацию и службы	org.freedesktop.ModemManager1.USSD
Ограничение возможности запросов информации о сетевом времени и часовом поясе	Политика ограничивает возможность запрашивать информацию о сетевом времени	org.freedesktop.ModemManager1.Time
Ограничение возможности отправки, сохранения, изменения и удаления текстовых сообщений	Политика ограничивает возможность отправки или манипулирования текстовыми сообщениями устройства	org.freedesktop.ModemManager1.Messaging
Ограничение возможности приема входящих голосовых вызовов или начала исходящего голосового вызова	Политика ограничивает возможность голосовых вызовов	org.freedesktop.ModemManager1.Voice
Ограничение возможности просмотра информации о географическом положении и позиционировании	Политика ограничивает возможность просмотра информации о географическом положении	org.freedesktop.ModemManager1.Location
Ограничение возможности управления демоном Modem Manager	Политика ограничивает возможность управления диспетчером модемов	org.freedesktop.ModemManager1.Control
Ограничение возможности управления прошивкой мобильного широкополосного устройства	Политика ограничивает возможность управления микропрограммой мобильного широкополосного устройства	org.freedesktop.ModemManager1.Firmware

10.4.6.4.3.6. Ограничения службы PackageKit

Список политик, настраивающих ограничения службы PackageKit приведены в таблице 42.

Т а б л и ц а 42 – Ограничения службы PackageKit

Политика	Описание	Правило Polkitd
Ограничение возможности восстановления пакетов в системе	Данная политика ограничивает пользователей возможность восстановления системы пакетов, если в ней возникли проблемы, например, пропали зависимости, посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.repair-system
Ограничение возможности добавления ключа электронной подписи	Данная политика ограничивает пользователей возможность добавления ключа подписи в список доверенных ключей системы посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.system-trust-signing-key
Ограничение возможности обновления пакетов	Данная политика ограничивает пользователей возможность обновления пакетов, установленных в систему, посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.system-update
Ограничение возможности обновления системных источников пакетов	Данная политика ограничивает пользователей возможность обновления системных источников пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.system-sources-refresh
Ограничение возможности переустановки пакетов	Данная политика ограничивает пользователей возможность переустановки пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-reinstall
Ограничение возможности принятия лицензионного соглашения	Данная политика ограничивает возможность принятия пользовательского соглашения программ посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-eula-accept
Ограничение возможности редактирования источников пакетов	Данная политика ограничивает пользователей возможность редактирования источников пакетов в системе посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.system-sources-configure
Ограничение возможности удаления пакетов	Данная политика ограничивает пользователей возможность удаления пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-remove
Ограничение возможности установки пакетов	Данная политика ограничивает пользователей возможность установки пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-install
Ограничение возможности установки непроверенных пакетов	Данная политика ограничивает пользователей возможность установки ненадежных или непроверенных пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-install-untrusted

10.4.6.4.3.7. Ограничения Realmd

Список политик, настраивающих ограничения Realmd приведены в таблице 43.

Т а б л и ц а 43 – Ограничения Realmd

Политика	Описание	Правило Polkitd
Ограничение возможности запустить обнаружение области Kerberos REALM	Данная политика управляет ограничением возможности запустить обнаружение области Kerberos REALM	org.freedesktop.realmd.discover-realm
Ограничение возможности изменения политики входа в систему	Данная политика управляет ограничением возможности изменения политики входа в систему	org.freedesktop.realmd.login-policy
Ограничение возможности присоединения машины к домену или Kerberos REALM	Данная политика управляет ограничением возможности присоединения машины к домену или Kerberos REALM	org.freedesktop.realmd.configure-realm
Ограничение возможности отключения машины из домена или Kerberos REALM	Данная политика управляет ограничением возможности удаления машины из домена или Kerberos REALM	org.freedesktop.realmd.deconfigure-realm

10.4.6.4.3.8. Ограничения Udisks2

Список политик, настраивающих ограничения Udisks2 приведены в таблице 44.

Т а б л и ц а 44 – Ограничения Udisks2

Политика	Описание	Правило Polkitd
Общая политика ограничения возможности монтирования	Данная политика ограничивает возможность монтирования съемных запоминающих устройств, монтирования системных разделов, монтирования съемных запоминающих устройств в удаленных сеансах	org.freedesktop.udisks2.filesystem-mount org.freedesktop.udisks2.filesystem-mount-other-seat org.freedesktop.udisks2.filesystem-mount-system
Ограничение возможности включения/отключения SMART	Данная политика управляет ограничением возможности включения/отключения SMART	org.freedesktop.udisks2.ata-smart-enable-disable

Окончание таблицы 44

Политика	Описание	Правило Polkitd
Ограничение возможности запуска самопроверки SMART	Данная политика управляет ограничением возможности запуска самопроверки SMART	org.freedesktop.udisks2.ata-smart-selftest
Ограничение возможности монтирования системных разделов	Данная политика ограничивает возможность монтирования системных разделов. Системное устройство хранения информации – это неизвлекаемое устройство. Для таких устройств переменная HintSystem установлена в значение True. Жесткий диск с установленной ОС относится к системным устройствам	org.freedesktop.udisks2.file-system-mount-system
Ограничение возможности монтирования съемных запоминающих устройств в удаленных сеансах	Данная политика ограничивает возможность монтирования съемных запоминающих устройств с устройства, подключенного к удаленному рабочему месту (например, на другом компьютере или удаленной сессии)	org.freedesktop.udisks2.file-system-mount-other-seat
Ограничение возможности монтирования файловой системы	Данная политика управляет ограничением возможности монтирования файловой системы устройства	org.freedesktop.udisks2.file-system-mount
Ограничение возможности надежно стереть жесткий диск	Данная политика управляет ограничением возможности надежно стереть жесткий диск	org.freedesktop.udisks2.ata-secure-erase
Ограничение возможности обновить данные SMART	Данная политика управляет ограничением возможности обновить данные SMART	org.freedesktop.udisks2.ata-smart-update
Ограничение возможности отправить команду ожидания для диска с удаленного места	Данная политика управляет ограничением возможности отправить команду ожидания для диска с удаленного места	org.freedesktop.udisks2.ata-standby-other-seat
Ограничение возможности отправить команду режима ожидания на системный диск	Данная политика управляет ограничением возможности отправить команду режима ожидания на системный диск	org.freedesktop.udisks2.ata-standby-system
Ограничение возможности отправить резервную команду	Данная политика управляет ограничением возможности отправить резервную команду	org.freedesktop.udisks2.ata-standby
Ограничение возможности разрешения на проверку состояния питания жесткого диска	Данная политика управляет ограничением возможности разрешения на проверку состояния питания жесткого диска	org.freedesktop.udisks2.ata-check-power
Ограничение возможности установить данные SMART из большого двоичного объект	Данная политика управляет ограничением возможности установить данные SMART из большого двоичного объекта	org.freedesktop.udisks2.ata-smart-simulate

10.4.6.4.3.9. Другие политики

Список политик Polkit, которые не относятся к вышеприведенным группам приведены в таблице 45.

Т а б л и ц а 45 – Другие политики Polkit

Политика	Описание	Правило Polkitd
Ограничение возможности запуска программы от имени другого пользователя	Данная политика управляет ограничением возможности запуска программы от имени другого пользователя	org.freedesktop.policykit.exec

10.4.6.4.4. Политики доступа к съемным носителям

Эта групповая политика позволяет централизованно для компьютеров или пользователей настраивать доступ к съемным запоминающим устройствам (CD, DVD, USB и др.).

П р и м е ч а н и е . Политика полного запрета на доступ к съемным носителям реализована через правила в Polkit (`/etc/polkit-1/rules.d/`).

Правила для пользовательской политики обрабатываются до правил для машинной политики. Для машинной политики создается файл правил `49-gpoa_disk_permissions.rules`, для пользовательской политики – `48-gpoa_disk_permissions_user.<USERNAME>.rules`.

Для настройки этой политики следует перейти в «Компьютер»/«Пользователь» → «Административные шаблоны» → «Система» → «Доступ к съемным запоминающим устройствам» (рис. 386).

П р и м е ч а н и е . На данный момент реализована только политика «Съемные запоминающие устройства всех классов: Запретить любой доступ» (машинная и пользовательская).

Щелкнуть левой кнопкой мыши на политике «Съемные запоминающие устройства всех классов: Запретить любой доступ», откроется диалоговое окно настройки политики. Можно не задавать настройку политики, включить или отключить (рис. 387).

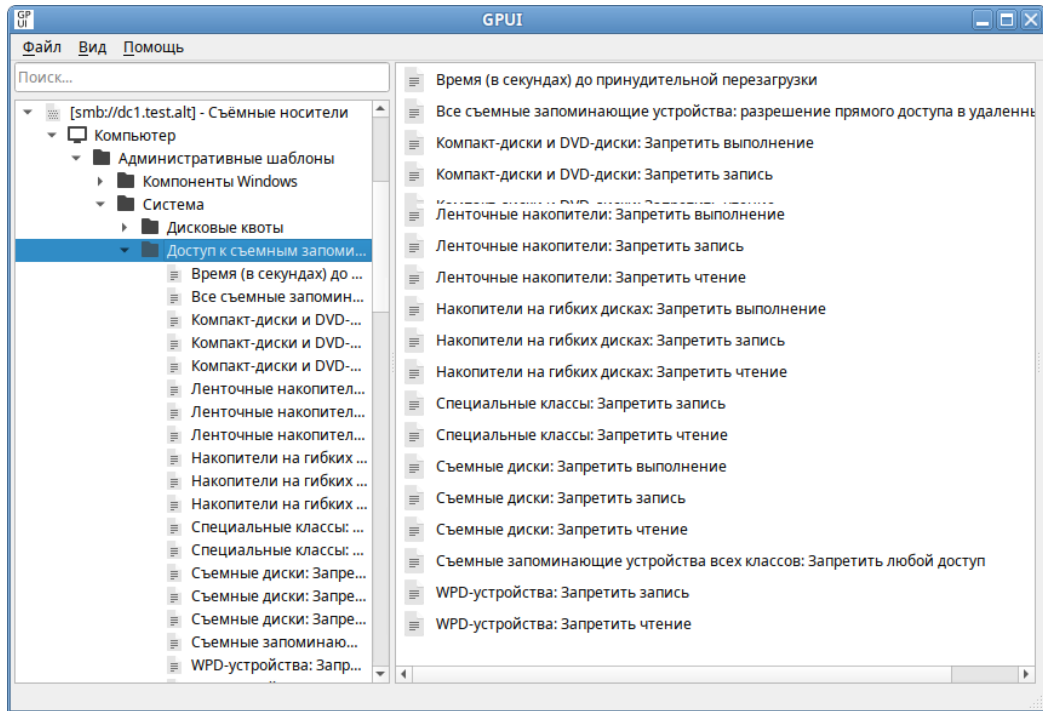


Рис. 386 – «Доступ к съемным запоминающим устройствам»

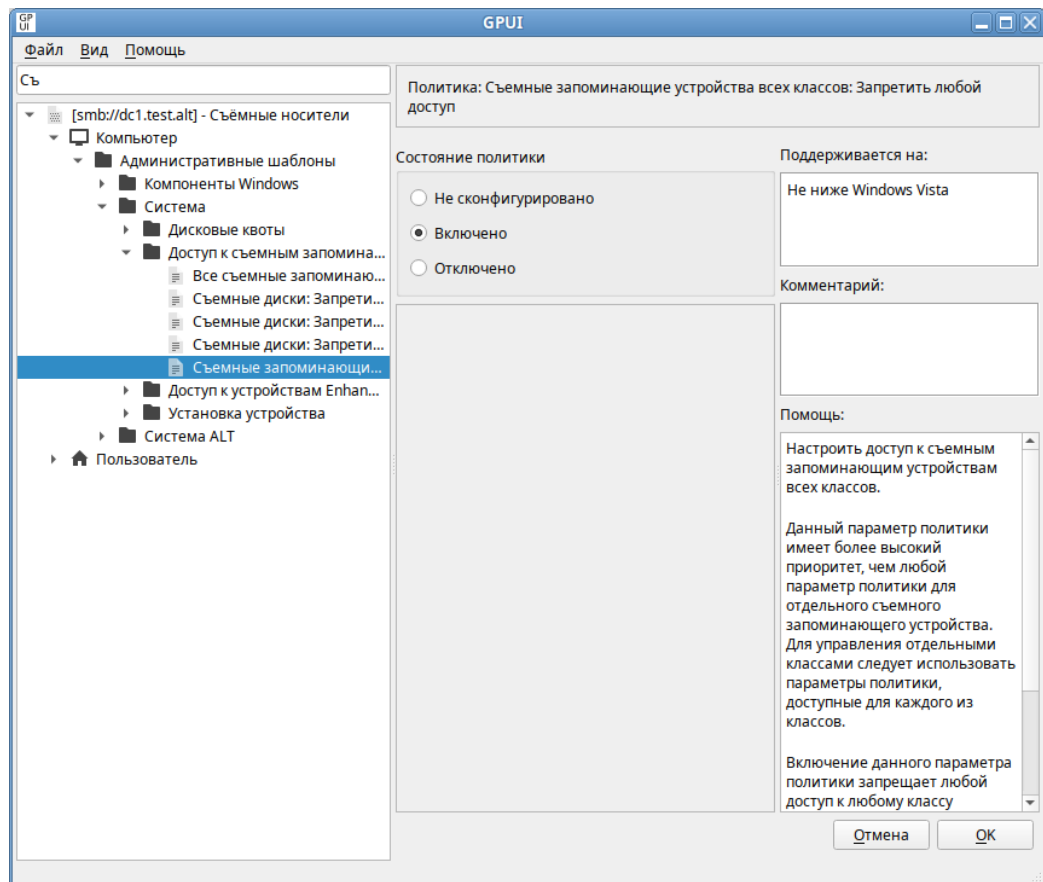


Рис. 387 – Настройки политики «Съемные запоминающие устройства всех классов: Запретить любой доступ»

Для включения запрета на доступ следует выбрать параметр «Включено», для отключения – «Отключено» или «Не сконфигурировано».

Настройки политики управления пакетами хранятся в файлах {GUID GPT}/Machine/Registry.pol и {GUID GPT}/User/Registry.pol.

Пример файла Registry.pol:

```
PReg  
[Software\Policies\Microsoft\Windows\RemovableStorageDevices;Deny_All;;;]
```

10.4.6.4.5. Управление gsettings

Данные групповые политики позволяют управлять ключами gsettings. В свою очередь gsettings управляет ключами dconf.

В настоящий момент реализованы настройки удаленного доступа к рабочему столу (VNC) через Vino и настройки графической среды МАТЕ, а именно:

- настройки фона рабочего стола;
- настройки хранителя экрана;
- настройки ограничений пользователя.

Машинные политики являются действующими по умолчанию, а пользовательские, при установке, замещают машинные. У машинных политик имеются блокировки, при установке которых пользовательские настройки игнорируются, а для применения используются значения, установленные машинными политиками.

Порядок применения политик:

- 1) машинные политики применяются при загрузке компьютера;
- 2) машинные политики без блокирования могут применяться, но только в том случае, если пользователь ни разу не изменял эти политики;
- 3) машинные политики с блокировкой применяются независимо от пользовательских настроек;
- 4) пользовательские политики применяются при логине пользователя и только в случае, если нет таких же машинных политик с блокировкой.

Для настройки политики следует перейти в «Компьютер»/ «Пользователь» → «Административные шаблоны» → «Система ALT» → «Настройки Mate»/ «Удаленный доступ через Vino». Выбрать раздел, в правом окне редактора отобразится список политик (рис. 388).

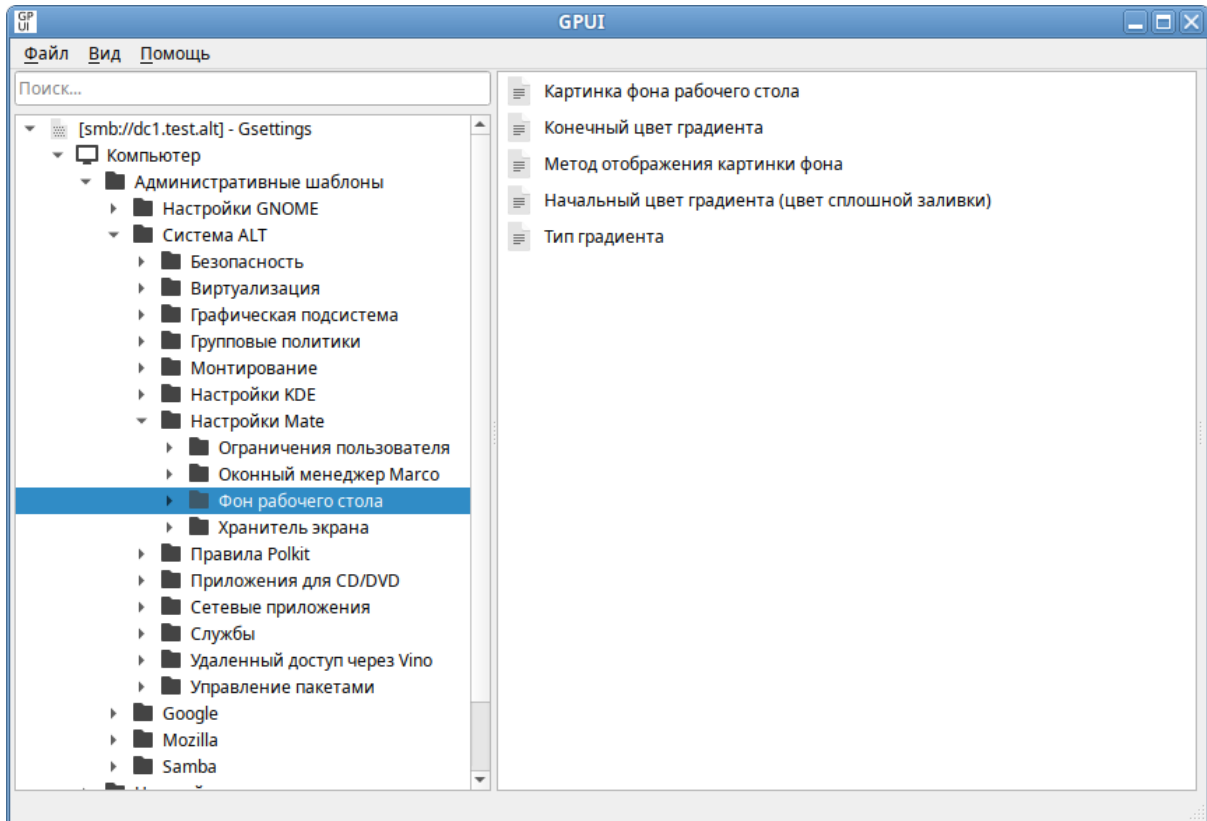


Рис. 388 – Управление настройками gsettings

При выборе политики, откроется диалоговое окно настройки политики (рис. 389).

Можно не задавать настройку политики, включить или отключить. Если выбрать параметр «Включено», в разделе «Параметры» в выпадающем списке можно указать настройки политики (рис. 390).

Политика, управляющая настройкой фона рабочего стола, изменяет ключ KEY в схеме org.mate.background. В реестре Windows изменяет в Software\BaseALT\Policies\gsettings ключ org.mate.background.KEY. Блокировка устанавливается в ветке реестра Software\BaseALT\Policies\GSettingsLocks, ключ org.mate.background.KEY.

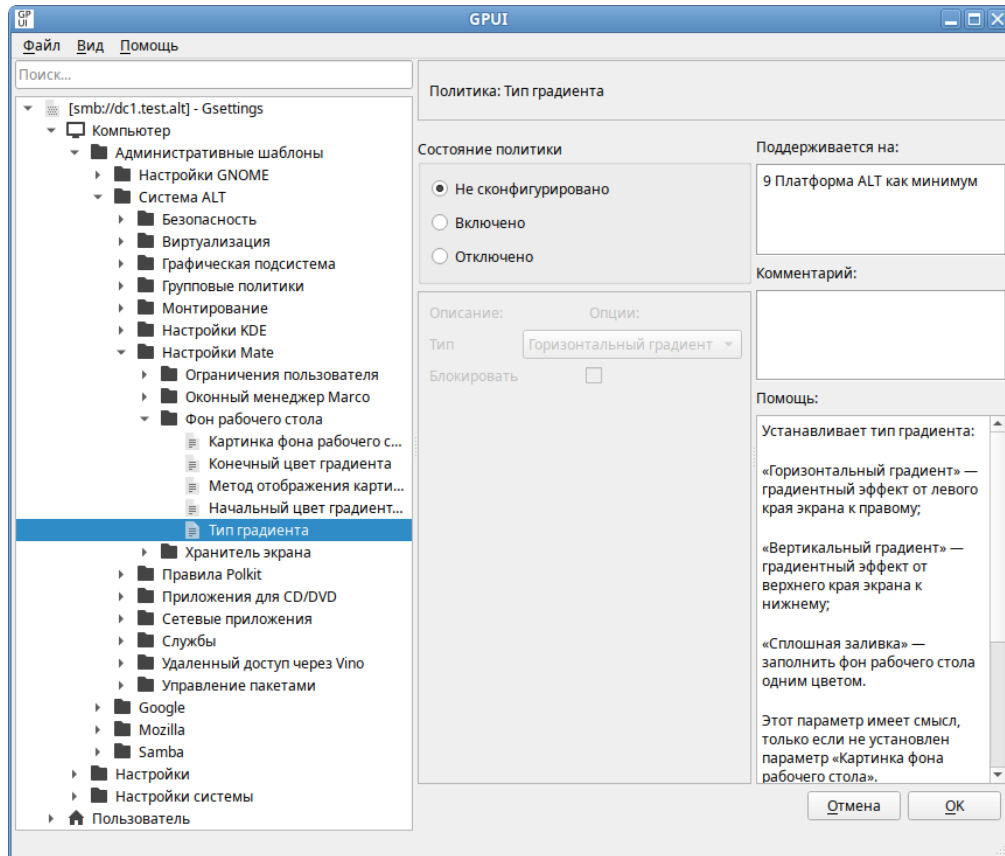


Рис. 389 – Диалоговое окно настройки политики «Тип градиента»

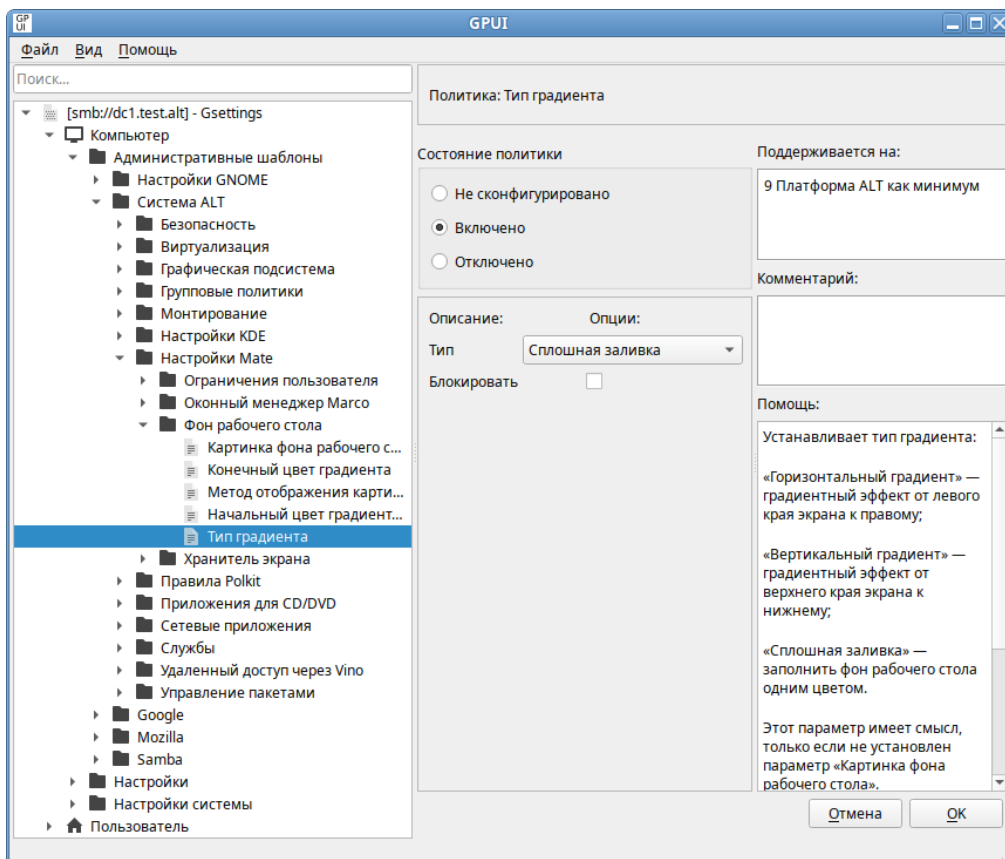


Рис. 390 – Установка градиента в политике «Тип градиента»

Настройки фона рабочего стола приведены в таблице 46.

Т а б л и ц а 46 – Настройки фона рабочего стола

Политика	Ключ	Описание	Значение
Картинка фона рабочего стола	picture-filename	Позволяет устанавливать изображение в качестве фона рабочего стола, задав имя файла, содержащего изображение	Строка, содержащая путь (с точки зрения клиента) к файлу изображения (например, /usr/share/backgrounds/mate/nature/Wood.jpg)
Метод отображения картинки фона	picture-options	Устанавливает метод отображения изображения, заданного параметром «Картинка фона рабочего стола»	«None» («нет») – нет изображения. «Wallpaper» («мозаика») – дублирует изображение в оригинальном размере таким образом, что изображение полностью покрывает рабочий стол. «Centered» («по центру») – отображает изображение в центре рабочего стола в соответствии с оригинальным размером изображения. «Scaled» («масштаб») – увеличивает изображение, сохраняя пропорции, до тех пор, пока величина одной из границ изображения не совпадет с величиной одной из границ экрана. «Stretched» («растянуть») – увеличивает изображение для соответствия размеру рабочего стола, изменяя пропорции при необходимости. «Zoom» («приближение») – увеличивает наименьшую из сторон изображения до тех пор, пока ее величина не совпадет с величиной соответствующей границы экрана; изображение может быть обрезано по другой стороне. «Stretched» («заполнение») – увеличивает изображение, сохраняя пропорции, до тех пор, пока величина одной из границ изображения не совпадет с величиной одной из границ экрана
Тип градиента	color-shading-type	Устанавливает тип градиента фона рабочего стола. Этот параметр имеет смысл, только если не установлен параметр «Картинка фона рабочего стола»	«Вертикальный градиент» – градиентный эффект от верхнего края экрана к нижнему краю. «Горизонтальный градиент» – градиентный эффект от левого края экрана к правому. «Сплошная заливка» – заполнить фон рабочего стола одним цветом

Окончание таблицы 46

Политика	Ключ	Описание	Значение
Конечный цвет градиента	secondary-color	Устанавливает «конечный» цвет градиента фона рабочего стола. Данным цветом заканчивается градиент и, в зависимости от типа градиента, параметр определяет цвет правого или нижнего края рабочего стола. Данный параметр не используется, если в параметре «Тип градиента» выбрана «Сплошная заливка»	Ключевое слово цвета (red, aqua, navy и т. д.). Строка типа #RRGGBB. Строка типа rgb(0, 0, 0)
Начальный цвет градиента	primary-color	Устанавливает начальный цвет градиента фона рабочего стола. Данным цветом начинается градиент и, в зависимости от типа градиента, параметр определяет цвет левого или верхнего края рабочего стола, или цвет сплошной заливки	Ключевое слово цвета (red, aqua, navy и т. д.). Строка типа #RRGGBB. Строка типа rgb(0, 0, 0)

Политика, управляющая настройкой хранителя экрана, изменяет ключ KEY в схеме org.mate.screensaver. В реестре Windows изменяет в Software\BaseALT\Policies\gsettings ключ org.mate.screensaver.KEY. Блокировка устанавливается в ветке реестра Software\BaseALT\Policies\GSettingsLocks, ключ org.mate.screensaver.KEY.

Настройки хранителя экрана приведены в таблице 47.

Т а б л и ц а 47 – Настройки хранителя экрана

Политика	Ключ	Описание	Значение
Время смены тем	cycle-delay	Устанавливает интервал (в минутах) между сменами тем хранителя экрана. Этот параметр имеет смысл только при активированном параметре «Включение хранителя экрана» и если для параметра «Режим работы» установлено значение «Случайные темы»	Время в минутах
Время до блокировки паролем	lock-delay	Устанавливает количество минут, по истечении которых после активации хранителя экрана, компьютер будет заблокирован. Имеет смысл только при активированном параметре «Включение хранителя экрана» и «Блокировка компьютера»	Время в минутах
Блокировка компьютера	lock-enabled	Включает блокировку компьютера при активации хранителя экрана. Блокировка будет включена через интервал времени, установленный настройкой «Время до блокировки паролем». Имеет смысл только при активированном параметре «Включение хранителя экрана»	-
Время выхода из сеанса	logout-delay	Устанавливает количество минут, по истечении которых после активации хранителя экрана, при разблокировании пользователю будет предоставлена возможность выхода из сеанса. Имеет смысл только при активированном параметре «Включение хранителя экрана» и «Выход из сеанса после блокировки»	Время в минутах
Выход из сеанса после блокировки	logout-enabled	После некоторой задержки добавляет кнопку выхода из системы к диалогу разблокирования экрана. Время задержки указывается в настройке «Время выхода из сеанса». Имеет смысл только при активированном параметре «Включение хранителя экрана» и «Блокировка компьютера»	-
Переключить пользователя после блокировки	user-switch-enabled	Добавляет кнопку «Переключить пользователя» к диалогу разблокирования экрана. Имеет смысл только при активированном параметре «Включение хранителя экрана» и «Блокировка компьютера» (так как без блокировки не появляется диалог с кнопкой)	-

Окончание таблицы 47

Политика	Ключ	Описание	Значение
Режим работы	mode	Устанавливает режим работы хранителя экрана. Имеет смысл только при активированном параметре «Включение хранителя экрана»	Доступны следующие режимы: «Отключен» – режим отключен «Пустой экран» – не показывать никаких изображений, только черный экран; «Выбранная тема» – показывать одну (указанную) тему хранителя экрана; «Случайные темы» – выбрать тему хранителя экрана случайным образом
Включение хранителя экрана	idle-activation-enabled	Обеспечивает включение хранителя экрана при бездействии системы	-

Политика, управляющая настройкой ограничений пользователя, изменяет ключ KEY в схеме org.mate.lockdown. В реестре Windows изменяет в Software\BaseALT\Policies\gsettings ключ org.mate.lockdown.KEY. Блокировка устанавливается в ветке реестра Software\BaseALT\Policies\GSettingsLocks, ключ org.mate.lockdown.KEY.

Настройки ограничений пользователя приведены в таблице 48.

Т а б л и ц а 48 – Настройки ограничений пользователя

Политика	Ключ	Описание	Значение
Запрет блокировки экрана	picture-filename	Запрещает пользователю блокировать экран паролем. При установке данной настройки, значение параметра «Блокировка компьютера» игнорируется	-
Запрет пользователю завершать сеанс	disable-logout	Запрещает пользователю завершать свой сеанс	-
Запрет выбора тем рабочего стола	picture-filename	Запрещает пользователю изменять тему оформления графической среды MATE	-
Запрет переключения пользователей	disable-user-switching	Запрещает пользователю переключение на другую учетную запись, пока активен его сеанс. Отключает кнопку «Переключить пользователя» в диалоговом окне, вызываемом при выборе в главном меню пункта «Завершить сеанс»	-

Политика, управляющая настройкой удаленного доступа VNC, изменяет ключ KEY в схеме org.gnome.Vino. В реестре Windows изменяет в Software\BaseALT\Policies\gsettings ключ org.gnome.Vino.KEY. Блокировка устанавливается в ветке реестра Software\BaseALT\Policies\GSettingsLocks, ключ org.gnome.Vino.KEY.

Настройки ограничений пользователя приведены в таблице 49.

Т а б л и ц а 49 – Настройки удаленного доступа VNC

Политика	Ключ	Описание	Значение
Альтернативный порт	alternative-port	Устанавливает альтернативный порт для удаленного подключения к рабочему столу. Используется только при установленном параметре «Включить альтернативный порт»	Значение номера порта в пределах от 5 000 до 50 000. По умолчанию используется порт 5900
Методы аутентификации	authentication-methods	Устанавливает методы аутентификации пользователей, подключающихся к рабочему столу. Используется только при установленном параметре «Пароль для подключения»	«None» – пароль для подключения не требуется. «Vnc» – для подключения нужен пароль
Удаленный доступ	enabled	Разрешает удаленный доступ к рабочему столу с использованием протокола RFB и VNC	«Включено» – удаленный доступ разрешен. «Отключено» – удаленный доступ запрещен
Иконка подключения	icon-visibility	Управляет отображением значка подключения в области уведомления	«Никогда» – значок не отображается. «Всегда» – значок отображается всегда. «Только при подключении клиента» – значок отображается при подключении удаленного пользователя
Подтверждение при подключении	prompt-enabled	Включает запрос подтверждения при любой попытке доступа к рабочему столу. Рекомендуется при отсутствии защиты подключения паролем	«Включено» – запрашивается подтверждение доступа. «Отключено» – подтверждение доступа не запрашивается
Включить альтернативный порт	prompt-enabled	Включить прослушивание альтернативного порта для удаленных подключений (вместо порта по умолчанию 5 900). Порт указывается в параметре «Альтернативный порт»	«Включено» – включить прослушивание альтернативного порта. «Отключено» – не включать прослушивание альтернативного порта

Окончание таблицы 49

Политика	Ключ	Описание	Значение
Удаленное управление	view-only	Запрещает удаленное управление рабочим столом. Удаленным пользователям, разрешается только просматривать рабочий стол, но не управлять мышью и клавиатурой	«Включено» – удаленное управление разрешено. «Отключено» – удаленное управление запрещено

Политика, управляющая настройкой оконного менеджера Marco, изменяет ключ KEY в схеме org.mate.Marco.general. В реестре Windows изменяет в Software\BaseALT\Policies\gsettings ключ org.mate.pMarco.general.KEY. Блокировка устанавливается в ветке реестра Software\BaseALT\Policies\GSettingsLocks, ключ org.mate.Marco.general.KEY.

Настройки оконного менеджера Marco приведены в таблице 50.

Т а б л и ц а 50 – Настройки оконного менеджера Marco

Политика	Ключ	Описание	Значение
Иконки заголовка окна	button-layout	Настройки расположения кнопок в заголовке окна	Строка вида: menu:minimize,maximize,spacer,close . Разделителем правой и левой половин является двоеточие. Имена кнопок разделяются запятыми. Например, строка 'menu:minimize,maximize,spacer,close' – расположить кнопку меню окна слева, а справа кнопки свернуть, распахнуть, закрыть окно. Дублирование кнопок не допускается. Неизвестные имена кнопок игнорируются без уведомления. Специальный элемент spacer может использоваться для вставки пробела между двумя кнопками
Действие по нажатию средней кнопки	action-middle-click-titlebar	Установка действия, выполняемого по нажатию средней кнопки мыши по заголовку окна	«Свернуть в заголовок» («toggle_shade») – свернуть окно в заголовок. По двойному щелчку окно разворачивается обратно. «На весь экран» («toggle_maximize») – распахнуть окно на весь экран или восстановить исходный размер.

Продолжение таблицы 50

Политика	Ключ	Описание	Значение
			<p>«Растянуть по вертикали» («toggle_maximize_vertically») – развернуть окно вертикально без изменения его ширины.</p> <p>«Растянуть по горизонтали» («toggle_maximize_horizontally») – развернуть окно горизонтально без изменения его высоты.</p> <p>«Свернуть» («minimize») – свернуть окно.</p> <p>«Показать меню» («menu») – показать меню окна.</p> <p>«Задвинуть» («lower») – поместить окно под другими.</p> <p>«Ничего не делать» («none») – никакого действия не производить.</p> <p>«Последнее действие» («last») – повторить предыдущее действие</p>
Действие по нажатию правой кнопки	action-right-click-titlebar	Установка действия, выполняемого по нажатию правой кнопки мыши по заголовку окна	См. значение политики «Действие по нажатию средней кнопки»
Размер окна переключения Alt+Tab	alt-tab-max-columns	Устанавливает количество колонок в окне переключения приложений Alt+Tab	Количество колонок
Действие по двойному щелчку	action-double-click-titlebar	Установка действия, выполняемого по двойному щелчку левой кнопкой мыши по заголовку окна	См. значение политики «Действие по нажатию средней кнопки»
Изменение размеров при перетаскивании	primary-color	<p>Включает изменение размеров окна при перетаскивании его в различные области экрана.</p> <p>Если включено, перетаскивание окна на границу экрана распахивает окно вертикально и изменяет горизонтальный размер до половины доступного пространства.</p> <p>Если активирован параметр «Распахнуть окно при перетаскивании к верхнему краю экрана», перетаскивание окна вверх разворачивает окно</p>	-

Продолжение таблицы 50

Политика	Ключ	Описание	Значение
Разворачивание при перетаскивании	allow-top-tiling	Включает разворачивание окна во весь экран при перетаскивании его к верхнему краю экрана. Этот параметр имеет смысл только при активированном параметре «Изменение размеров при перетаскивании»	-
Задержка при восстановлении	alt-tab-max-columns	Временной интервал в миллисекундах, по истечении которого окно в фокусе будет поднято поверх остальных. Этот параметр имеет смысл только при активированном параметре «Автоматически поднимать окно, получившее фокус»	Время в миллисекундах
Автоматически поднимать окно, получившее фокус	auto-raise	При включении, окно, получившее фокус, автоматически отображается поверх остальных. Параметр «Переключение фокуса окон» должен быть установлен в «sloppy» или «mouse». Интервал, по истечении которого, окно поднимается, устанавливается в параметре «Задержка при восстановлении»	-
Новые окна по центру	center-new-windows	Если включено, то новые окна будут открываться по центру экрана. В противном случае они будут открыты в левом верхнем углу экрана	-

Продолжение таблицы 50

Политика	Ключ	Описание	Значение
Миниатюры при переключении окон	compositing -fast-alt-tab	Если включено, то вместо миниатюр предварительного просмотра в окне переключения Alt+Tab будут отображаться значки приложения	-
Переключение фокуса на новое окно	focus-new-windows	Определяет, как новое окно получает фокус	«Smart» – новое окно получает фокус при создании. «Strict» – окна, запущенные из терминала, не получают фокус
Режим активации окна	focus-mode	Режим переключения фокуса в окно определяет, как активируются окна	«Click» – для активации окна на нем надо щелкнуть. «Sloppy» – окно активируется, когда на него перемещается указатель мыши. «Mouse» – окно активируется, когда в него перемещается указатель мыши, и перестает быть активным, когда указатель мыши уходит из него
Размер иконок в окне Alt+Tab	icon-size	Устанавливает размер значков, отображаемых в окне переключения приложений Alt+Tab	Интервал допустимых значений: 8 – 256
Количество рабочих областей (мест)	num-workspaces	Установка количества рабочих мест	Интервал допустимых значений 1 – 36
Расположение новых окон	placement-mode	Указывает, как будут позиционироваться новые окна	«Automatic» («Автоматически») – система выбирает местоположение на основе доступного пространства на рабочем столе, или располагает каскадом, если нет места. «Pointer» («Указатель») – новые окна размещаются в соответствии с положением указателя мыши. «Manual» («Ручной») – пользователь должен вручную расположить новое окно с помощью мыши или клавиатуры
Граница окна при переключении	show-tab-border	Выделять границу выбранного окна при переключении с помощью Alt+Tab	-

Окончание таблицы 50

Политика	Ключ	Описание	Значение
Тема оформления	theme	Устанавливает тему, отвечающую за отображение границ окон, заголовка и т. д.	Строка, содержащая название темы (например, Dorple)
Шрифт заголовка	titlebar-font	Устанавливает шрифт заголовков окон. Этот параметр игнорируется, если активирован параметр «Системный шрифт в заголовке окон»	Строка, содержащая название шрифта и через пробел, размер шрифта (например, Noto Sans Bold 10)
Системный шрифт в заголовке окон	titlebar-uses-system-font	Если включено, в заголовках окон используется стандартный системный шрифт. Параметр «Шрифт заголовка окна» при этом игнорируется	-
Переключение рабочих областей (столов)	wrap-style	Определяет, каким образом пролистывать от одного рабочего стола к другому на границе переключателя рабочих мест	«No wrap» – при попытке пролистать рабочее место за границу переключателя ничего не произойдет. «Classic» – конец одной строки ведет на начало следующей и конец одной колонки ведет к началу следующей. «Toroïdal» – конец каждой строки ведет к ее же началу, и конец каждой колонки ведет к ее же началу

Политика, управляющая настройкой клавиатуры, изменяет ключ KEY в схеме org.mate.peripherals-keyboard. В реестре Windows изменяет в Software\BaseALT\Policies\gsettings ключ org.mate.peripherals-keyboard.KEY. Блокировка устанавливается в ветке реестра Software\BaseALT\Policies\GSettingsLocks, ключ org.mate.peripherals-keyboard.KEY.

Настройки клавиатуры приведены в таблице 51.

Т а б л и ц а 51 – Настройки клавиатуры

Политика	Ключ	Описание	Значение
Задержка перед повтором	delay	Задержка перед повтором нажатой и удерживаемой клавиши	Время в миллисекундах
Скорость повтора	rate	Устанавливает скорость повтора нажатой и удерживаемой клавиши	Количество повторов в секунду
Повторять удерживаемую нажатой клавишу	repeat	Включить повтор нажатой и удерживаемой клавиши. Если нажать и удерживать клавишу при включенном повторе ввода, действие, соответствующее клавише, будет повторяться. Например, если нажать и удерживать клавишу с буквой, то эта буква будет многократно повторена.	-

10.4.6.4.6. Управление пакетами

Эта групповая политика позволяет централизованно для компьютеров устанавливать и удалять пакеты.

Примечание. Для возможности установки и удаления пакетов, на компьютерах, на которых будет применяться политика, должен быть установлен пакет `rsakekit`.

Для настройки политики следует перейти в «Компьютер»/«Пользователь» → «Административные шаблоны» → «Система ALT» → «Управление пакетами». Выбрать раздел, в правом окне редактора отобразится список политик (рис. 391).

Для задания списка пакетов, которые нужно установить, щелкнуть левой кнопкой мыши на политике «Установка пакетов», откроется диалоговое окно настройки политики (рис. 392).

Для включения политики следует установить отметку в поле «Включено». Для задания списка пакетов, которые должны быть установлены/удалены нажать кнопку «Редактировать» и в открывшемся окне ввести список пакетов, по одному на каждой строке (рис. 393).

Для добавления/удаления строк можно воспользоваться соответствующими кнопками.

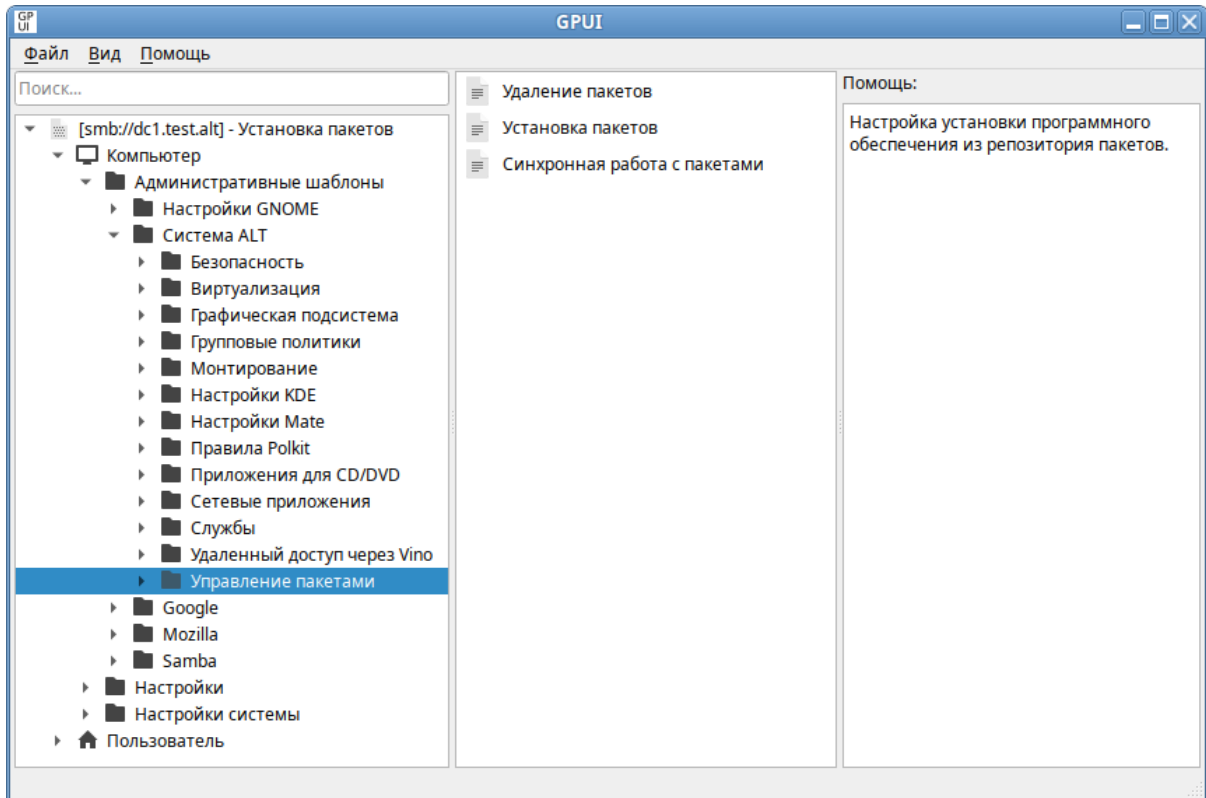


Рис. 391 – Раздел «Управление пакетами»

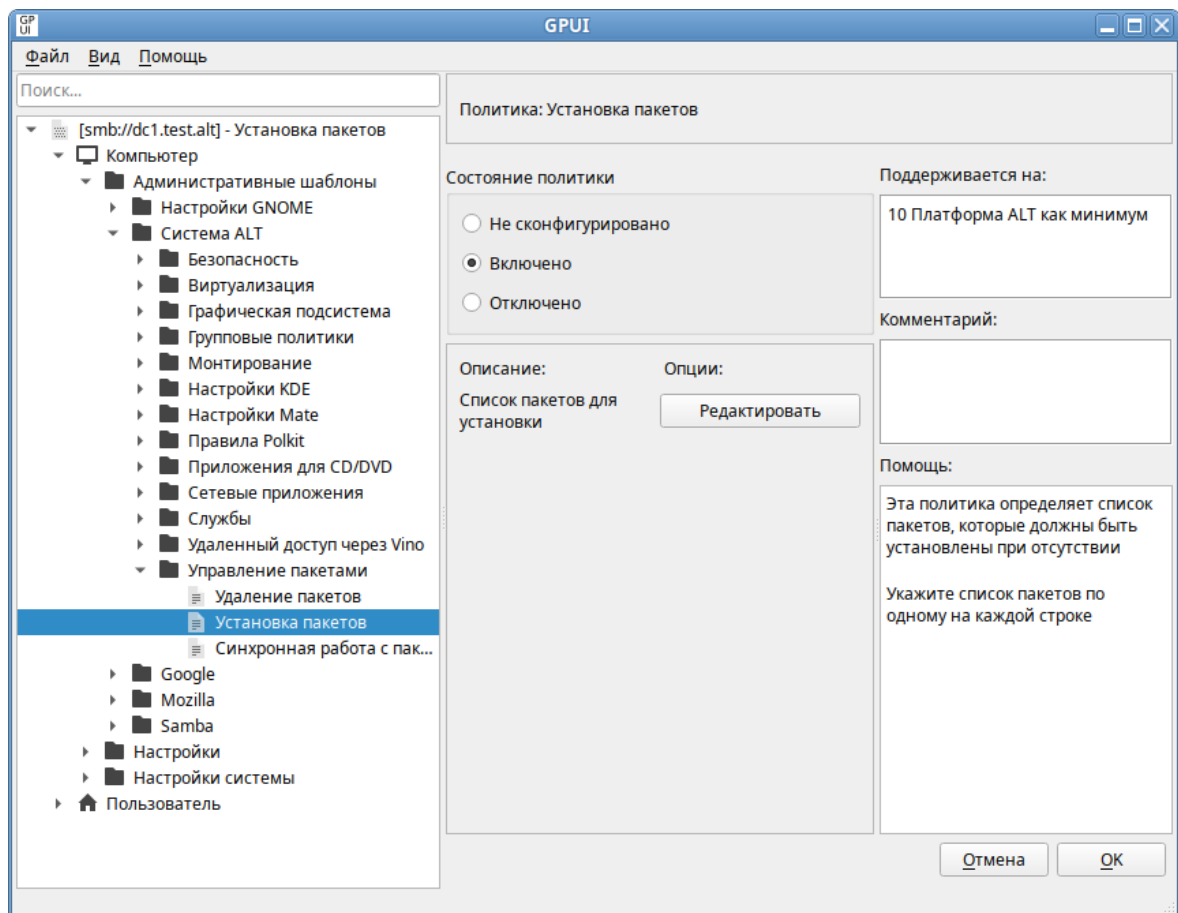


Рис. 392 – Диалоговое окно «Установка пакетов»

Примечание. Для задания списка пакетов, которые нужно удалить, нужно выбрать политику «Удаление пакетов».

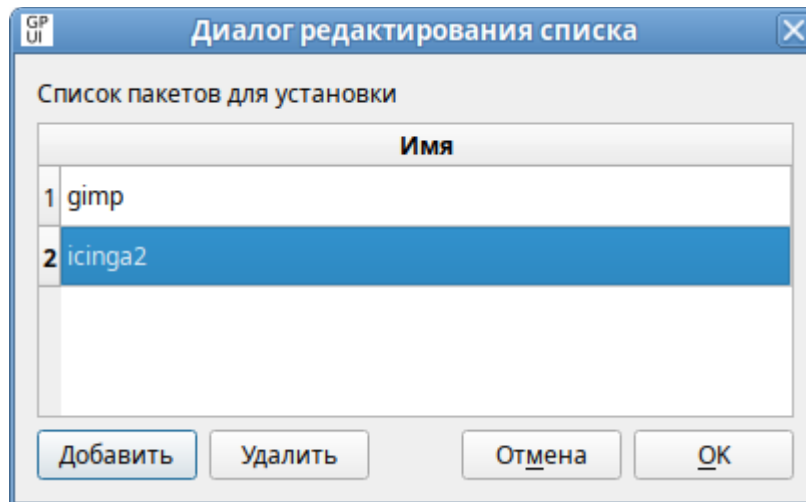


Рис. 393 – Список пакетов для установки

Можно также включить политику «Синхронная работа с политиками». Включение данной настройки запретит работу (установка, удаление) с пакетами в фоновом режиме, что может замедлить работу компьютера при применении политики (при загрузке машины, если политика машинная, или входе пользователя в систему, если политика пользовательская).

Для включения политики «Синхронная работа с политиками» следует в разделе «Компьютер»/«Пользователь» → «Административные шаблоны» → «Система ALT» → «Управление пакетами» выбрать пункт «Синхронная работа с пакетами», в открывшемся окне установить отметку в поле «Включено» и нажать кнопку «ОК», для сохранения изменений (рис. 394).

Политики управления пакетами относятся к экспериментальным, поэтому на машинах с ОС Альт СП, где они применяются, должны быть включены экспериментальные групповые политики (о том, как включить экспериментальные групповые политики указано в п. 10.4.6.4.7).

Все настройки политики управления пакетами хранятся в файлах {GUID GPT}/Machine/Registry.pol и {GUID GPT}/User/Registry.pol.

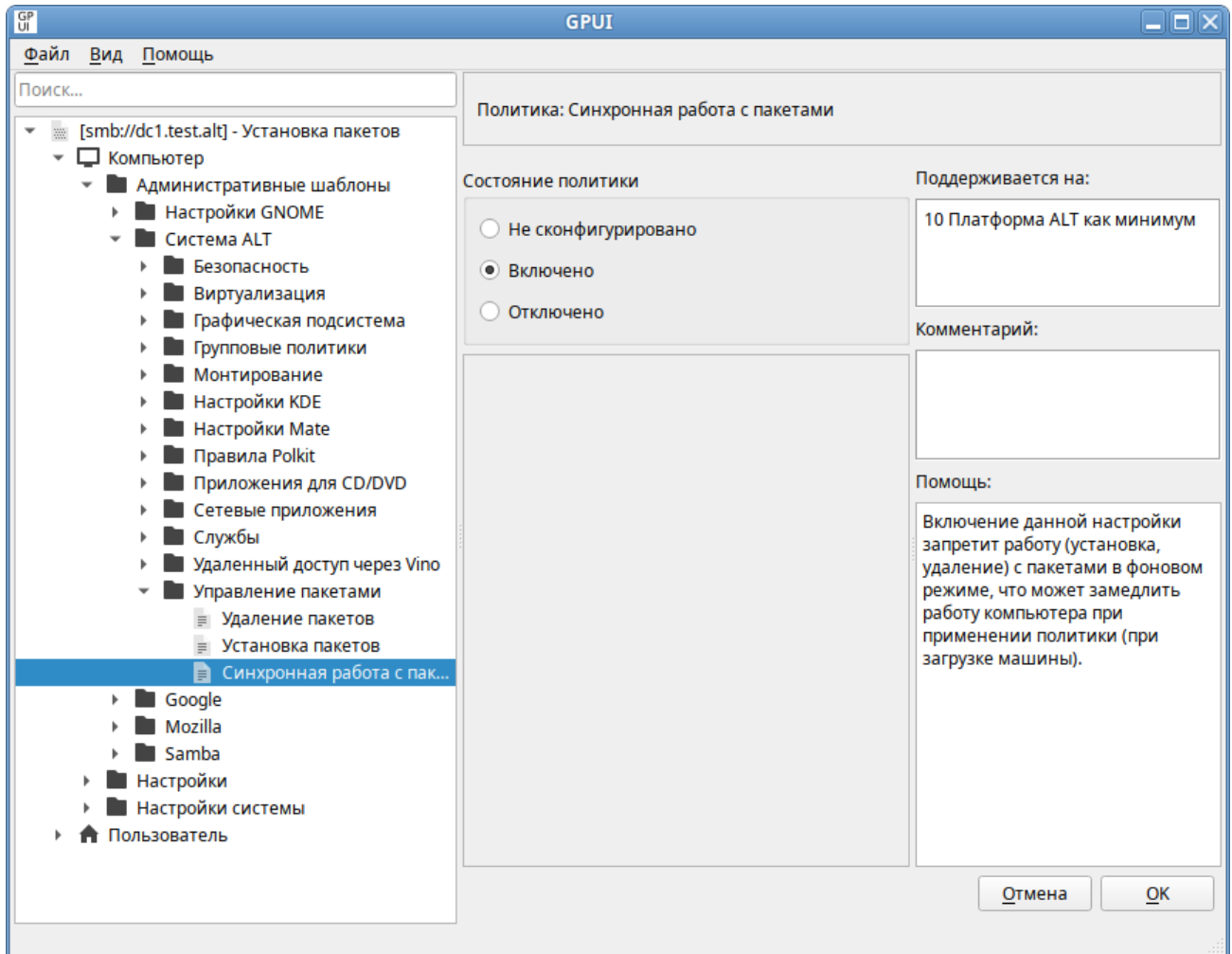


Рис. 394 – Политика «Синхронная работа с политиками»

Пример файла Registry.pol:

```
PReg
[Software\BaseALT\Policies\GPUUpdate;GlobalExperimental;;;]
[Software\BaseALT\Policies\Packages;Sync;;;]
[Software\BaseALT\Policies\Packages\Install;gimp;;;gimp]
[Software\BaseALT\Policies\Packages\Install;icinga2;;;icinga2]
[Software\BaseALT\Policies\Packages\Remove;python3-
tools;;;python3-tools]
```

10.4.6.4.7. Экспериментальные групповые политики

На машинах с ОС Альт СП, где применяются экспериментальных политики, должны быть включены «Экспериментальные групповые политики».

Для включения экспериментальных групповых политик следует в разделе «Компьютер»/«Пользователь» → «Административные шаблоны» → «Система ALT» → «Групповые политики» выбрать пункт «Экспериментальные групповые политики» и установить в открывшемся окне отметку в поле «Включено» (рис. 395).

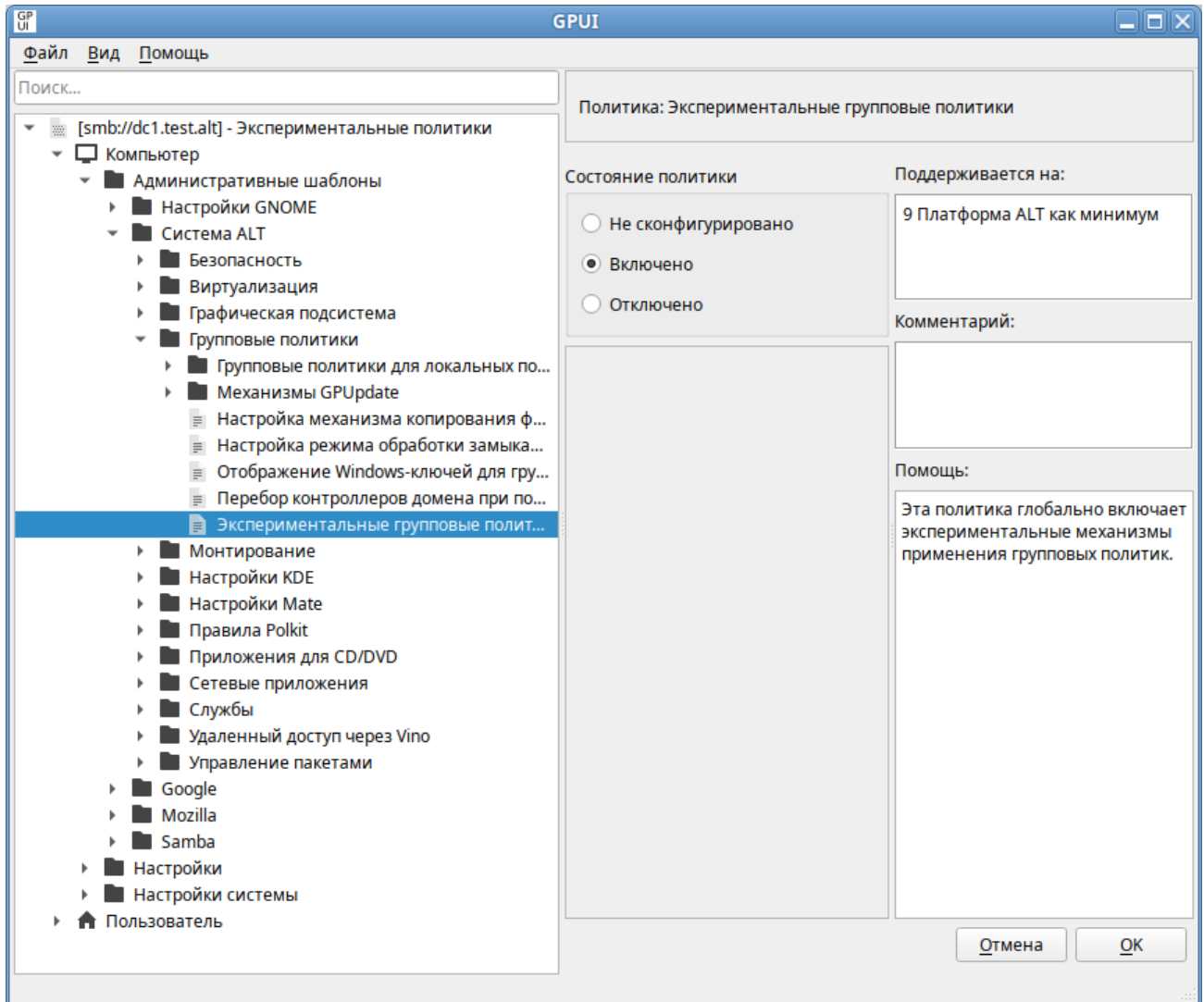


Рис. 395 – «Экспериментальные групповые политики»

10.4.6.4.8. Механизмы GPUupdate

Каждый механизм применения групповых политик можно отдельно включить или отключить. Для этого следует включить/отключить соответствующую политику в разделе «Компьютер»/«Пользователь» → «Административные шаблоны» → «Система ALT» → «Групповые политики» → «Механизмы GPUupdate».

Например, включить/отключить механизм групповых политик управления пакетами (Packages) можно, включив/отключив политики «Установка и удаление программ» или «Установка и удаление программ для пользователей» (рис. 396).

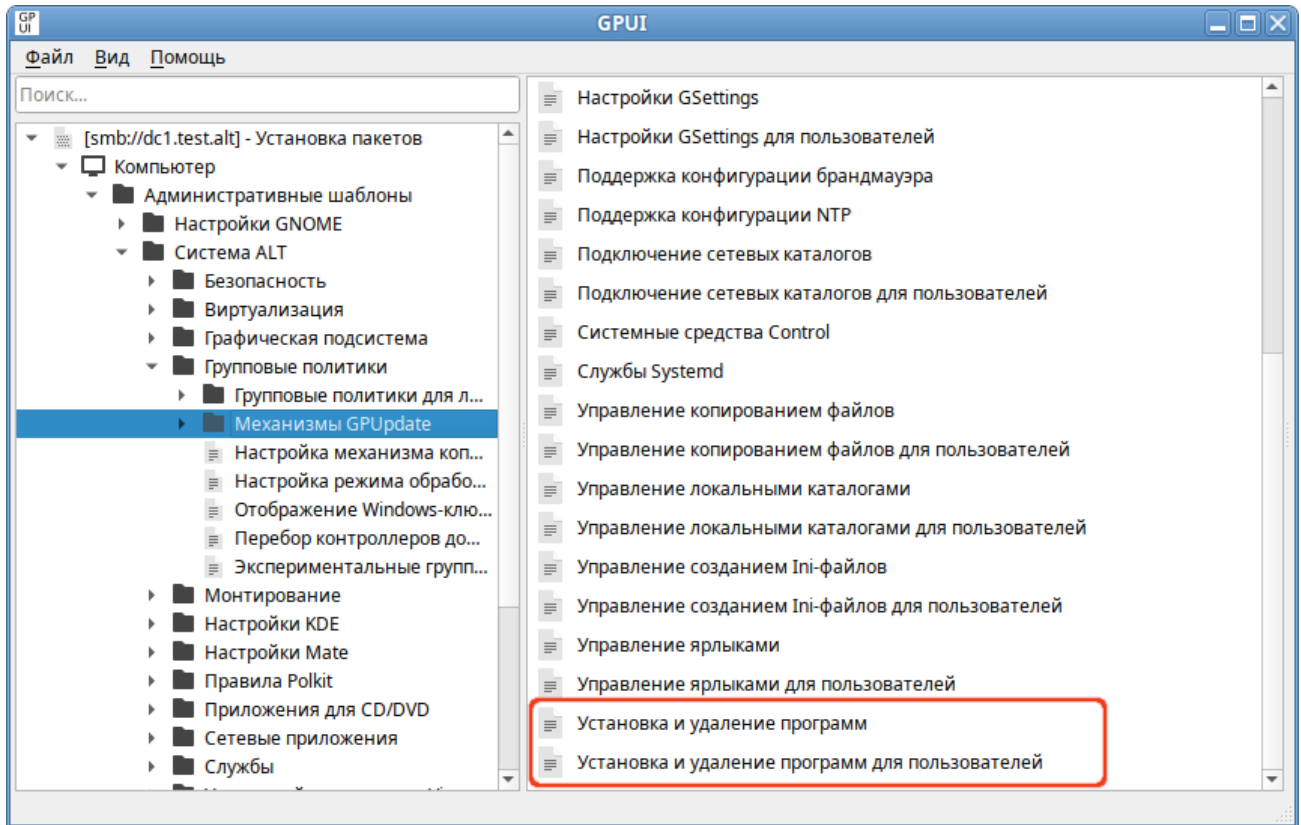


Рис. 396 – Механизм применения групповых политик

10.4.6.4.9. Управление политиками браузера Chromium

Эти групповые политики позволяют централизованно для компьютеров управлять настройками интернет-браузера Google Chromium.

Механизм Chromium в составе пакета `gupdate` формирует JSON-файл для веб-браузера из шаблонов групповых политик. Во время запуска веб-браузер Google Chromium считывает файл `/etc/chromium/policies/managed/policies.json` и применяет параметры групповых политик. Групповые политики на основе `policies.json` предоставляют кроссплатформенную совместимость, что позволяет управлять веб-браузерами в любом дистрибутиве «Альт» с установленным окружением рабочего стола.

Примечание. Данный механизм реализован только для машинных политик.

Примечание. Настройка политик для веб-браузера Chromium требует дополнительной установки ADMX-файлов Google Chrome (пакет `admx-chromium`).

Результат применения параметров групповой политики для Chromium можно проверить, указав в адресной строке URL: `chrome://policy` (рис. 397).

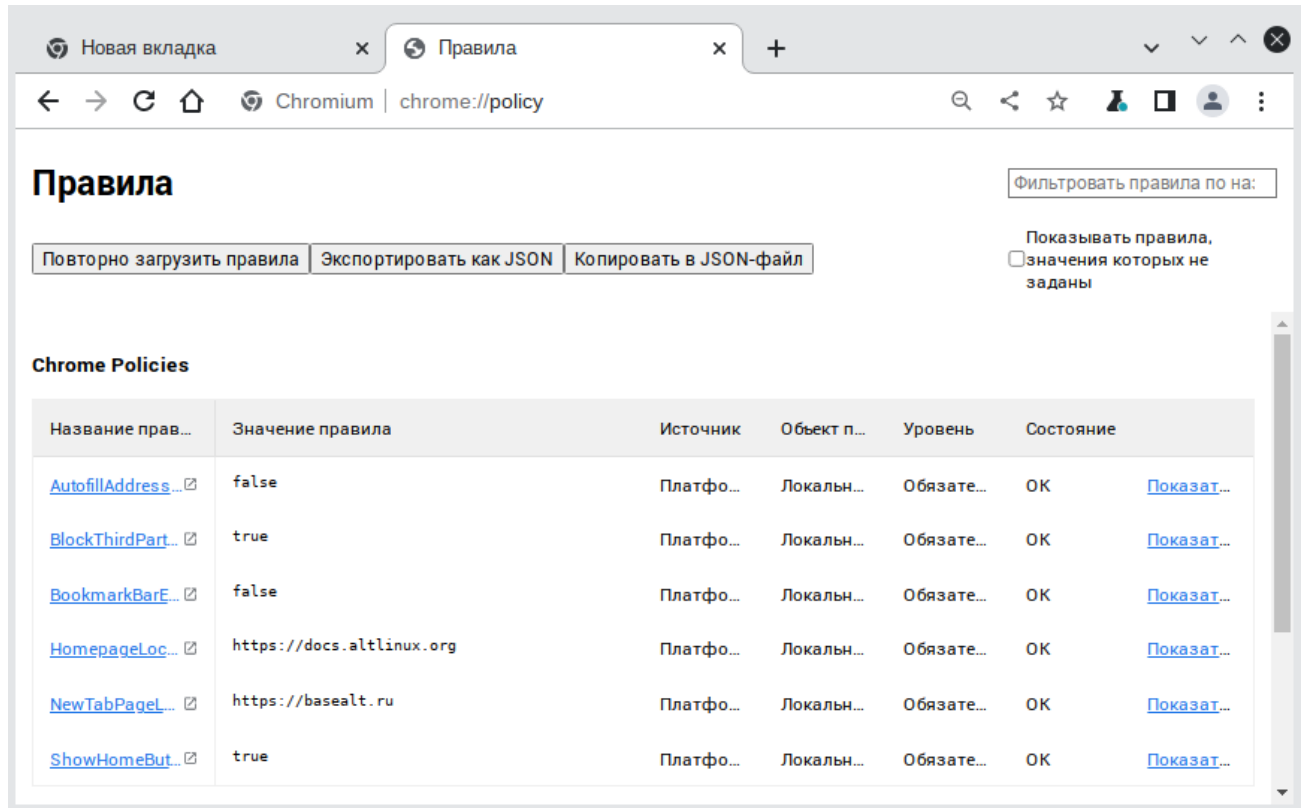


Рис. 397 – Активные политики веб-браузера Chromium

В качестве примера ниже рассмотрена политика установки URL домашней страницы.

Для редактирования политик веб-браузера Chromium следует перейти в «Компьютер» → «Административные шаблоны» → «Google» → «Google Chrome». Отобразится список политик (рис. 398).

Для установки URL домашней страницы следует выбрать пункт «Главная страница и страница быстрого доступа при запуске», щелкнуть левой кнопкой мыши на политике «Настройка URL домашней страницы», откроется диалоговое окно настройки политики. Выбрать параметр «Включено», в разделе «Описание» ввести URL и нажать кнопку «ОК» (рис. 399).

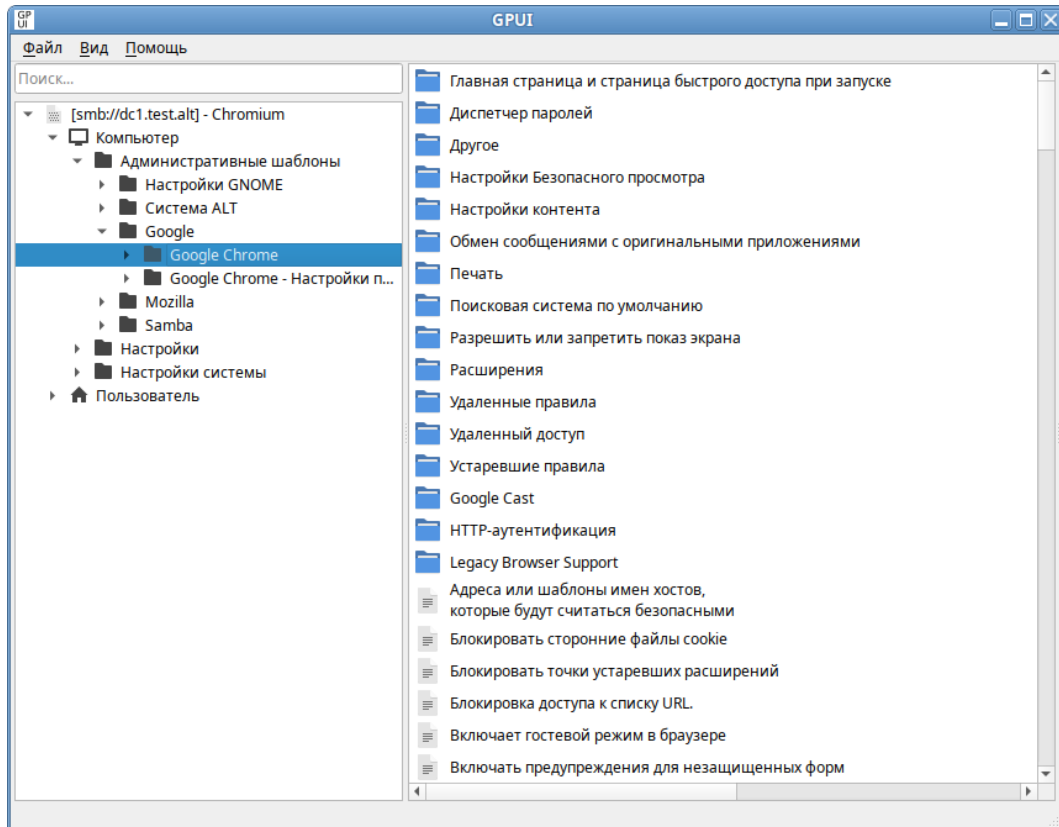


Рис. 398 – Политики настройки веб-браузера Chromium

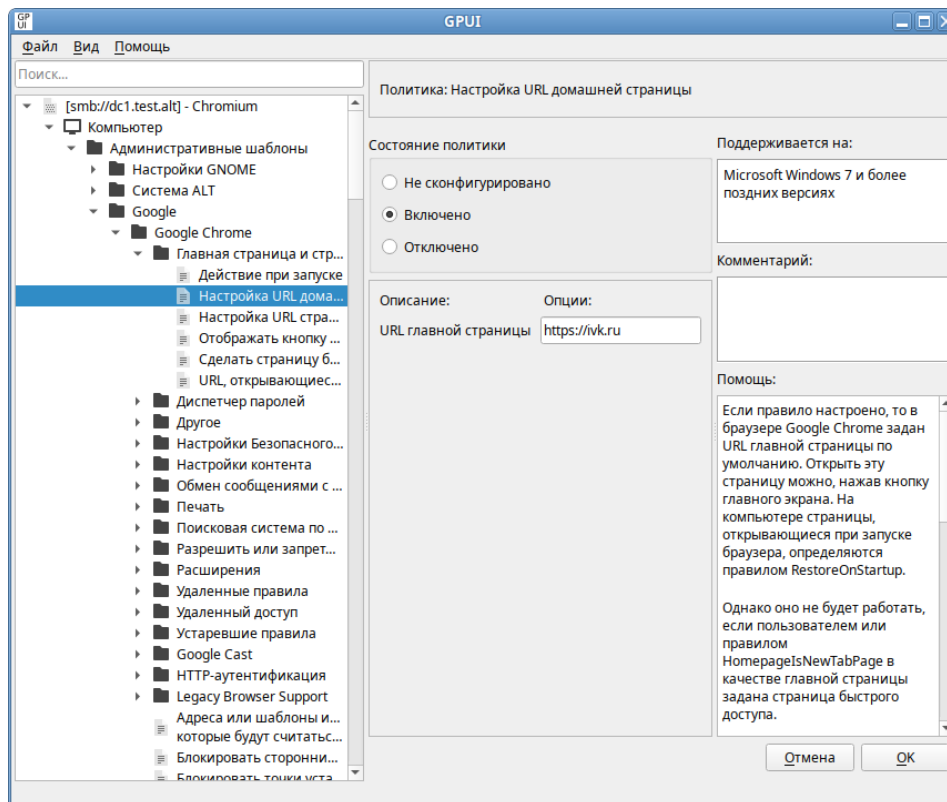


Рис. 399 – Установка URL домашней страницы Chromium

В результате применения данной политики будет установлена домашняя страница по умолчанию, а также будет заблокирована возможность изменения домашней страницы пользователем (рис. 400).

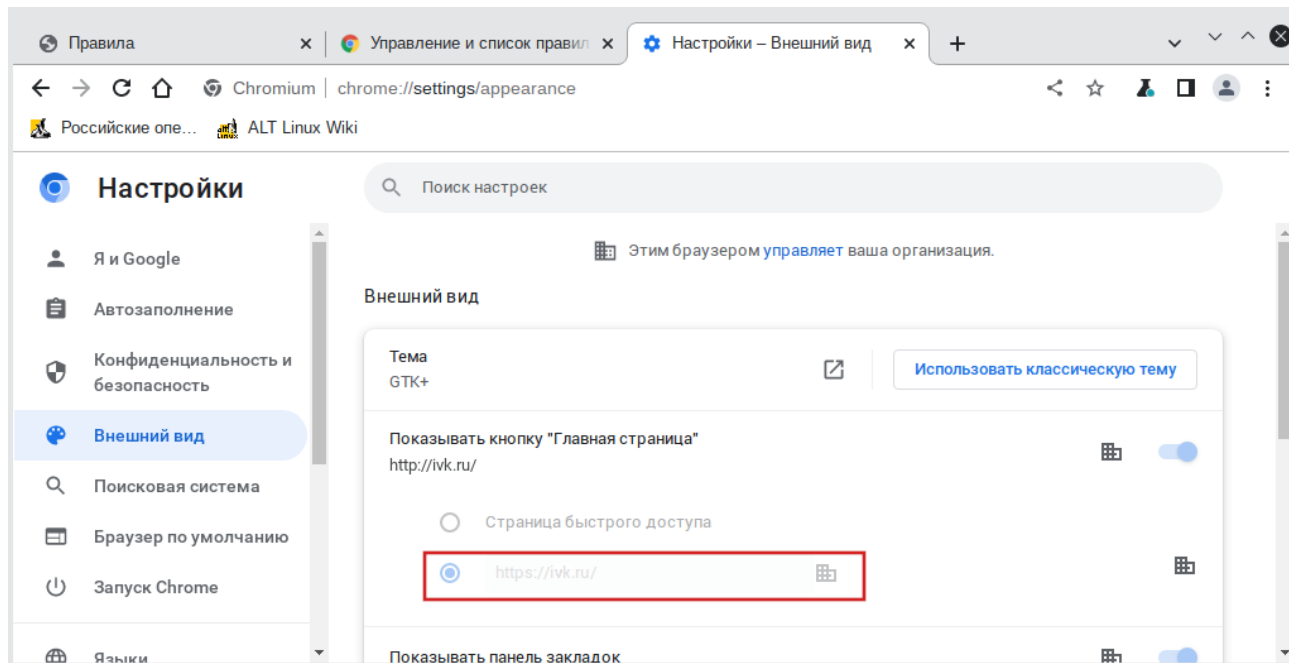


Рис. 400 – Настройки веб-браузера Chromium

Все настройки политики веб-браузера Chromium хранятся в файле {GUID GPT}/Machine/Registry.pol.

Пример файла Registry.pol:

```
PReg[Software\Policies\Google\Chrome;HomepageLocation;;;https://ivk.ru]
```

В таблице 52 описаны только некоторые политики. Полный список политик и их описание можно найти в веб-браузере Chromium, указав в адресной строке URL: chrome://policy и установив отметку на пункте «Показывать правила, значения которых не заданы».

Т а б л и ц а 52 – Примеры политик управляющих настройками браузера Chromium

Политика	Ключ	Описание
Действие при запуске	RestoreOnStartup	<p>Настройка процесса запуска Chromium.</p> <p>При выборе значения «Восстановить последний сеанс» или «Открыть список URL и восстановить последний сеанс» будут отключены некоторые функции, такие как удаление данных о работе в веб-браузере или сессионных файлов cookie при завершении работы.</p> <p>Если для политики указано значение «Открыть список URL и восстановить последний сеанс», веб-браузер будет восстанавливать предыдущий сеанс и открывать URL, заданные в политике «URL, открывающиеся при запуске», в отдельном окне. Если пользователь не закроет страницы с этими URL, они также будут восстановлены в новом сеансе.</p> <p>Если политика находится в состоянии «Включено», пользователи не смогут изменить эту настройку в Chromium</p>
Настройка URL домашней страницы	HomepageLocation	<p>Позволяет установить URL домашней страницы и запрещает пользователям его изменять.</p> <p>Если политика находится в состоянии «Включено», можно установить домашнюю страницу по умолчанию (открыть эту страницу в Chromium можно, нажав кнопку «Главная страница» на панели инструментов).</p> <p>Пользователи при этом не смогут изменить домашнюю страницу.</p> <p>Если политика находится в состоянии «Отключено», пользователи не смогут установить домашнюю страницу.</p> <p>Если политика находится в состоянии «Не сконфигурировано», пользователь может сам установить и изменить домашнюю страницу.</p> <p>Данная политика не будет работать, если пользователем или политикой «Сделать страницу быстрого доступа главной» в качестве главной страницы была задана страница быстрого доступа</p>
Настройка URL страницы быстрого доступа	NewTabPageLocation	<p>Позволяет установить URL страницы быстрого доступа по умолчанию и запрещает пользователям его изменять.</p> <p>Страница быстрого доступа появляется, когда пользователь открывает новую вкладку или окно.</p> <p>Политика не определяет, какие страницы открываются при запуске. Для этого применяется политика «Действие при запуске». Но если страница быстрого доступа используется в качестве главной или стартовой страницы, эта политика также распространяется и на них.</p> <p>Если политика находится в состоянии «Не сконфигурировано» или URL не указан, используется страница быстрого доступа, установленная по умолчанию</p>

Продолжение таблицы 52

Политика	Ключ	Описание
Отображать кнопку «Главная страница» на панели инструментов	ShowHomeButton	<p>Позволяет управлять отображением кнопки «Главная страница» на панели инструментов.</p> <p>Если политика находится в состоянии «Включено», кнопка «Главная страница» отображается на панели инструментов.</p> <p>Если политика находится в состоянии «Отключено», кнопка «Главная страница» не будет отображаться.</p> <p>Если эта политика настроена, пользователи не смогут изменить эту настройку в Chromium. В противном случае пользователи смогут добавить или скрыть кнопку главного экрана</p>
Сделать страницу быстрого доступа главной	HomepageIsNewTabPage	<p>Если политика находится в состоянии «Включено», в качестве главной страницы используется страница быстрого доступа. Заданный URL главной страницы игнорируется.</p> <p>Если политика находится в состоянии «Отключено» или «Не сконфигурировано», страница быстрого доступа открывается, только когда в качестве URL главной страницы указан путь <code>chrome://newtab</code>.</p> <p>Если эта политика настроена, пользователи не смогут изменить главную страницу в Chromium. Если политика не настроена, они смогут выбрать, устанавливать ли страницу быстрого доступа в качестве главной</p>
URL, открывающиеся при запуске	RestoreOnStartupURLs	<p>Если для политики «Действие при запуске» задано значение «Открыть одну или несколько страниц», в данной политике можно настроить список URL-адресов.</p> <p>В противном случае при запуске будет открываться страница быстрого доступа</p>
Включить сохранение паролей	PasswordManagerEnabled	<p>Если политика находится в состоянии «Включено» или «Не сконфигурировано», Chromium будет предлагать запоминать введенные пароли (а также предлагать их при следующем входе).</p> <p>Если политика находится в состоянии «Отключено», пользователям будут доступны только ранее сохраненные пароли, а сохранить новые будет нельзя.</p> <p>Если политика настроена, пользователи не могут изменить ее в Chromium. В противном случае пользователи при желании смогут отключить функцию сохранения паролей</p>
Включить поисковую систему по умолчанию	DefaultSearchProviderEnabled	<p>Если политика находится в состоянии «Включено», то при вводе в адресную строку текста (не URL) будет выполняться поиск в используемой по умолчанию поисковой системе.</p> <p>Задать поисковую систему по умолчанию можно с помощью других политик. Если значения для этих политик не установлены, пользователь может сам выбрать поисковую систему по умолчанию.</p>

Продолжение таблицы 52

Политика	Ключ	Описание
		Если политика находится в состоянии «Отключено», то поиск текста, введенного в адресную строку, не выполняется
Название поисковой системы по умолчанию	DefaultSearchProviderName	Если политика «Включить поисковую систему по умолчанию» включена, то данная политика задает название поисковой системы по умолчанию. Если параметр «Включить поисковую систему по умолчанию» не задан, то используется имя хоста, указанное в URL поискового запроса
Показ URL страницы быстрого доступа в поисковой системе по умолчанию	DefaultSearchProviderNewTabURL	Если политика «Включить поисковую систему по умолчанию» включена, то данная политика указывает URL поисковой системы, используемой для страницы быстрого доступа. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», страница быстрого доступа не будет использоваться
URL поиска для поисковой системы по умолчанию	DefaultSearchProviderSearchURL	Если политика «Включить поисковую систему по умолчанию» включена, то данная политика содержит URL поисковой системы, используемой по умолчанию. В URL должна быть строка '{searchTerms}', которая во время отправки запроса заменяется на текст пользователя. URL поисковой системы Google можно указать так: '{google:baseURL}search?q={searchTerms}&{google:RLZ}{google:originalQueryForSuggestion}{google:assistedQueryStats}{google:searchFieldtrialParameter}{google:searchClient}{google:sourceId}ie={inputEncoding}'
Включить панель закладок	BookmarkBarEnabled	Если политика находится в состоянии «Включено», в Chromium будет видна панель закладок. Если политика находится в состоянии «Отключено», панель закладок будет всегда скрыта. Если эта политика настроена, пользователи не смогут ее изменить. Если политика находится в состоянии «Не сконфигурировано», пользователи смогут самостоятельно решать, использовать эту функцию или нет.
Разрешить пользователям менять фон на странице быстрого доступа	NTPCustomBackgroundEnabled	Если политика находится в состоянии «Отключено», пользователи не смогут изменять фон страницы быстрого доступа. Уже используемые изображения удаляются без возможности восстановления. Если политика находится в состоянии «Включено» или «Не сконфигурировано», пользователи могут изменять фон страницы быстрого доступа
Блокировать изображения на этих сайтах	ImagesBlockedForUrls	Позволяет задать список шаблонов URL для указания сайтов (значение * не поддерживается для этой политики), на которых запрещен показ изображений. Если политика находится в состоянии «Включено», Chromium будет блокировать изображения на указанных сайтах.

Продолжение таблицы 52

Политика	Ключ	Описание
		Если политика находится в состоянии «Не сконфигурировано», то действует политика «Настройка изображений по умолчанию») при условии, что изображение задано. В противном случае применяются персональные настройки пользователя
Блокировка доступа к списку URL	URLBlocklist	Если политика находится в состоянии «Включено», страницы с запрещенными URL не загружаются (задаются шаблоны запрещенных URL). Если политика находится в состоянии «Не сконфигурировано», веб-браузер не блокирует URL. Формат шаблона URL должен соответствовать требованиям, указанным на странице https://www.chromium.org/administrators/url-blocklist-filter-format . В политике URLAllowlist можно задавать не более 1000 исключений
Всегда открывать PDF-файлы во внешнем приложении	AlwaysOpenPdfExternally	Если политика находится в состоянии «Включено», встроенное средство просмотра PDF-файлов в Chromium отключается, они начинают обрабатываться как скачанный контент, а пользователю разрешается открывать их в приложении, установленном по умолчанию. Если политика находится в состоянии «Отключено», для просмотра PDF-файлов будет использоваться плагин PDF (если он не отключен пользователем). Если политика находится в состоянии «Не сконфигурировано», пользователи смогут настраивать этот параметр самостоятельно
Всегда указывать место для скачивания	PromptForDownloadLocation	Если политика находится в состоянии «Включено», то при скачивании каждого файла пользователь должен указать, в какой каталог его сохранить. Если политика находится в состоянии «Отключено», скачивание выполняется без запроса каталога для сохранения. Если политика находится в состоянии «Не сконфигурировано», пользователи могут выбрать каталог, в который всегда будут сохраняться файлы
Выбор каталога для скачиваний	DownloadDirectory	В этой политике указывается каталог, в котором веб-браузер Chromium сохраняет скачиваемые файлы. Данный каталог используется, даже если пользователь выбрал каталог для сохранения или установил флаг, позволяющий выбирать каталог при каждом скачивании файла. Эта политика отменяет действие политики DefaultDownloadDirectory. Если политика находится в состоянии «Не сконфигурировано», веб-браузер Chromium скачивает файлы в каталог по умолчанию, а пользователь может его изменить. Список переменных можно посмотреть на странице https://www.chromium.org/administrators/policy-list-3/user-data-directory-variables

Продолжение таблицы 52

Политика	Ключ	Описание
Доступ к поисковой системе по умолчанию в контекстном меню	DefaultSearchProviderContextMenuAccessAllowed	Позволяет использовать поисковую систему по умолчанию в контекстном меню. Если политика находится в состоянии «Включено» или «Не сконфигурировано», поиск в системе по умолчанию будет доступен в контекстном меню. Если политика находится в состоянии «Отключено», поиск будет недоступен в контекстном меню. Значение этой политики применяется только в том случае, если включена политика «Включить поисковую систему по умолчанию»
Доступность режима инкогнито	IncognitoModeAvailability	Определяет, может ли пользователь просматривать страницы в Chromium в режиме инкогнито. Если политика находится в состоянии «Включено» или значение не задано, страницы можно открывать в режиме инкогнито. Если политика находится в состоянии «Отключено», пользователи не смогут открывать страницы в режиме инкогнито. Если для политики выбрано значение «Включить принудительно», страницы можно просматривать ТОЛЬКО в режиме инкогнито
Удаление истории просмотров и загрузок веб-браузера	AllowDeletingBrowserHistory	Определяет, может ли пользователь удалять историю просмотров и скачиваний. Если политика находится в состоянии «Включено» или «Не сконфигурировано», то историю просмотров и скачиваний можно удалить. Если политика находится в состоянии «Отключено», то историю просмотров и скачиваний удалить нельзя
Разрешить вызов окна выбора файлов	AllowFileSelectionDialogs	Если политика находится в состоянии «Включено» или «Не сконфигурировано», то пользователи смогут открывать в Chromium окна выбора файлов. Если политика находится в состоянии «Отключено», и пользователь выполняет действия, для которых нужно открыть окно выбора файлов (например, импортирует закладки, загружает файлы, сохраняет ссылки и т. д.), вместо окна отображается сообщение и предполагается, что пользователь нажал кнопку «Отмена» в окне выбора файлов
Включить поисковые подсказки	SearchSuggestEnabled	Если политика находится в состоянии «Включено», в адресной строке Chromium при поиске будут появляться подсказки. Если политика находится в состоянии «Отключено», поисковые подсказки не отображаются. Эта политика не влияет на показ в строке поиска закладок и страниц из истории просмотров. Если политика настроена, пользователи не могут изменить ее. Если политика не настроена, подсказки при поиске будут включены, но пользователи смогут отключить их в любое время

Продолжение таблицы 52

Политика	Ключ	Описание
Настройка изображений по умолчанию	DefaultImagesSetting	<p>Если политика находится в состоянии «Включено» и выбрано значение 1 – «Разрешить показ изображений на всех сайтах», на всех сайтах могут показываться изображения. При значении 2 – «Запретить показ изображений на всех сайтах», показ изображений на сайтах запрещен.</p> <p>Если политика находится в состоянии «Не сконфигурировано», показ изображений разрешен, но пользователи могут изменять этот параметр</p>
Разрешить полноэкранный режим	FullscreenAllowed	<p>Если политика находится в состоянии «Включено» или «Не сконфигурировано», то при наличии разрешений пользователи, приложения и расширения смогут включать полноэкранный режим, в котором виден только контент веб-страниц.</p> <p>Если политика находится в состоянии «Отключено», то полноэкранный режим будет заблокирован для всех пользователей, приложений и расширений</p>
Включить анонимный сбор данных	UrlKeyedAnonymizedDataCollectionEnabled	<p>Если политика находится в состоянии «Включено», то всегда выполняется анонимный сбор данных о URL (эти сведения отправляются в Google с целью улучшить поиск и просмотр веб-страниц).</p> <p>Если политика находится в состоянии «Отключено», сбор данных о URL не выполняется.</p> <p>Если политика находится в состоянии «Не сконфигурировано», пользователь может разрешить или запретить анонимный сбор данных о URL</p>
Управляемые закладки	ManagedBookmarks	<p>Политика позволяет установить список закладок в Chromium.</p> <p>Если политика настроена, будет создан список закладок. Каждая закладка представляет собой словарь, где ключам name и url соответствуют значения – название закладки и URL-адрес сайта</p> <pre> ([{"name": "Документация", "url": "docs.altlinux.org"}, {"name": "Wiki", "url": "altlinux.org"}]). </pre> <p>По умолчанию папка называется «Управляемые закладки».</p> <p>Чтобы изменить это название, нужно добавить в правило дополнительный словарь с единственным ключом toplevel_name и названием папки в качестве значения. Также можно задать подпапку для закладок. Для этого вместо ключа url следует использовать ключ children, а в качестве его значения указать список вложенных закладок или папок</p> <pre> ([{"toplevel_name": "ALT"}, {"name": "BaseALT", "url": "basealt.ru"}, {"name": "ALT docs", "children": [{"name": "Документация", "url": "docs.altlinux.org"}, {"name": "Wiki", "url": "altlinux.org"}]}]). </pre>

Продолжение таблицы 52

Политика	Ключ	Описание
		<p>Chromium дополняет неполные URL так же, как при их вводе в адресной строке. Например, адрес altlinux.org будет преобразован в https://altlinux.org/.</p> <p>Пользователи не смогут изменять папки с закладками, а только скрывать их на панели. Управляемые закладки не синхронизируются с аккаунтом пользователя, а расширения не могут их изменять</p>
Отключить синхронизацию данных с Google	SyncDisabled	<p>Если политика находится в состоянии «Включено», синхронизация данных в Chromium с помощью сервисов, размещенных в Google, отключается. Полностью отключить сервис «Chrome Sync» можно через Google Admin console.</p> <p>Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователи могут самостоятельно решать, использовать ли им сервис «Chrome Sync»</p>
Включает гостевой режим в браузере	BrowserGuestModeEnabled	<p>Если политика находится в состоянии «Включено» или «Не сконфигурировано», разрешается использовать гостевой доступ. При гостевом доступе все окна для профилей Chromium открываются в режиме инкогнито. При гостевом доступе все окна для профилей Chromium открываются в режиме инкогнито.</p> <p>Если политика находится в состоянии «Отключено», в веб-браузере не разрешается использовать гостевые профили</p>
Удаление данных о работе в веб-браузере при выходе	ClearBrowsingDataOnExitList	<p>Политика позволяет настроить список данных о работе в веб-браузере, которые должны удаляться, когда пользователь закрывает все окна веб-браузера. Можно указать следующие типы данных:</p> <ul style="list-style-type: none"> - browsing_history (история веб-браузера); - download_history (история скачиваний); - cookies_and_other_site_data (файлы cookie и другие данные сайтов); - cached_images_and_files (изображения и другие файлы, сохраненные в кэше); - password_signin (пароли); - autofill (автозаполнение); - site_settings (настройки сайтов); - hosted_app_data (данные размещенных приложений). <p>У этой политики нет приоритета над политикой «Удаление истории просмотров и загрузок веб-браузера».</p> <p>Эта политика работает, если политика «Отключить синхронизацию данных с Google» находится в состоянии «Включено». В противном случае политика игнорируется.</p>

Продолжение таблицы 52

Политика	Ключ	Описание
		<p>Если Chromium закрывается непредвиденно (например, из-за сбоя в работе веб-браузера или ОС), данные о работе в веб-браузере удаляются при следующей загрузке профиля. Если политика находится в состоянии «Отключено», то данные о работе, при закрытии веб-браузера, не удаляются</p>
Задать объем кэша в байтах	DiskCacheSize	<p>Если для политики задано значение «None», Chromium использует объем кэша по умолчанию для хранения кэшированных файлов на диске. В этом случае пользователи не могут изменить правило.</p> <p>Если политика находится в состоянии «Включено», Chromium будет использовать указанный размер кэша независимо от того, указали ли пользователи значение экспериментального параметра <code>--disk-cache-size</code>. Объем кэша задается в байтах, например, чтобы задать размер кэша 300МБ, нужно указать 314572800. Значения меньше нескольких мегабайтов округляются.</p> <p>Если политика находится в состоянии «Не сконфигурировано», Chromium использует объем по умолчанию. В этом случае пользователи могут менять размер кэша с помощью экспериментального параметра <code>--disk-cache-size</code>.</p> <p>Указанное в правиле значение используется различными подсистемами в веб-браузере как справочное. Поэтому фактический объем используемого дискового пространства может превышать указанное значение, но будет иметь такой же порядок</p>
Список разрешенных серверов для аутентификации	AuthServerAllowlist	<p>Это правило указывает, какие серверы можно использовать для встроенной проверки подлинности Windows (IWA). Встроенная проверка подлинности включается, только когда Chromium получает запрос на аутентификацию от прокси-сервера или от сервера из списка разрешенных.</p> <p>Если политика находится в состоянии «Не сконфигурировано», Chromium отвечает на запросы IWA только после того, как определяет, находится ли сервер в интранете. Если сервер находится в Интернете, Chromium игнорирует поступающие от него IWA запросы (веб-сайту не разрешается использовать аутентификацию SPNEGO с помощью веб-браузера). Названия серверов нужно разделять запятыми. Допустимы подстановочные знаки (*)</p>
Позволяет управлять расширениями	ExtensionSettings	<p>Это правило контролирует настройки управления расширениями в Chromium, включая те, которые заданы другими правилами. Оно заменяет любые ранее действовавшие правила.</p> <p>Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователи могут самостоятельно настраивать расширения.</p>

Продолжение таблицы 52

Политика	Ключ	Описание
		<p>Если политика находится в состоянии «Включено», настройки расширений задает администратор с помощью кода, указанного в параметрах политики:</p> <ul style="list-style-type: none"> - идентификатор расширения или URL обновления привязывается только к одной конкретной настройке; - идентификатор * действует на все расширения, для которых в политике не задана отдельная конфигурация. <p>Если указан URL обновления, заданная конфигурация применяется ко всем расширениям, в манифесте которых приведен этот URL.</p> <p>Пример значения:</p> <pre> { "hdokiejnpimakedhajhdlcegeplioahd": { "installation_mode": "force_installed", "update_url": "https://clients2.google.com/service/update2/crx" }, "pioclpoplcldbaefihamjohnefbikjilc": { "installation_mode": "force_installed", "update_url": "https://clients2.google.com/service/update2/crx" } } </pre> <p>Параметры политики:</p> <ol style="list-style-type: none"> 1) <code>allowed_types</code> – типы приложений и расширений, которые пользователям разрешено устанавливать в веб-браузере (допустимые строки: «<code>extension</code>», «<code>hosted_app</code>», «<code>legacy_packaged_app</code>», «<code>tplatform_appeme</code>», «<code>theme</code>», «<code>user_script</code>»). Используется только для настройки конфигурации по умолчанию со значением *; 2) <code>blocked_install_message</code> – уведомление (не более 1000 символов), которое будет появляться на устройствах пользователей при попытке установить запрещенные расширения; 3) <code>blocked_permissions</code> – запрещает пользователям устанавливать и запускать расширения, требующие разрешений API (список доступных разрешений указан в манифесте расширения); 4) <code>installation_mode</code> – указывает, разрешено ли добавлять заданные расширения. Допустимые режимы: <ul style="list-style-type: none"> - <code>allowed</code> – пользователи могут установить это расширение (поведение по умолчанию); <code>blocked</code> – пользователи не могут установить это расширение; - <code>removed</code> – пользователи не могут установить это расширение. Если расширение было установлено, оно будет удалено;

Окончание таблицы 52

Политика	Ключ	Описание
		<p>-force_installed – расширение устанавливается автоматически. Пользователи не могут его удалить. В этом режиме нужно указать ссылку для скачивания расширения (параметр update_url);</p> <p>-автоматически – пользователи могут его удалить. В этом режиме нужно указать ссылку для скачивания расширения (параметр update_url);</p> <p>5) install_sources – список URL страниц, с которых разрешено загружать и устанавливать расширения. Нужно разрешить URL расположения CRX-файла и страницы, с которой начинается скачивание (то есть URL перехода);</p> <p>6) minimum_version_required – отключает расширения (в том числе установленные принудительно) более ранних версий, чем определено этим параметром. Формат строки версии аналогичен формату, который используется в манифесте расширения;</p> <p>7) update_url – определяет, откуда загружается расширение. Можно указать URL интернет-магазина Chrome, Opera или использовать XML-файл:</p> <p>-если расширение размещено в интернет-магазине Chrome, следует указать https://clients2.google.com/service/update2/crx</p> <p>-если расширение размещено в интернет-магазине Opera, следует указать https://extension-updates.opera.com/api/omaha/update/</p> <p>8) override_update_url – указывает, что для всех последующих обновлений расширения будет использоваться URL из поля update_url или update в политике ExtensionInstallForcelist. Если это политика не настроена или отключена, будет использоваться URL из манифеста расширения;</p> <p>9) verified_contents_url – указывает путь до файла «extension.verified_contents». С его помощью расширение проверяется на доверие (используется, если нет доступа в интернет);</p> <p>10) normal_installed – расширение устанавливается runtime_allowed_hosts – разрешает взаимодействие расширений с указанными сайтами, даже если они указаны в поле runtime_blocked_hosts. Можно указать до 100 сайтов;</p> <p>11) toolbar_pin – определяет, закреплён ли значок расширения на панели инструментов. Возможные значения:</p> <p>-force_pinned – значок расширения закреплён на панели инструментов и постоянно виден. Пользователь не может скрыть его в меню расширения;</p> <p>-default_unpinned – расширение скрыто в меню расширений (по умолчанию), пользователь может закрепить его на панели инструментов.</p>

10.4.6.4.10. Управление политиками веб-браузера Firefox

Эти групповые политики позволяют централизованно для компьютеров управлять настройками веб-браузера Mozilla Firefox.

Механизм Firefox в составе пакета `groupupdate` формирует JSON-файл для веб-браузера из шаблонов групповых политик. Во время запуска веб-браузер Mozilla Firefox считывает собственный файл `policies.json` и применяет параметры групповых политик. Групповые политики на основе `policies.json` предоставляют кроссплатформенную совместимость, что позволяет управлять веб-браузерами в любом дистрибутиве «Альт» с установленным окружением рабочего стола.

Путь к файлу `policies.json`, в зависимости от версии веб-браузера Mozilla Firefox:

- `/etc/firefox/policies` – новые версии;
- `/usr/lib64/firefox/distribution` – старые версии.

Примечание. Данный механизм реализован только для машинных политик.

Примечание. Настройка политик для веб-браузера Mozilla Firefox требует дополнительной установки ADMX-файлов Firefox (пакет `admx-firefox`).

Результат применения параметров групповой политики для Mozilla Firefox можно проверить, указав в адресной строке URL: `about:policies#active` (рис. 401).

В качестве примера ниже рассмотрена политика установки URL домашней страницы.

Для редактирования политик веб-браузера Mozilla Firefox следует перейти в «Компьютер» → «Административные шаблоны» → «Mozilla» → «Firefox» (рис. 402).

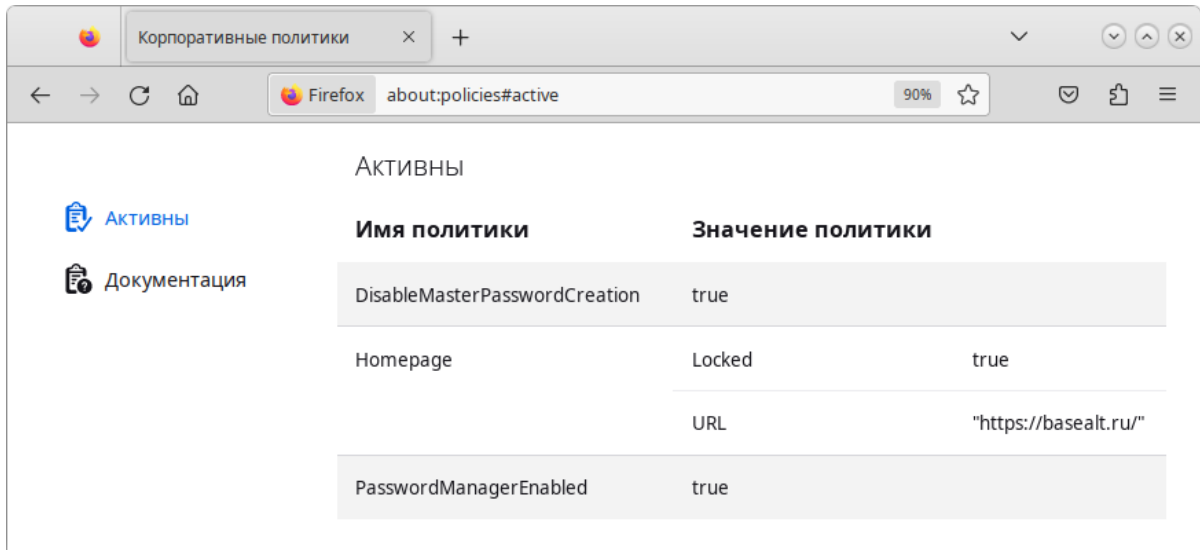


Рис. 401 – Активные политики веб-браузера Mozilla Firefox

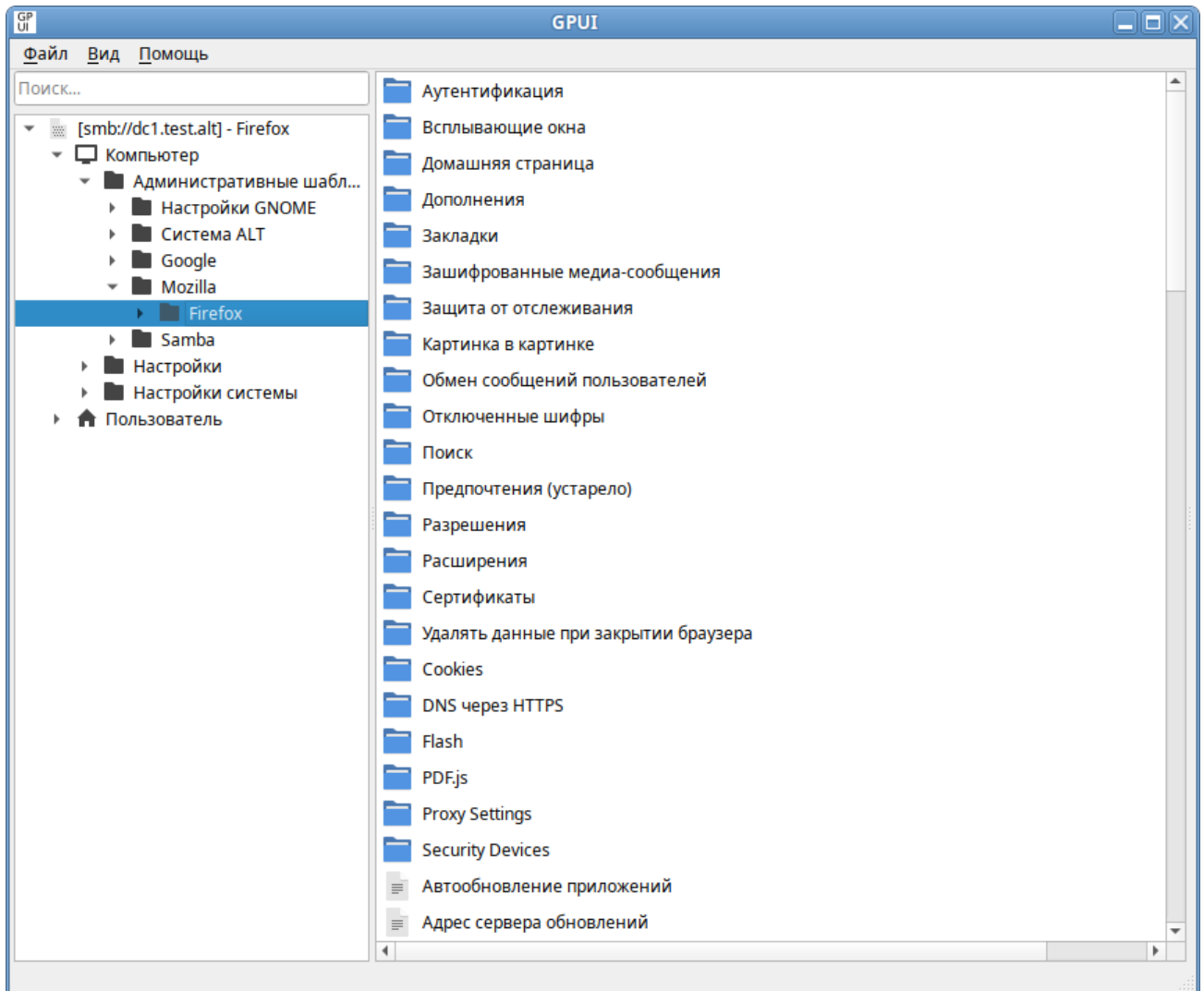


Рис. 402 – Политики настройки веб-браузера Mozilla Firefox

Раскрыть группу «Домашняя страница», щелкнуть левой кнопкой мыши на политике «URL для домашней страницы», откроется диалоговое окно настройки политики. Выбрать параметр «Включено», в разделе «Описание» ввести URL и нажать кнопку «ОК» (рис. 403).

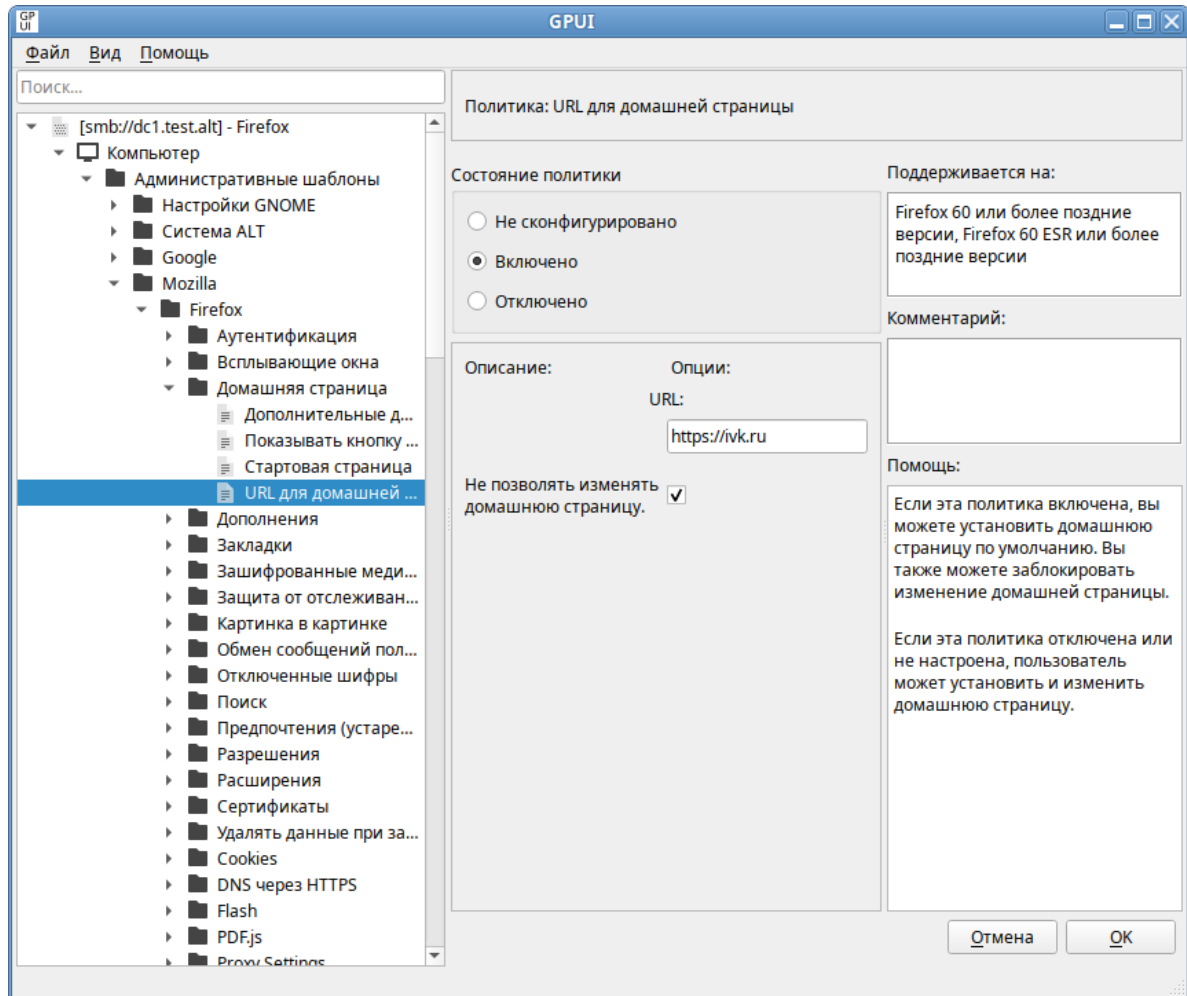


Рис. 403 – Диалоговое окно «URL для домашней страницы»

В результате применения данной политики будет установлена домашняя страница по умолчанию, а также будет заблокирована возможность изменения домашней страницы пользователем (рис. 404).

Все настройки политики веб-браузера Mozilla Firefox хранятся в файле {GUID GPT}/Machine/Registry.pol.

Пример файла Registry.pol:

```
PReg[Software\Policies\Mozilla\Firefox\Homepage;URL;;;https://ivk.ru]
[Software\Policies\Mozilla\Firefox\Homepage;Locked;;;]
```

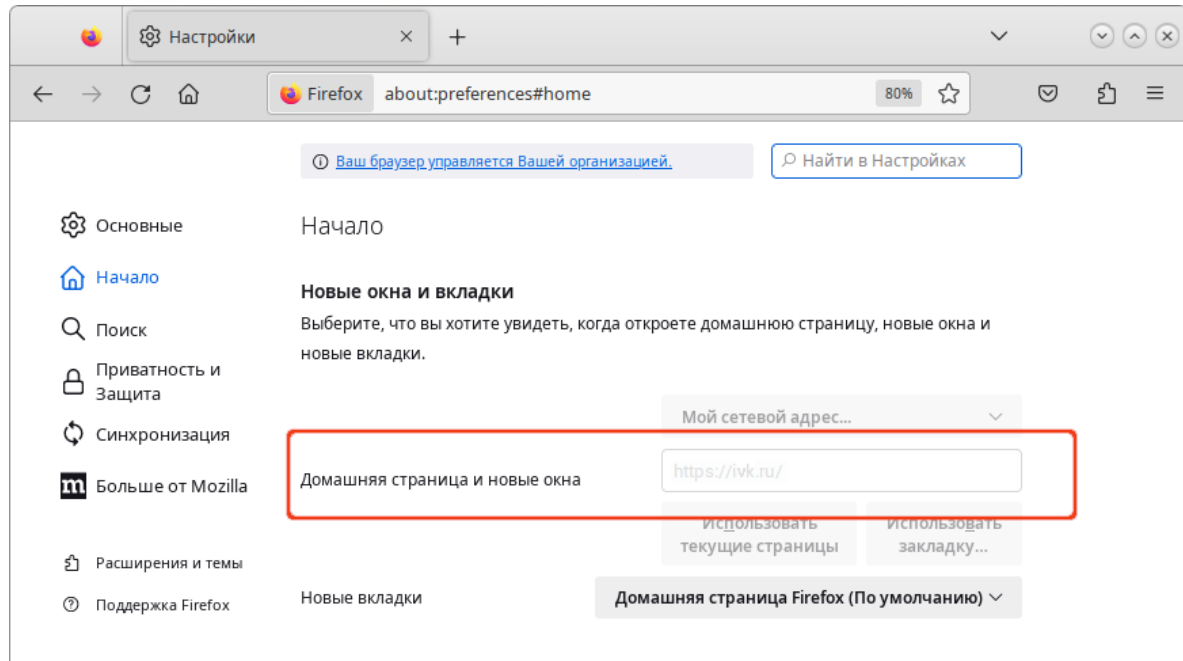


Рис. 404 – Настройки веб-браузера Mozilla Firefox

Примеры политик управляющих настройками веб-браузера Mozilla Firefox представлены в таблице 53. Полный список политик и их описание можно найти в веб-браузере Mozilla Firefox, указав в адресной строке URL:

`about:policies#documentation`

Т а б л и ц а 53 – Примеры политик управляющих настройками веб-браузера Mozilla Firefox

Политика	Ключ	Описание
Менеджер паролей	PasswordManagerEnabled	Позволяет запретить доступ к менеджеру паролей через настройки и блокирует <code>about:logins</code> . Если эта политика находится в состоянии «Включено» или «Не сконфигурировано», менеджер паролей доступен в настройках и на странице <code>about:logins</code> . Если эта политика находится в состоянии «Отключено», Firefox запрещает доступ к менеджеру паролей через настройки и блокирует <code>about:logins</code>
Отключить создание мастер-пароля	DisableMasterPasswordCreation	Позволяет отключить возможность установить мастер-пароль (основной пароль). Если эта политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователи могут создать мастер-пароль. Если эта политика находится в состоянии «Включено», то она работает так же, как установка политики «Основной (главный) пароль» состоянии «Отключено», и пользователи не могут создать мастер-пароль.

Продолжение таблицы 53

Политика	Ключ	Описание
		Если используются и политика «Отключить создание мастер-пароля», и «Основной (главный) пароль», то политика «Отключить создание мастер-пароля» имеет приоритет
Предлагать сохранить логины	OfferToSaveLogins	Позволяет настроить будет ли Firefox предлагать запоминать сохраненные логины и пароли. Если политика находится в состоянии «Отключено», Firefox не будет предлагать сохранять логины и пароли веб-сайтов. Если политика находится в состоянии «Включено» или «Не сконфигурировано», Firefox будет предлагать сохранять логины и пароли веб-сайтов
Отключить инструменты разработчика	DisableDeveloperTools	Позволяет управлять доступом к инструментам разработчика. Если политика находится в состоянии «Включено», инструменты веб-разработчика недоступны в Firefox. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», инструменты веб-разработчика доступны в Firefox
Отключить приватный просмотр	DisablePrivateBrowsing	Запрещает доступ к приватному просмотру. Если политика находится в состоянии «Включено», приватный просмотр запрещен. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», приватный просмотр разрешен
Нет закладок по умолчанию	NoDefaultBookmarks	Отключает создание закладок по умолчанию (идуших вместе с Firefox), и смарт-закладки (часто посещаемые, недавние). Если политика находится в состоянии «Включено», закладки по умолчанию и смарт-закладки (наиболее посещаемые, недавние теги) не создаются. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», создаются закладки по умолчанию и смарт-закладки (наиболее посещаемые, последние теги). Примечание: эта политика эффективна только в том случае, если она используется до первого запуска профиля
Запрос места загрузки	PromptForDownloadLocation	Спрашивает, куда сохранять файлы при загрузке. Если политика находится в состоянии «Отключено», файлы будут сохраняться в каталог, указанный в настройках (пользователю не предлагается указать место для загрузки файла). Если политика находится в состоянии «Включено», пользователю будет всегда выдаваться запрос на сохранение файла. Если политика находится в состоянии «Не сконфигурировано», пользователю будет выдаваться запрос на сохранение файла, но он может изменить значение по умолчанию

Продолжение таблицы 53

Политика	Ключ	Описание
Блокировка редактора настроек (about:config)	BlockAboutConfig	Блокирует доступ к странице about:config. Если эта политика находится в состоянии «Включено», пользователь не может получить доступ к about:config. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь может получить доступ к about:config
Блокировка страницы управления профилями (about:profiles)	BlockAboutProfiles	Блокирует доступ к странице about:profiles. Если политика находится в состоянии «Включено», пользователь не может получить доступ к профилям about:profiles. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь может получить доступ к профилям about:profiles
Блокировка информации об устранении неполадок	BlockAboutSupport	Блокирует доступ к странице about:support. Если политика находится в состоянии «Включено», пользователь не может получить доступ к информации для устранения неполадок или about:support. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь может получить доступ к информации для устранения неполадок или about:support
Captive Portal (портал захвата)	CaptivePortal	Включает или отключает тест соединения (поддержку перехватывающего портала). Если политика находится в состоянии «Отключено», то поддержка captive portal отключена. Если политика находится в состоянии «Включено» или «Не сконфигурировано», то поддержка captive portal включена. П р и м е ч а н и е . Веб-браузер Mozilla Firefox при запуске проверяет, требует ли используемое сетевое соединение вход в систему. Во время теста Firefox пытается подключиться к <code>http://detectportal.firefox.com/success.txt</code> , чтобы проверить возможность соединения с этим адресом. Этот адрес также используется для проверки поддержки активного сетевого соединения IPv6. Отключение этой функциональности уменьшает количество автоматических подключений и может немного ускорить запуск веб-браузера
Отключить встроенную программу просмотра PDF (PDF.js)	DisableBuiltinPDFViewer	Отключает PDF.js, встроенный просмотрщик PDF в Firefox. Если политика находится в состоянии «Включено», файлы PDF не просматриваются в Firefox. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», файлы PDF просматриваются в Firefox

Продолжение таблицы 53

Политика	Ключ	Описание
Отключить команды обратной связи	DisableFeedbackCommands	Отключает команды отправки отзывов в меню «Справка» («Отправить отзыв...» и «Сообщить о поддельном сайте...»). Если политика находится в состоянии «Включено», пункты меню «Отправить отзыв...» и «Сообщить о поддельном сайте...» недоступны из меню «Справка». Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пункты меню «Отправить отзыв...» и «Сообщить о поддельном сайте...» доступны из меню «Справка»
Отключить снимки экрана Firefox	DisableFirefoxScreenshots	Отключает функцию Firefox Screenshots. Если политика находится в состоянии «Включено», снимки экрана Firefox недоступны. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», доступны скриншоты Firefox
Отключить учетные записи Firefox	DisableFirefoxAccounts	Отключает службы, основанные на Аккаунте Firefox, включая синхронизацию. Если политика находится в состоянии «Включено», учетные записи Firefox отключены, в том числе отключена синхронизация. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», доступны Аккаунты Firefox и синхронизация
Отключить исследования Firefox	DisableFirefoxStudies	Запрещает Firefox выполнять исследования. Если политика находится в состоянии «Включено», Firefox никогда не будет проводить исследования SHIELD или опросы Heartbeat. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь может включить исследования SHIELD или опросы Heartbeat. Для получения дополнительной информации см. https://support.mozilla.org/en-US/kb/shield и https://wiki.mozilla.org/Firefox/Shield/Heartbeat
Отключить кнопку «Забыть»	DisableForgetButton	Закрывает доступ к кнопке «Забыть». Если политика находится в состоянии «Включено», кнопка «Забыть о части истории веб-серфинга» недоступна. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», кнопка «Забыть о части истории веб-серфинга» доступна
Запретить показывать пароли в сохраненных логинах	DisablePasswordReveal	Не позволяет просматривать пароли у сохраненных логинов. Если политика находится в состоянии «Включено», пользователи не могут отображать пароли в сохраненных логинах.

Продолжение таблицы 53

Политика	Ключ	Описание
		Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователи могут отображать пароли в сохраненных логинах
Отключить Pocket	DisablePocket	Отключает сохранение страниц в Pocket. Если политика находится в состоянии «Включено», Pocket недоступен. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», Pocket доступен. Примечание. Pocket – это специальный сервис для хранения различной информации, найденной в ходе веб-серфинга
Отключить импорт профиля	DisableProfileImport	Отключает команду меню для импорта данных из другого веб-браузера. Если политика находится в состоянии «Включено», опция «Импортировать данные из другого браузера...» в окне закладок недоступна. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», опция «Импортировать данные из другого браузера...» доступна
Отключить обновление профиля	DisableProfileRefresh	Отключает кнопку «Обновить Firefox» на странице about:support. Если политика находится в состоянии «Включено», кнопка «Обновить Firefox» будет недоступна на странице about:support. Если эта политика отключена или не настроена, кнопка «Обновить Firefox» доступна
Отключить безопасный режим	DisableSafeMode	Отключает функцию для перезапуска в безопасном режиме. Если политика находится в состоянии «Включено», пользователь не может перезапустить веб-браузер в безопасном режиме. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», безопасный режим разрешен
Не проверять веб-браузер по умолчанию	DontCheckDefaultBrowser	Отключает проверку веб-браузера по умолчанию при запуске. Если политика находится в состоянии «Включено», Firefox не проверяет, является ли он веб-браузером по умолчанию при запуске. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», Firefox при запуске проверяет, является ли он веб-браузером по умолчанию
Аппаратное ускорение	HardwareAcceleration	Отключает аппаратное ускорение. Если политика находится в состоянии «Отключено», аппаратное ускорение не может быть включено.

Продолжение таблицы 53

Политика	Ключ	Описание
		Если политика находится в состоянии «Включено» или «Не сконфигурировано», включено аппаратное ускорение
Основной (главный) пароль	PrimaryPassword	Требовать или не давать использовать мастер-пароль. Если политика находится в состоянии «Отключено», пользователи не могут создать основной пароль. Если политика находится в состоянии «Включено» или «Не сконфигурировано», пользователи могут создать основной пароль
Прогнозирование сети	NetworkPrediction	Включает или отключает прогнозирование сети (предварительная выборка DNS). Предварительная выборка DNS – это технология, используемая Firefox для ускорения загрузки новых веб-сайтов. Если политика находится в состоянии «Отключено», прогнозирование сети (предварительная выборка DNS) будет отключено. Если политика находится в состоянии «Включено» или «Не сконфигурировано», будет включено прогнозирование сети (предварительная выборка DNS)
Новая вкладка	NewTabPage	Включает или отключает страницу новой вкладки. Если эта политика находится в состоянии «Отключено», в новой вкладке будет загружена пустая страница. Если эта политика в состоянии «Включено» или «Не сконфигурировано», в новой вкладке будет загружена страница по умолчанию
Подсказки по поиску	SearchSuggestEnabled	Включает или отключает поисковые предложения. Если эта политика находится в состоянии «Отключено», поисковые подсказки будут отключены. Если эта политика в состоянии «Включено», поисковые подсказки будут включены. Если эта политика в состоянии «Не сконфигурировано», поисковые подсказки будут включены, но пользователь может отключить их
Показывать кнопку «Домашняя страница Firefox» на панели инструментов	ShowHomeButton	Включает кнопку «Домашняя страница Firefox» на панели инструментов. Если политика находится в состоянии «Отключено», кнопка «Домашняя страница Firefox» не будет отображаться на панели инструментов. Если политика находится в состоянии «Включено», кнопка «Домашняя страница Firefox» отображается на панели инструментов
Блокировка менеджера дополнений (about:addons)	BlockAboutAddons	Блокирует доступ к менеджеру дополнений (about:addons). Если политика находится в состоянии «Отключено» или «Не сконфигурировано» пользователь может получить доступ к менеджеру дополнений (about:addons).

Продолжение таблицы 53

Политика	Ключ	Описание
		Если политика находится в состоянии «Включено», пользователь не может получить доступ к менеджеру дополнений (about:addons)
URL для домашней страницы	Homepage	Устанавливает URL домашней страницы при старте веб-браузера и, если нужно, блокирует ее смену. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь может установить и изменить домашнюю страницу. Если политика находится в состоянии «Включено», можно установить домашнюю страницу по умолчанию, а также заблокировать возможность изменения домашней страницы
SPNEGO	SPNEGO	Включает аутентификацию через SPNEGO/Kerberos. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», никаким веб-сайтам не разрешается использовать аутентификацию SPNEGO с помощью веб-браузера. Если политика находится в состоянии «Включено», указанным веб-сайтам разрешается использовать аутентификацию SPNEGO в веб-браузере. Записи в списке имеют формат altlinux.org или https://altlinux.org
Разрешить неполное доменное имя (Non FQDN)	Authentication AllowNonFQDN	Разрешить SPNEGO или NTLM для неполных доменных имен (Non FQDN). Если политика находится в состоянии «Отключено» или «Не сконфигурировано», NTLM и SPNEGO не будут включены для неполных доменных имен. Если политика находится в состоянии «Включено» (и флаги отмечены), SPNEGO или NTLM будут включены для неполных доменных имен (Non FQDN)
Отключить историю форм	DisableFormHistory	Отключает запоминание истории поиска и данных форм. Если политика находится в состоянии «Включено», Firefox не запоминает историю форм или поиска. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», Firefox будет помнить историю форм и поиска
Не разрешать изменять настройки аутентификации	Authentication Locked	Блокирует настройки аутентификации от изменений пользователем. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь не может изменить параметры проверки подлинности. Если политика находится в состоянии «Включено» (и флаги отмечены), пользователь может изменить параметры проверки подлинности

Продолжение таблицы 53

Политика	Ключ	Описание
Расширения для установки	Extensions\Install	<p>Задаёт список URL-адресов или собственных путей для устанавливаемых расширений.</p> <p>Если политика находится в состоянии «Отключено» или «Не сконфигурировано», расширения не устанавливаются.</p> <p>Если политика находится в состоянии «Включено», можно указать список URL-адресов или путей расширений, которые будут устанавливаться при запуске Firefox. При каждом изменении этого списка политики будут переустанавливаться.</p> <p>URL политики нужно задавать в формате *.xpi (например, https://addons.mozilla.org/firefox/downloads/file/3450175/adaptor_rutoken_plugin-1.0.5.0.xpi). Также можно указать путь на локальный каталог, в который, политикой копирования файлов (см.п. 10.4.6.5.5), скопировать расширение в формате *.xpi</p>
Управление расширениями	ExtensionSettings	<p>Это правило позволяет управлять всеми аспектами расширений.</p> <p>Политика сопоставляет идентификатор расширения с его конфигурацией. Если указан идентификатор расширения, конфигурация будет применяться только к указанному расширению. Конфигурация по умолчанию может быть установлена для специального идентификатора *, который будет применяться ко всем расширениям, для которых не задана пользовательская конфигурация в этой политике. Чтобы получить идентификатор расширения, можно установить расширение и посмотреть идентификатор на странице <code>about:support</code> в разделе «Расширения». Если политика находится в состоянии «Отключено» или «Не сконфигурировано», расширения не будут управляться.</p> <p>Если политика находится в состоянии «Включено», можно использовать JSON для описания политики управления расширениями</p> <p>Пример JSON:</p> <pre> { "*": { "blocked_install_message": "Custom error message" }, "adblockultimate@adblockultimate.net": { "installation_mode": "force_installed", "install_url": "file:///home/user/file.xpi" }, "rutokenplugin@rutoken.ru": { "installation_mode": "force_installed", "install_url": "https://addons.mozilla.org/.../plugin.xpi" } } </pre>

Продолжение таблицы 53

Политика	Ключ	Описание
		<p>Конфигурация для каждого расширения – это еще один словарь, который может содержать следующие поля:</p> <ul style="list-style-type: none"> - <code>installation_mode</code> – режим установки расширения. Допустимые значения: <ul style="list-style-type: none"> а) <code>allowed</code> – разрешает установку расширения пользователем (поведение по умолчанию). Поле <code>install_url</code> не используется и будет автоматически определено на основе идентификатора; б) <code>blocked</code> – блокирует установку расширения и удаляет его, если оно уже установлено; в) <code>force_installed</code> – расширение устанавливается автоматически и не может быть удалено пользователем. Этот параметр недействителен для конфигурации по умолчанию и требует <code>install_url</code>; г) <code>normal_installed</code> – расширение устанавливается автоматически, но может быть отключено пользователем. Этот параметр недействителен для конфигурации по умолчанию и требует <code>install_url</code>; - <code>install_url</code> – сопоставляется с URL-адресом, указывающим, откуда Firefox может загрузить расширение (при <code>force_installed</code> или <code>normal_installed</code>). При установке из локальной файловой системы следует использовать URL-адрес <code>file:///</code>. При установке с сайта <code>addons.mozilla.org</code> можно использовать URL-адрес в виде <code>https://addons.mozilla.org/firefox/downloads/file/3450175/adaptor_rutoken_plugin-1.0.5.0.xpi</code>; - <code>install_sources</code> – список источников, из которых разрешена установка расширений с использованием шаблонов соответствия URL. Этот параметр не нужен, если разрешена установка только определенных расширений по идентификатору. Данный параметр можно использовать только для конфигурации по умолчанию; - <code>minimum_version_required</code> – отключает расширения (в том числе установленные принудительно) более ранних версий, чем определено этим параметром. Формат строки версии аналогичен формату, который используется в манифесте расширения; - <code>allowed_types</code> – белый список разрешенных типов расширений/приложений, которые можно установить в Firefox. Значение представляет собой список строк (допустимые строки: «<code>extension</code>», «<code>theme</code>», «<code>dictionary</code>», «<code>locale</code>»). Этот параметр можно использовать только для конфигурации по умолчанию;

Окончание таблицы 53

Политика	Ключ	Описание
		<ul style="list-style-type: none"> - <code>override_update_url</code> – указывает, что для всех последующих обновлений расширения будет использоваться URL из поля <code>update_url</code> или <code>update</code> в политике <code>ExtensionInstallForcelist</code>. Если это политика не настроена или отключена, будет использоваться URL из манифеста расширения; - <code>override_update_url</code> – указывает, что для всех последующих обновлений расширения будет использоваться URL из поля <code>update_url</code> или <code>update</code> в политике <code>ExtensionInstallForcelist</code>. Если это политика не настроена или отключена, будет использоваться URL из манифеста расширения; - <code>blocked_install_message</code> – сообщение об ошибке, которое будет отображаться для пользователей, если им заблокирована установка расширения. Этот параметр можно использовать только для конфигурации по умолчанию; - <code>restricted_domains</code> – массив доменов, на которых нельзя запускать сценарии контента. Этот параметр можно использовать только для конфигурации по умолчанию; - <code>updates_disabled</code> – логическое значение, указывающее, следует ли отключать автоматические обновления для отдельного расширения; - <code>default_area</code> – указывает, где должен быть размещен значок расширения. Возможные значения: <code>navbar</code> и <code>menupanel</code>

10.4.6.4.11. Управление политиками браузера «Яндекс.Браузера»

Эти групповые политики позволяют централизованно для компьютеров управлять настройками «Яндекс.Браузера».

Механизм Yandex в составе пакета `gupdate` формирует JSON-файл для веб-браузера из шаблонов групповых политик. Во время запуска веб-браузер «Яндекс.Браузер» считывает файл `/etc/opt/yandex/browser/policies/managed/policies.json` и применяет параметры групповых политик. Групповые политики на основе `policies.json` предоставляют кроссплатформенную совместимость, что позволяет управлять веб-браузерами в любом дистрибутиве «Альт» с установленным окружением рабочего стола.

Примечание. Для случаев, если требуется вести параллельно другой файл с конфигурациями, можно создать файл `/etc/opt/yandex/browser/policies/managed/policies_local.json` и вносить изменения в него. При коллизиях будет применена последняя прочитанная настройка.

Примечание. Данный механизм реализован только для машинных политик.

Примечание. Настройка политик для веб-браузера «Яндекс.Браузера» требует дополнительной установки ADMX-файлов Yandex (пакет `admx-yandex-browser`).

Результат применения параметров групповой политики для «Яндекс.Браузера» можно проверить, указав в адресной строке URL: `browser://policy` (рис. 405).

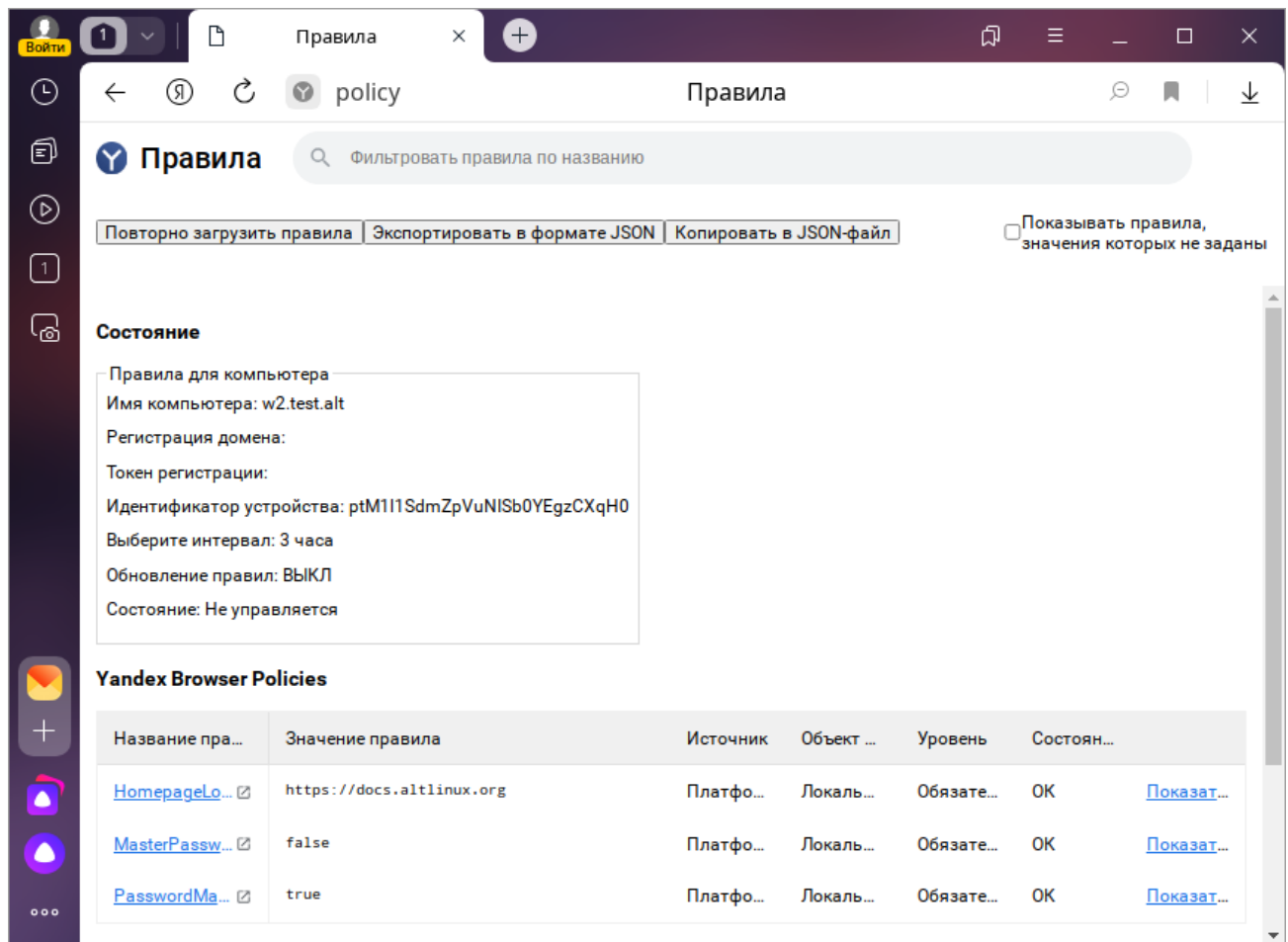


Рис. 405 – Активные политики «Яндекс.Браузера»

В качестве примера ниже рассмотрена политика установки URL домашней страницы.

Для редактирования политик веб-браузера «Яндекс.Браузера» следует перейти в «Компьютер» → «Административные шаблоны» → «Яндекс» → «Яндекс.Браузер». Отобразится список политик (рис. 406).

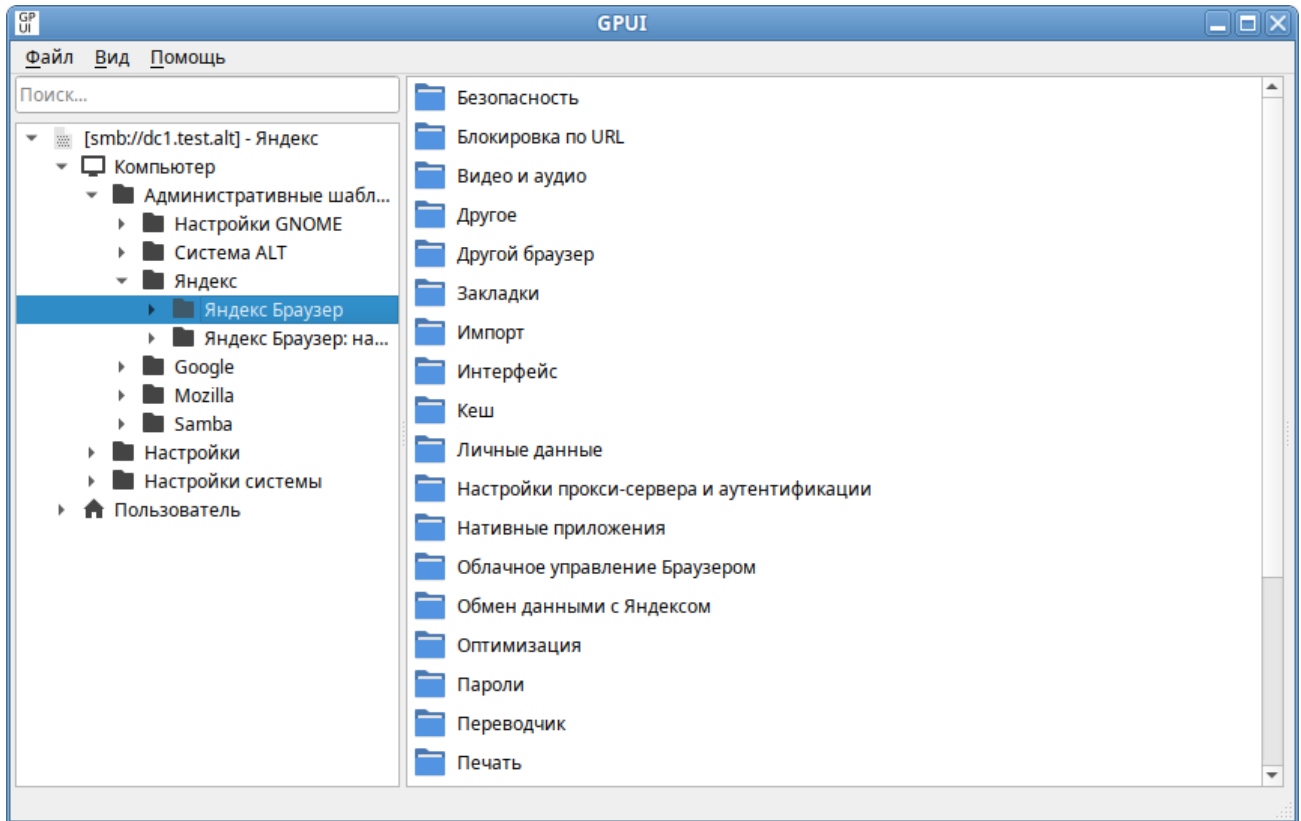


Рис. 406 – Политики настройки «Яндекс.Браузера»

Для установки URL домашней страницы следует выбрать пункт «Поведение», щелкнуть левой кнопкой мыши на политике «Задать URL домашней страницы», откроется диалоговое окно настройки политики. Выбрать параметр «Включено», в разделе «Описание» ввести URL и нажать кнопку «ОК» (рис. 407).

В результате применения данной политики будет установлена домашняя страница по умолчанию, а также будет заблокирована возможность изменения домашней страницы пользователем (рис. 408).

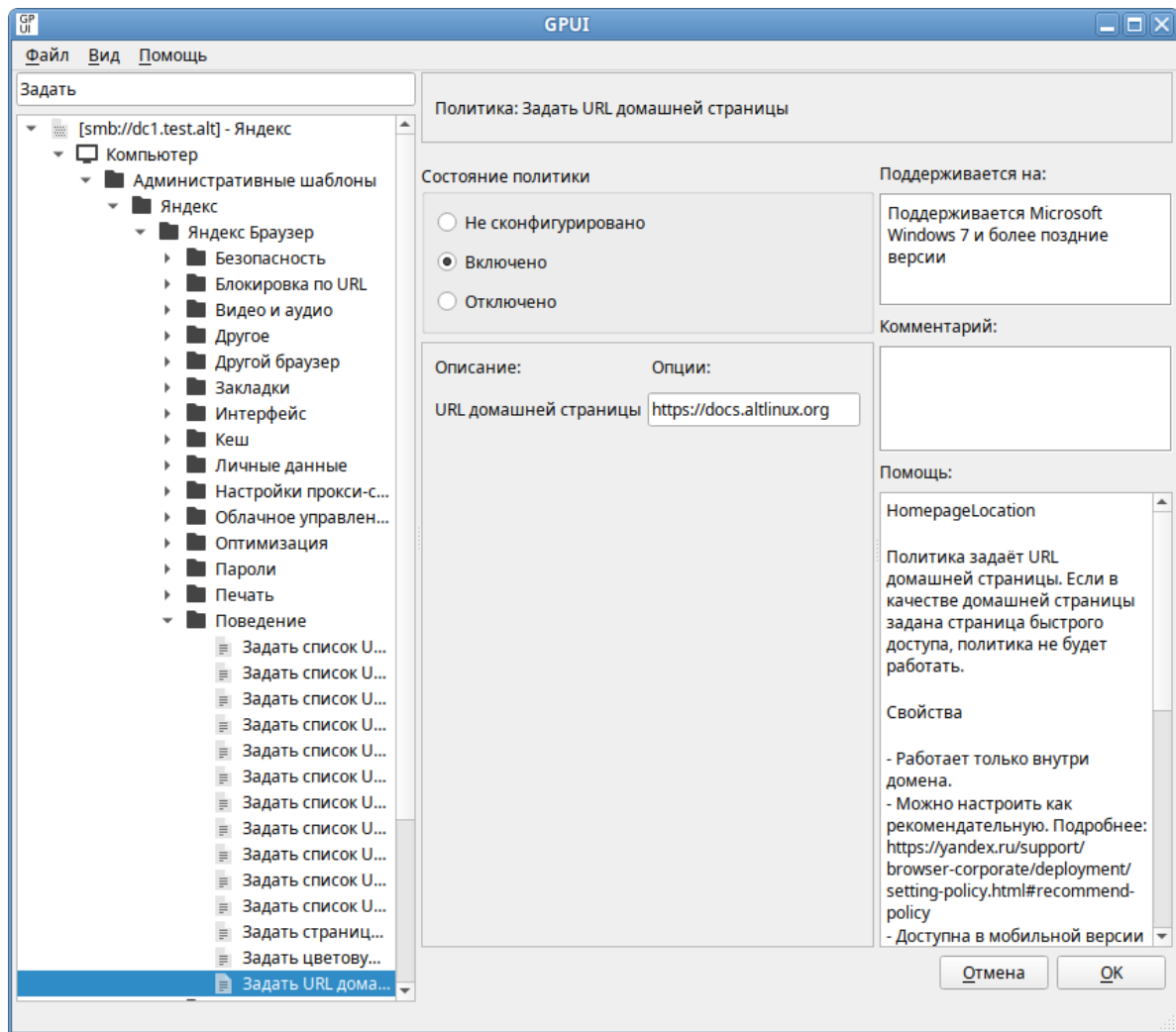


Рис. 407 – Установка URL домашней страницы «Яндекс.Браузера»

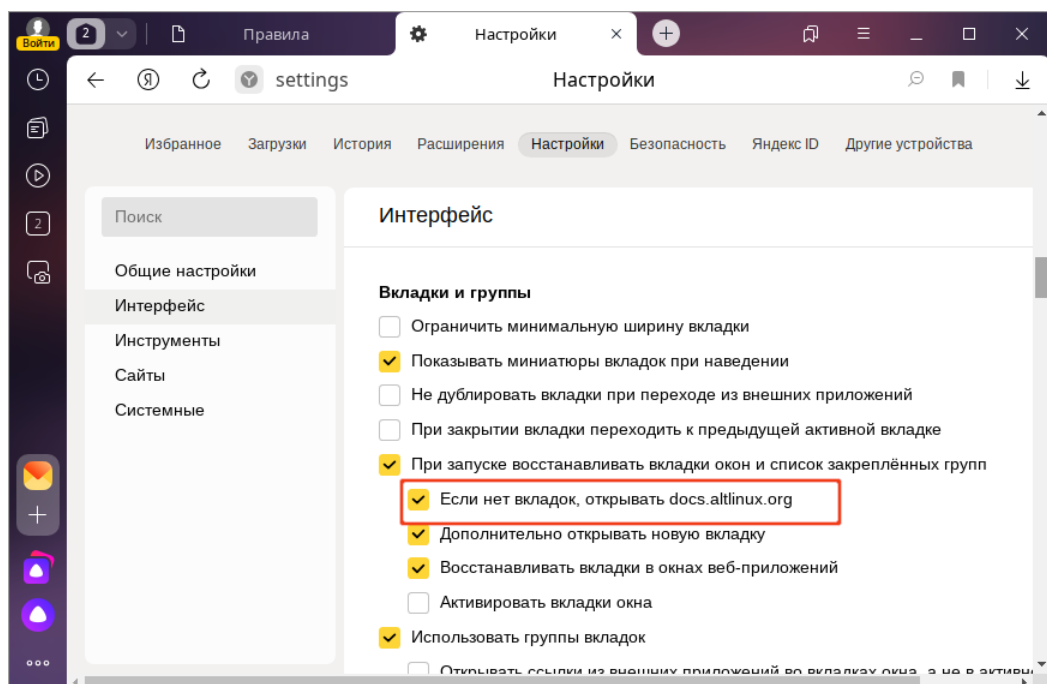


Рис. 408 – Настройки «Яндекс.Браузера»

Все настройки политики «Яндекс.Браузера» хранятся в файле {GUID GPT}/Machine/Registry.pol.

Пример файла Registry.pol:

```
Preg[Software\Policies\YandexBrowser;BlockExternalExtensions;;;]
[Software\Policies\YandexBrowser\URLBlocklist;https://mail.ru;; ;
https://mail.ru]
[Software\Policies\YandexBrowser\AutoOpenFileTypes;pdf;;pdf]
[Software\Policies\YandexBrowser;HomepageLocation;;4;https://docs
.altlinux.org]
```

В таблице 54 описаны только некоторые политики. Полный список политик и их описание можно найти в «Яндекс.Браузере», указав в адресной строке URL: browser://policy/ и установив отметку на пункте «Показывать правила, значения которых не заданы».

Т а б л и ц а 54 – Примеры политик управляющих настройками «Яндекс.Браузера»

Политика	Ключ	Описание
Включить или отключить панель закладок	BookmarkBarEnabled	Политика позволяет принудительно включить или принудительно отключить панель закладок в «Яндекс.Браузере». Если политика находится в состоянии «Включено», панель закладок отображается. Если политика находится в состоянии «Отключено», панель закладок не отображается. Если политика находится в состоянии «Не сконфигурировано», пользователь может самостоятельно решать, включить или отключить панель закладок
Настроить закладки	EditBookmarksEnabled	Политика включает или отключает возможность изменения закладок. Если политика находится в состоянии «Включено» или «Не сконфигурировано», пользователи могут добавлять, изменять и удалять закладки. Если политика находится в состоянии «Отключено», пользователи не могут добавлять, изменять и удалять закладки. Закладки, созданные до отключения политики, останутся доступными
Задать форматы файлов, которые будут автоматически открываться после скачивания	AutoOpenFileTypes	Политика позволяет задать форматы файлов, которые будут автоматически открываться после скачивания. Если политика находится в состоянии «Включено», в ней можно перечислить форматы файлов, которые будут автоматически открываться после скачивания (например, txt, jpg).

Продолжение таблицы 54

Политика	Ключ	Описание
		Если политика находится в состоянии «Отключено» или «Не сконфигурировано», после скачивания будут автоматически открываться файлы только тех форматов, которые выбрал пользователь в контекстном меню загруженного файла (например, «Открывать JPG автоматически»)
Запретить открывать файлы офисных форматов в браузере	CloudDocumentsDisabled	Политика запрещает пользователям открывать файлы офисных форматов в браузере. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь может открывать в браузере файлы офисных форматов. Если политика находится в состоянии «Включено», пользователю запрещено открывать в браузере файлы офисных форматов
Настроить показ всплывающих окон	DefaultPopupsSetting	Политика разрешает или запрещает всплывающие окна на всех сайтах. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», всплывающие окна блокируются на всех сайтах. Пользователи могут разрешать или блокировать всплывающие окна в настройках браузера. Если политика находится в состоянии «Включено», администратор может определить режим применения политики: - «Блокировать на всех сайтах»; - «Разрешить на всех сайтах». Пользователи не могут разрешать или блокировать всплывающие окна в настройках браузера
Разрешить полноэкранный режим	FullscreenAllowed	Политика разрешает или запрещает активацию полноэкранного режима. В этом режиме все элементы интерфейса «Яндекс.Браузера» скрыты, и на экране отображается только содержимое сайта. Если политика находится в состоянии «Включено» или «Не сконфигурировано», пользователи могут активировать полноэкранный режим, нажав клавишу <F11>. Полноэкранный режим может быть активирован приложениями и расширениями, если у них есть на это разрешения. Если политика находится в состоянии «Отключено», полноэкранный режим отключен для всех пользователей, приложений и расширений
Задать URL домашней страницы	HomepageLocation	Политика задает URL домашней страницы. Если в качестве домашней страницы задана страница быстрого доступа, политика не будет работать. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователи могут сами установить URL домашней страницы в настройках браузера.

Продолжение таблицы 54

Политика	Ключ	Описание
		Если политика находится в состоянии «Включено», можно установить домашнюю страницу по умолчанию. URL должен иметь стандартный вид (например, https://altlinux.org). Домашняя страница откроется, если в последний раз браузер был закрыт без вкладок или сочетанием клавиш <Alt> + <Home>. Пользователи не могут менять домашнюю страницу в браузере.
Отключить контекстное меню для выделенного текста	InstaserpDisabled	Политика позволяет отключить контекстное меню, всплывающее при выделении текста на странице. Если политика находится в состоянии «Включено», контекстное меню не показывается, пользователи не могут включить его в настройках (опция «При выделении текста показывать кнопки "Найти" и "Копировать"» неактивна). Если политика находится в состоянии «Отключено», контекстное меню показывается, пользователи не могут отключить его в настройках. Если политика находится в состоянии «Не сконфигурировано», контекстное меню показывается, пользователи могут отключить его в настройках.
Отображать боковую панель	SidePanelMode	Политика позволяет настроить режим отображения боковой панели и запретить пользователям его менять. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователи могут самостоятельно настроить режим отображения боковой панели. Если политика находится в состоянии «Включено», администратор может выбрать режим отображения боковой панели: - «Закрепить только на экране новой вкладки»; - «Закрепить на сайтах»; - «Скрыть»
Включить автозаполнение адресов	AutofillAddressEnabled	Политика разрешает пользователям автозаполнение адресов. Если политика находится в состоянии «Включено» или «Не сконфигурировано», автозаполнение адресов включено. Если политика находится в состоянии «Отключено», автозаполнение адресов отключено, введенные адреса не сохраняются
Настроить режим Инкогнито	IncognitoModeAvailability	Политика определяет, могут ли пользователи включать режим Инкогнито. Если политика находится в состоянии «Не сконфигурировано», пользователи могут открывать страницы в режиме Инкогнито.

Продолжение таблицы 54

Политика	Ключ	Описание
		<p>Если политика находится в состоянии «Включено», администратор может определить режим применения политики:</p> <ul style="list-style-type: none"> - «Принудительное использование режима Инкогнито» – режим Инкогнито всегда включен; - «Режим Инкогнито доступен» – пользователи могут просматривать страницы как в обычном режиме, так и в режиме Инкогнито; - «Режим Инкогнито отключён» – пользователи могут просматривать страницы только в обычном режиме. <p>Если политика находится в состоянии «Отключено», пользователи могут просматривать страницы только в обычном режиме</p>
Запретить использовать мастер-пароль	MasterPasswordDisabled	<p>Политика запрещает пользователям использовать мастер-пароль.</p> <p>Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь может использовать мастер-пароль.</p> <p>Если политика находится в состоянии «Включено», мастер-пароль в браузере отключен</p>
Разрешить сохранять пароли	PasswordManagerEnabled	<p>Политика разрешает сохранять пароли в браузере и автоматически подставлять их при авторизации на сайтах.</p> <p>Если политика находится в состоянии «Не сконфигурировано», сохранение паролей в браузере включено. Пользователи могут включать и отключать сохранение паролей.</p> <p>Если политика находится в состоянии «Включено», сохранение паролей включено. Пользователи не могут включать и отключать сохранение паролей.</p> <p>Если политика находится в состоянии «Отключено», сохранение новых паролей отключено. Пользователи могут использовать уже сохраненные пароли.</p> <p>Пользователи не могут включать и отключать сохранение паролей</p>
Запретить сохранять историю просмотров	SavingBrowserHistoryDisabled	<p>Политика запрещает сохранять историю просмотров и синхронизировать открытые вкладки. При синхронизации информация передается на сервер Яндекса по защищенному каналу.</p> <p>Если политика находится в состоянии «Отключено» или «Не сконфигурировано», история посещенных страниц сохраняется в журнале браузера. Вкладки и Табло синхронизируются с сервером Яндекса.</p> <p>Если политика находится в состоянии «Включено», история посещенных страниц не сохраняется в журнале браузера. Пользователи не могут включить сохранение истории посещенных страниц. Только</p>

Продолжение таблицы 54

Политика	Ключ	Описание
		Табло синхронизируются с сервером Яндекса. Возможность переноса истории вручную отключена
Выбрать папку кеша на диске	DiskCacheDir	Политика определяет место хранения данных кеша. Чтобы не потерять данные, не следует указывать в политике корневую папку или папку, которая используется в других целях. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», браузер использует папку по умолчанию, однако пользователи могут ее изменить с помощью параметра disk-cache-dir. Если политика находится в состоянии «Включено», браузер хранит кеш на диске в заданной администратором папке. Пользователи не могут ее изменить с помощью параметра disk-cache-dir
Задать объем кеша в байтах	DiskCacheSize	Политика позволяет задать объем кеша в байтах. Значение используется различными подсистемами в браузере как справочное. Поэтому фактический объем используемого дискового пространства может превышать указанное значение, но будет иметь такой же порядок. Если политика находится в состоянии «Не сконфигурировано», браузер использует объем кеша по умолчанию. Если политика находится в состоянии «Включено», браузер использует заданный размер кеша независимо от параметра --disk-cache-size. Указывается максимальный размер кеша в байтах. Например, 104857600 – это 100 МБ. Если политика находится в состоянии «Отключено», браузер использует объем кеша по умолчанию, но пользователи могут менять размер кеша с помощью параметра --disk-cache-size
Блокировать внешние расширения	BlockExternalExtensions	Политика позволяет запретить установку внешних расширений. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», установка внешних расширений разрешена. Если политика находится в состоянии «Включено», установка внешних расширений запрещена
Блокировать URL'ы из заданного списка	URLBlocklist	Политика блокирует доступ к URL и локальным файлам, которые внесены в черный список. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», браузер не блокирует URL. Если политика находится в состоянии «Включено», страницы запрещенных URL не загружаются. В политике можно перечислить шаблоны запрещенных URL.

Продолжение таблицы 54

Политика	Ключ	Описание
		<p>Политика не действует на URL со встроенным кодом JavaScript и динамически загружаемые данные.</p> <p>Общий формат шаблона URL: <code>scheme://host:port/path</code>, где:</p> <ul style="list-style-type: none"> - <code>scheme</code> – схема обращения к ресурсу (например, <code>http</code>, <code>https</code>). Если префикс <code>scheme://</code> не задан, блокируются все пути и все протоколы (<code>http</code>, <code>https</code>, <code>ftp</code> и т.д.). Блокировать внутренние URL с префиксом <code>browser://</code> и <code>chrome://</code> не рекомендуется; - <code>host</code> – полное доменное имя или IP-адрес хоста. Имя или IP-адрес хоста должны быть указаны обязательно. По умолчанию блокируются все субдомены хоста. Чтобы этого избежать, можно добавить точку (.) перед именем хоста. Звездочка (*) блокирует все домены; - <code>port</code> – номер порта. Можно указать номер от 1 до 65535. Если номер не указан, блокируются все порты; - <code>path</code> – URL-адрес. <p>Общий формат шаблона локального файла <code>file://path</code>, где:</p> <ul style="list-style-type: none"> - <code>file</code> – путь до конкретного файла <code>.html</code>; <code>path</code> – абсолютный путь к каталогу с файлами (все пути, для которых <code>path</code> является префиксом, будут внесены в список)
Задать исключения для политики URLBlocklist	URLAllowlist	<p>Политика позволяет внести в белый список URL или локальный файл. Белый список разрешает доступ к явно перечисленным в нем URL и файлам, даже если они попадают под действие шаблонов из черного списка (см. описание политики «Блокировать URL’ы из заданного списка»).</p> <p>Если политика находится в состоянии «Отключено» или «Не сконфигурировано», исключений из правила URLBlocklist нет.</p> <p>Если политика находится в состоянии «Включено», указанные URL становятся доступны пользователям и считаются исключениями из правила URLBlocklist.</p> <p>Политика позволяет настроить исключения для определенных протоколов, субдоменов, отдельных доменов, портов или путей. Политика URLAllowlist имеет приоритет над правилом URLBlocklist. В этом правиле можно указать не более 1000 URL.</p> <p>Форматы шаблонов см. в описании политики «Блокировать URL’ы из заданного списка»</p>
Разрешить вызывать окно выбора файлов	AllowFileSelectionDialogs	<p>Политика разрешает или запрещает отображать окно выбора файлов и управляет настройками загрузки.</p> <p>Если политика находится в состоянии «Включено» или «Не сконфигурировано», пользователи могут открывать окна выбора файлов (импорт закладок или паролей, загрузка файлов, сохранение ссылок и т. д.).</p>

Продолжение таблицы 54

Политика	Ключ	Описание
		<p>Также пользователи могут сохранить файл с помощью контекстного меню и изменять настройки в разделе «Загруженные файлы» («Настройки» → «Инструменты» → «Загруженные файлы»).</p> <p>Если политика находится в состоянии «Отключено» и пользователь выполняет действия, для которых нужно открыть окно выбора файла (например, импорт закладок, загрузка файлов, сохранение ссылок и т. д.), вместо окна отображается сообщение и имитируется нажатие пользователем кнопки «Отмена» в окне выбора файлов</p>
Ограничить инструменты разработчика	DeveloperToolsAvailability	<p>Политика ограничивает использование инструментов разработчика. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», инструменты разработчика и консоль JavaScript запрещены только для расширений, ограниченных корпоративной политикой. Если политика находится в состоянии «Включено» можно установить ограничение на использование инструментов разработчика. Доступны следующие параметры:</p> <ul style="list-style-type: none"> - «Запретить»; - «Запретить для расширений, установленных в соответствии с корпоративной политикой, и разрешить во всех остальных случаях»; - «Разрешить»
Управлять настройками расширений	ExtensionSettings	<p>Политика управляет настройками расширений в «Яндекс.Браузере». Заменяет любые другие политики по настройке расширений.</p> <p>Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователи могут самостоятельно настраивать расширения.</p> <p>Если политика находится в состоянии «Включено», настройки расширений задает администратор с помощью кода, указанного в параметрах политики:</p> <ul style="list-style-type: none"> - идентификатор расширения или URL обновления привязывается только к одной конкретной настройке; - идентификатор «*» действует на все расширения, для которых в политике не задана отдельная конфигурация; - если указан URL обновления, заданная конфигурация применяется ко всем расширениям, в манифесте которых приведен этот URL. <p>Пример значения:</p> <pre>{ "hdokiejnpimakedhajhdlcegeplioahd": { "installation_mode": "force_installed", "update_url": "https://clients2.google.com/service/update2/crx" }, }</pre>

Продолжение таблицы 54

Политика	Ключ	Описание
		<pre data-bbox="746 318 1513 542"> "pioclpoplcdbaefihamjohnefbikjilc": { "installation_mode": "force_installed", "update_url": "https://clients2.google.com/service/update 2/crx" } } </pre> <p data-bbox="651 551 954 584">Параметры политики:</p> <ul data-bbox="651 593 1530 2080" style="list-style-type: none"> <li data-bbox="651 593 1530 808">- <code>allowed_types</code> – типы приложений и расширений, которые пользователям разрешено устанавливать в браузере (допустимые строки: «<code>extension</code>», «<code>hosted_app</code>», «<code>legacy_packaged_app</code>», «<code>platform_app</code>», «<code>theme</code>», «<code>user_script</code>»). Используется только для настройки конфигурации по умолчанию со значением *; <li data-bbox="651 817 1530 965">- <code>blocked_install_message</code> – уведомление (не более 1000 символов), которое будет появляться на устройствах пользователей при попытке установить запрещенные расширения; <li data-bbox="651 974 1530 1115">- <code>blocked_permissions</code> – запрещает пользователям устанавливать и запускать расширения, требующие разрешений API (список доступных разрешений указан в манифесте расширения); <li data-bbox="651 1124 1530 1742">- <code>installation_mode</code> – указывает, разрешено ли добавлять заданные расширения. Допустимые режимы: <ul data-bbox="699 1191 1530 1742" style="list-style-type: none"> <li data-bbox="699 1191 1530 1265">а) <code>allowed</code> – пользователи могут установить это расширение (поведение по умолчанию); <li data-bbox="699 1274 1530 1348">б) <code>blocked</code> – пользователи не могут установить это расширение; <li data-bbox="699 1357 1530 1453">в) <code>removed</code> – пользователи не могут установить это расширение. Если расширение было установлено, оно будет удалено; <li data-bbox="699 1462 1530 1603">г) <code>force_installed</code> – расширение устанавливается автоматически. Пользователи не могут его удалить. В этом режиме необходимо указать ссылку для скачивания расширения (параметр <code>update_url</code>); <li data-bbox="699 1612 1530 1742">д) <code>normal_installed</code> – расширение устанавливается автоматически. Пользователи могут его удалить. В этом режиме необходимо указать ссылку для скачивания расширения (параметр <code>update_url</code>); <li data-bbox="651 1751 1530 1892">- <code>install_sources</code> – список URL страниц, с которых разрешено загружать и устанавливать расширения. Необходимо разрешить URL расположения CRX-файла и страницы, с которой начинается скачивание (то есть URL перехода); <li data-bbox="651 1901 1530 2080">- <code>minimum_version_required</code> – отключает расширения (в том числе установленные принудительно) более ранних версий, чем определено этим параметром. Формат строки версии аналогичен формату, который используется в манифесте расширения;

Окончание таблицы 54

Политика	Ключ	Описание
		<ul style="list-style-type: none"> - update_url – определяет, откуда загружается расширение. Можно указать URL интернет-магазина Chrome, Opera или использовать XML-файл; - override_update_url – указывает, что для всех последующих обновлений расширения будет использоваться URL из поля update_url или update в политике ExtensionInstallForcelist. Если эта политика не сконфигурирована или отключена, будет использоваться URL из манифеста расширения; - verified_contents_url – указывает путь до файла extension.verified_contents. С его помощью расширение проверяется на доверие (используется, если нет доступа в интернет); - runtime_allowed_hosts – разрешает взаимодействие расширений с указанными сайтами, даже если они указаны в поле runtime_blocked_hosts. Можно указать до 100 сайтов; runtime_blocked_hosts – запрещает расширениям взаимодействовать с указанными сайтами или изменять их, в том числе вставлять скрипты, получать доступ к файлам cookie и изменять веб-запросы. Можно указать до 100 сайтов

10.4.6.4.12. Политика замыкания

Описание политики замыкания см. в п. 10.4.8.4.

Для настройки этой политики следует перейти в «Компьютер/Пользователь» → «Административные шаблоны» → «Система» → «Групповая политика» (рис. 409).

Щелкнуть левой кнопкой мыши на политике «Настройка режима обработки замыкания пользовательской групповой политики», откроется диалоговое окно настройки политики. Можно не задавать настройку политики, включить или отключить (рис. 410).

Примечание. Для быстрого доступа к политике можно ввести в поле «Поиск...» ключевое слово.

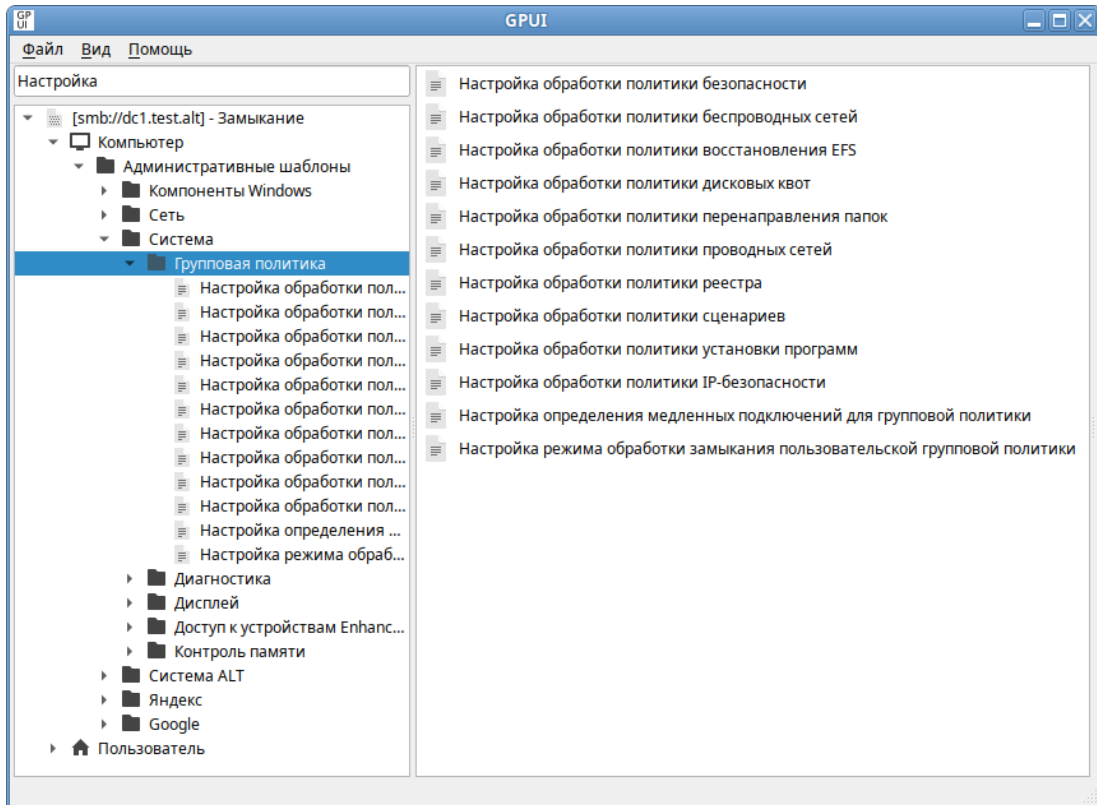


Рис. 409 – Политики ОС

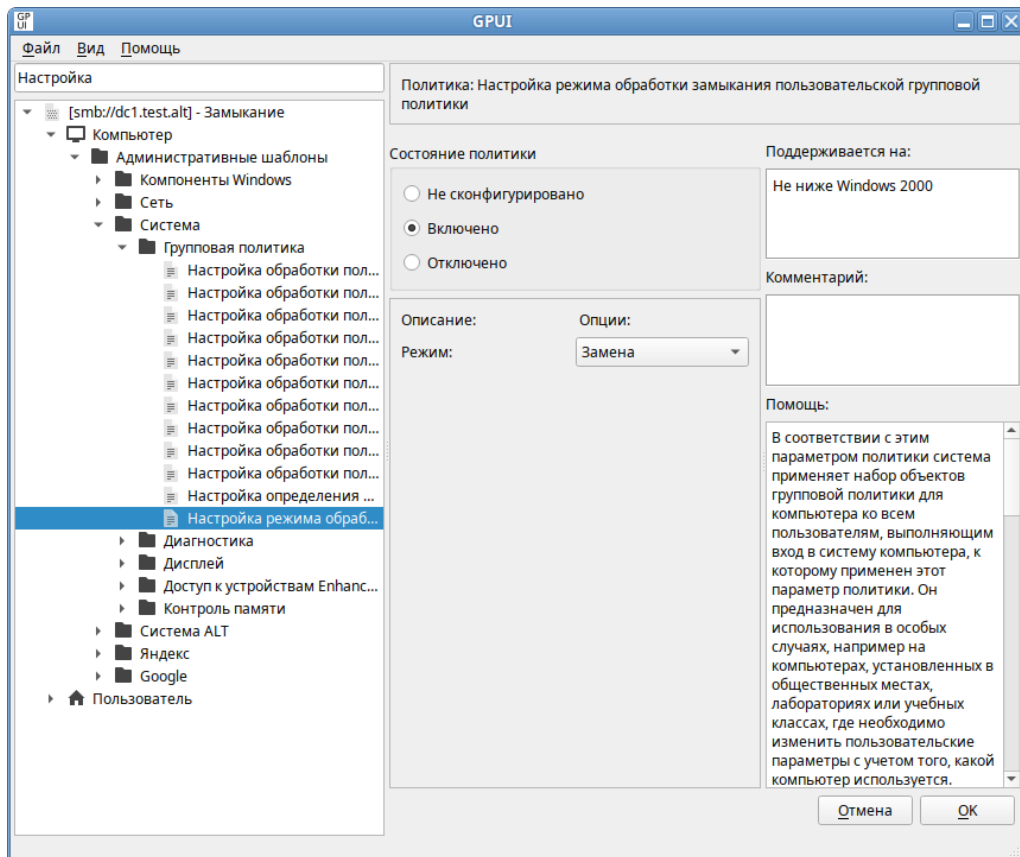


Рис. 410 – Политика «Настройка режима обработки замыкания пользовательской групповой политики»

Если выбрать параметр «Включено», в разделе «Опции» в выпадающем списке можно выбрать режим:

- «Слияние» – указывает, что параметры политики пользователя, определенные в объектах групповой политики компьютера, и обычно применяемые параметры пользователя для этого пользователя должны быть объединены. Если возникает конфликт этих параметров политики, то параметры пользователя в объектах групповой политики компьютера имеют приоритет над обычными параметрами пользователя;
- «Замена» – указывает, что параметры политики пользователя, определенные в объектах групповой политики компьютера, заменяют параметры политики пользователя, обычно применяемые для этого пользователя.

Если выбрать параметр «Отключено» или не настраивать этот параметр политики, порядок применения параметров определяется объектами групповой политики для пользователей.

10.4.6.5. Редактирование предпочтений

Если предпочтение настраивается в секции «Компьютер», групповая политика должна быть привязана к OU с компьютерами. Соответственно, если настраиваемый параметр относится к конфигурации пользователя, нужно назначить политику на OU с пользователями. Также следует убедиться, что объект, к которому должна применяться политика находится в нужном OU с компьютерами или пользователями.

10.4.6.5.1. Управление ярлыками

Групповая политика «Управление ярлыками» позволяет централизованно для компьютеров или пользователей:

- создавать ярлыки;
- удалять ярлыки;
- изменять свойства ярлыков.

Для настройки этой политики следует перейти в «Компьютер/Пользователь» → «Настройки» → «Настройки системы» → «Значки». В контекстном меню свободной области выбрать пункт «Новый» → «Значок» (рис. 411).

В открывшемся диалоговом окне «Диалог настроек» задать настройки политики (рис. 412).

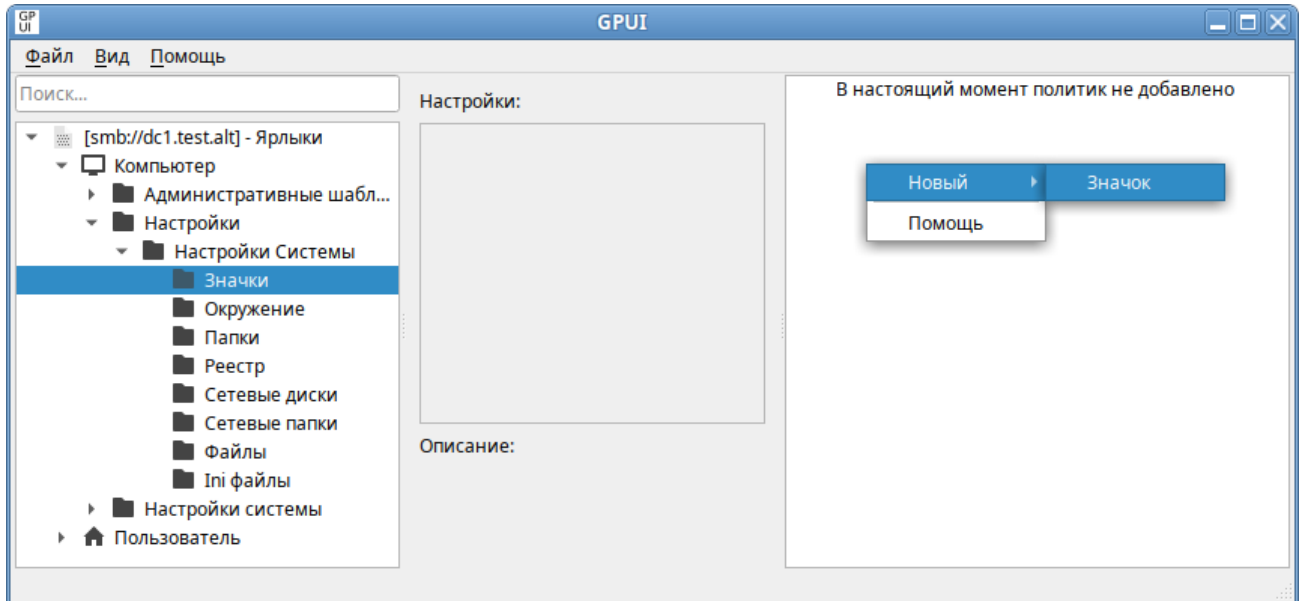


Рис. 411 – Создание новой политики «Значки»

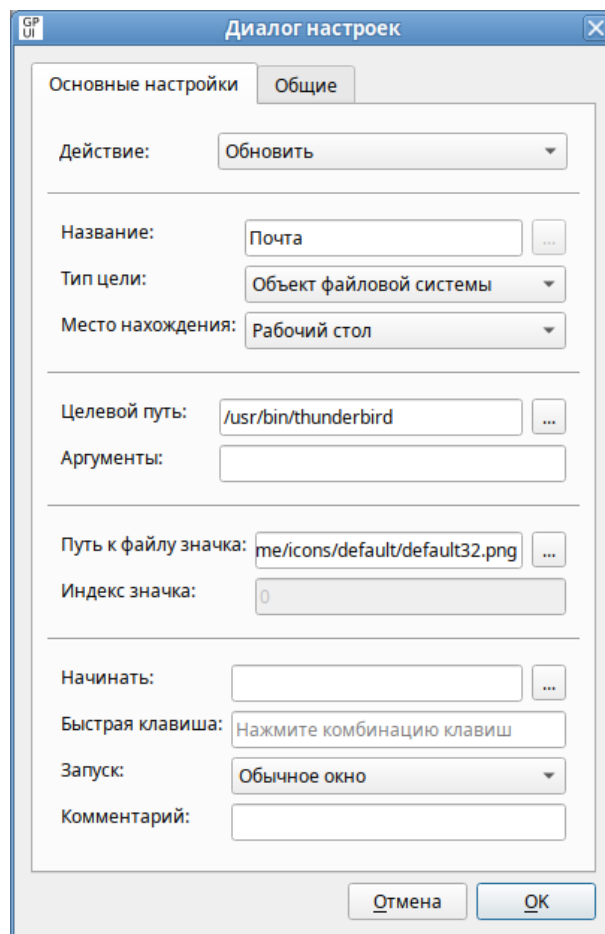


Рис. 412 – Диалоговое окно настройки политики «Значки»

Опции доступные на вкладке «Основные настройки»:

- 1) «Действие» – действие, которое будет выполняться для ярлыка:
 - «Создать» – создание нового ярлыка;
 - «Удалить» – удаление ярлыка;
 - «Заменить» – удаление и повторное создание ярлыка. Если ярлык не существует, то это действие создает новый ярлык;
 - «Обновить» – изменение параметров существующего ярлыка. Если ярлык не существует, то это действие создает ярлык. Это действие отличается от «Заменить» тем, что не удаляет ярлык, а только обновляет параметры ярлыка, определенные в элементе настройки;
- 2) «Название» – отображаемое имя для ярлыка. При изменении или удалении ярлыка имя должно совпадать с именем существующего ярлыка;
- 3) «Тип цели» – тип конечного объекта, на который указывает ярлык (при изменении или удалении ярлыка выбранный тип объекта должен соответствовать существующему ярлыку):
 - «Объект файловой системы» – путь в ФС, например, файл, папка, диск, общий ресурс или компьютер;
 - «URL-адрес» – URL-адрес, например, веб-сайт;
 - «Объект оболочки» – объект, например, принтер, элемент рабочего стола или панели управления, файл, папка, общий ресурс, компьютер или сетевой ресурс;
- 4) «Место нахождения» – место, где ярлык должен отображаться на компьютерах, для которых применяется политика. Размещения, отличные от «Общее...», относятся к текущему пользователю. При изменении существующего ярлыка выбранное размещение должно совпадать с размещением существующего ярлыка. Если выбран пункт «Укажите полный путь», то место задается полным путем в поле «Название» (при этом можно использовать переменные, например, чтобы разместить ярлык с именем «Почта» в подпапке «Ярлыки» в «Program File», нужно ввести %ProgramFilesDir%\Ярлыки\Почта). Чтобы разместить ярлык в

подпапке для выбранного размещения из списка, следует указать <название подпапки>\<имя ярлыка> в поле «Название», например, чтобы разместить ярлык с именем «Почта» в подпапке «Ярлыки» в размещении «Рабочий стол», нужно ввести Ярлыки/Почта в поле «Название» и выбрать «Рабочий стол» в поле «Место нахождения» (рис. 413);

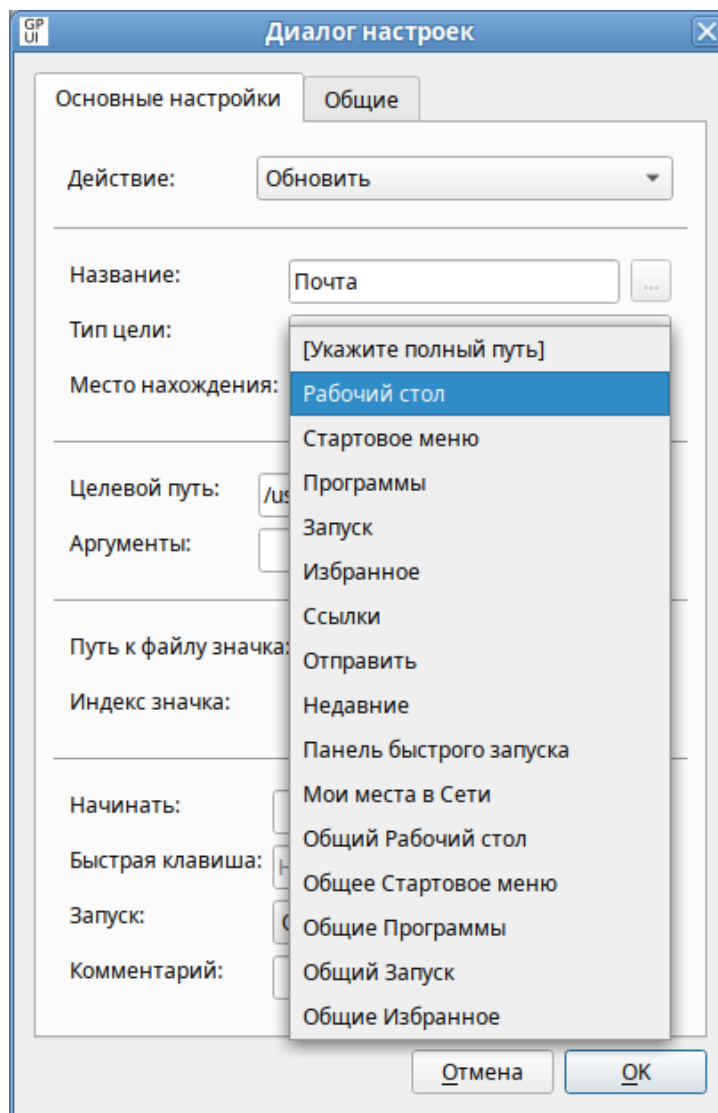



Рис. 413 – Диалог настроек

- 5) «Целевой путь» – локальный путь (с точки зрения клиента) для типа «Объект файловой системы», URL для типа «URL-адрес» или объект для типа «Объект оболочки». Если выбран тип цели «Объект файловой системы» или «URL-адрес», то это поле может принимать переменные. Это поле недоступно, если выбрано действие «Удалить»;

- 6) «Аргументы» – аргументы, которые будут использоваться при открытии целевого файла или папки. Это поле доступно только в том случае, если выбран тип цели «Объект файловой системы» и выбрано действие «Создать», «Заменить» или «Обновить»;
- 7) «Путь к файлу значка» и «Индекс значка» – значок для ярлыка. Для указания значка, отличного от значка по умолчанию нужно выбрать значок или ввести полный путь к значку (с точки зрения клиента) и указать индекс значка. Поле «Путь к файлу значка» принимает переменные. Эти поля недоступны, если выбрано действие «Удалить»;
- 8) «Начинать» – рабочий каталог, содержащий файлы, которые требуются для конечного объекта. Это поле принимает переменные. Поле доступно в случае, если выбрано действие «Создать», «Заменить» или «Обновить»;
- 9) «Быстрая клавиша» – сочетание клавиш для запуска ярлыка. Чтобы назначить сочетание клавиш следует установить курсор в поле «Быстрая клавиша» и нажать комбинацию клавиш. Чтобы удалить сочетание клавиш, можно нажать клавишу <CTRL> или <ALT>, или нажать на значок, расположенный справа от сочетания клавиш. Это поле недоступно, если выбрано действие «Удалить»;
- 10) «Запуск» – размер окна, в котором нужно открыть цель ярлыка. Поле доступно только в том случае, если выбран тип объекта «Объект файловой системы» или «Объект оболочки», и выбрано действие «Создать», «Заменить» или «Обновить»;
- 11) «Комментарий» – всплывающая подсказка, когда указатель мыши приостановлен на ярлыке. Поле принимает переменные. Поле доступно только в том случае, если выбран тип объекта «Объект файловой системы» или «Объект оболочки», и выбрано действие «Создать», «Заменить» или «Обновить».

 Чтобы ярлыку назначались корректные права (для пользовательской политики), нужно установить отметку в пункте «Выполнять в контексте безопасности текущего пользователя» на вкладке «Общие».

Все настройки политики для ярлыков хранятся в файлах:

```
{GUID GPT}/Machine/Preferences/Shortcuts/Shortcuts.xml
{GUID GPT}/User/Preferences/Shortcuts/Shortcuts.xml
```

Пример файла Shortcuts.xml:

```
<?xml version="1.0" encoding="utf-8"?>
<Shortcuts clsid="{872ECB34-B2EC-401b-A585-D32574AA90EE}">
<Shortcut bypassErrors="0"
changed="2022-11-17 11:07:40"
clsid="{4F2F7C55-2790-433e-8127-0739D1CFA327}"
desc=""
image="0"
name="Почта"
removePolicy="0"
status=""
uid="{dfd45a36-4634-47d9-8a22-5f702fba21bc}"
userContext="0">
<Properties
action="U"
arguments=""
comment=""
iconPath="/usr/lib64/thunderbird/chrome/icons/default/default32.png"
"
pidl=""
shortcutPath="%DesktopDir%\Почта"
startIn=""
targetPath="/usr/bin/thunderbird"
targetType="FILESYSTEM"
window=""/>
</Shortcut>
</Shortcuts>
```

10.4.6.5.2. Управление каталогами

Групповая политика «Управление каталогами» позволяет для всех пользователей заданной группы создавать унифицированную структуру каталогов.

Для настройки этой политики следует перейти в «Компьютер»/«Пользователь» → «Настройки» → «Настройки системы» → «Папки». В контекстном меню свободной области выбрать пункт «Новый» → «Папки»

(рис. 414).

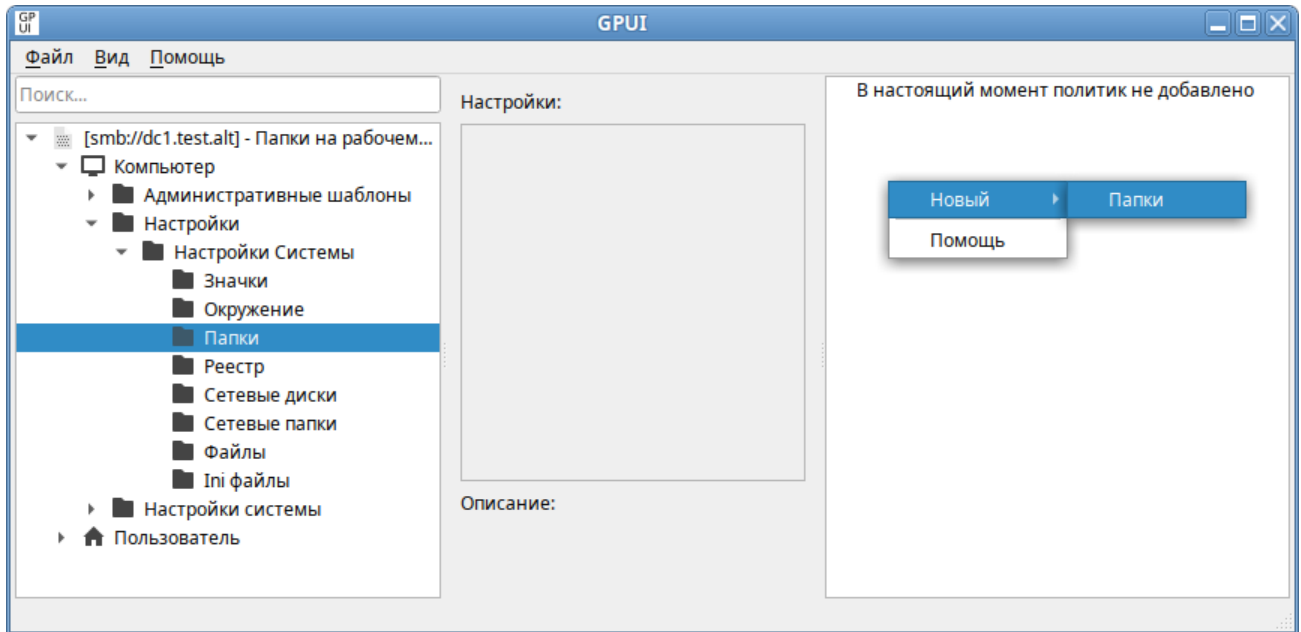


Рис. 414 – Создание новой политики «Папки»

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 415).

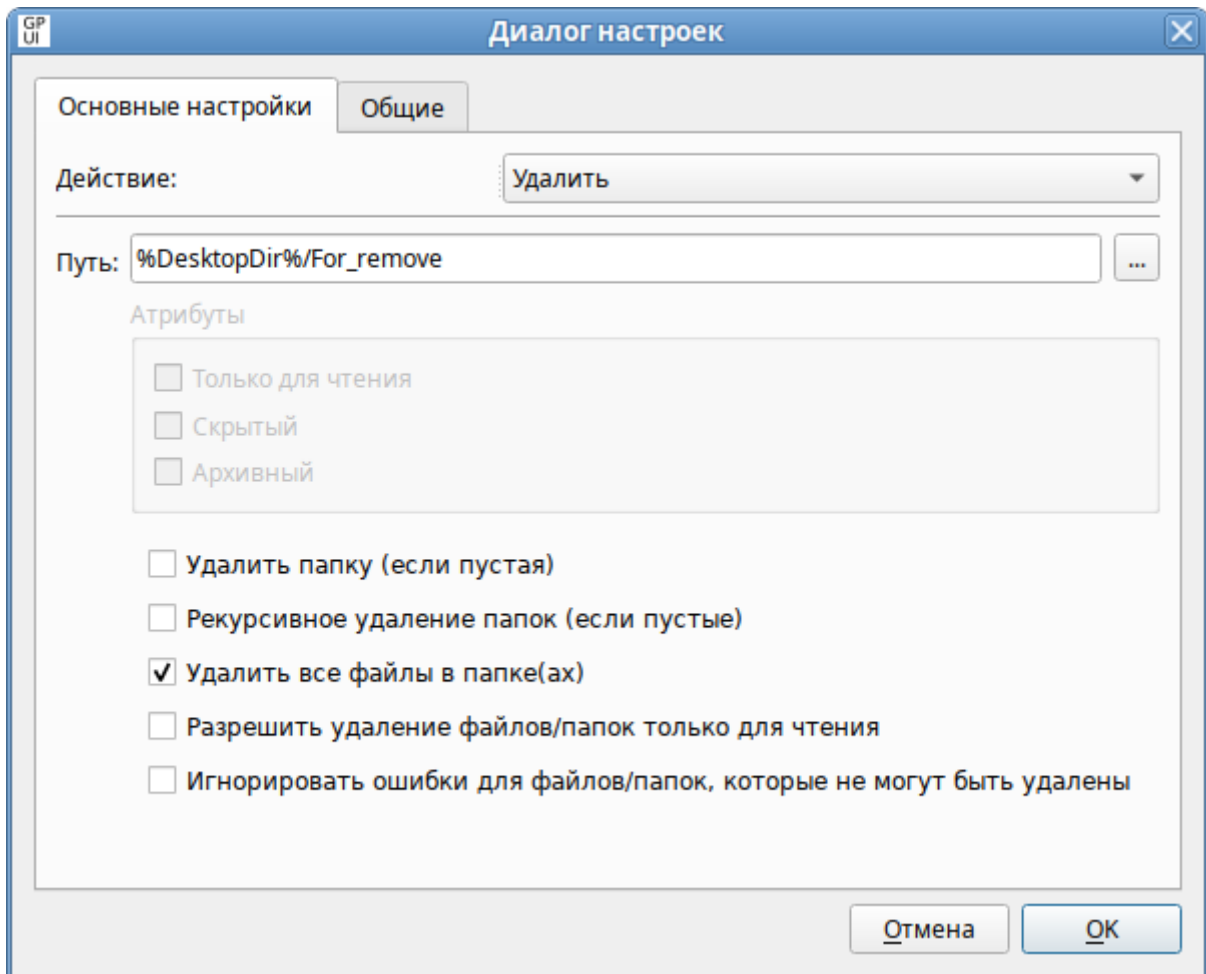


Рис. 415 – Диалоговое окно настройки политики «Папки»

Опции доступные на вкладке «Основные настройки»:

1) «Действие» – действие, которое будет выполняться для папки:

- «Создать» – создание новой папки;
- «Удалить» – удаление папки;
- «Заменить» – удаление и повторное создание папки. В результате выполнения действия «Заменить» содержимое существующей папки удаляется, и все существующие параметры папки перезаписываются. Если папка не существует, действие «Заменить» создает новую папку;
- «Обновить» – изменение параметров существующей папки. Если папки не существует, то это действие создает новую папку. Это действие отличается от «Заменить» тем, что не удаляет папку, а только обновляет параметры;

2) «Путь» – путь к папке (с точки зрения клиента). Это поле может содержать переменные (не следует вводить кавычки и завершающую косую черту);

3) «Атрибуты» – атрибуты файловой системы для папки (недоступны для действия «Удалить»):

- «Только для чтения»;
- «Скрытый»;
- «Архивный»;

4) следующие опции доступны только для действий «Заменить» и «Удалить»:

- «Удалить папку (если пустая)» – если включена эта опция папка, указанная в поле «Путь», удаляется, если она пуста. Будет ли эта папка пустой, оценивается после того, как были обработаны опции «Удалить все файлы в папке(ах)» и «Рекурсивное удаление папок (если пустые)». При выборе действия «Удалить» эта опция включена по умолчанию и ее невозможно отключить;
- «Рекурсивное удаление папок (если пустые)» – если включена эта опция, самый низкий уровень вложенных папок удаляется, если они пусты, повторяется для каждой родительской папки до достижения папки,

- указанной в поле «Путь». Пустые подпапки оцениваются после того, как опция «Удалить все файлы в папке(ах)» была обработана;
- «Удалить все файлы в папке(ах)» – если включена эта опция, удаляются все файлы в папке, которые разрешено удалять. Если также включена опция «Рекурсивное удаление папок (если пустые)», то удаляются также все файлы, которые разрешено удалять во всех подпапках;
 - «Разрешить удаление файлов/папок только для чтения» – если включена эта опция, атрибут «Только для чтения» отключается для удаляемых файлов и папок;
 - «Игнорировать ошибки для файлов/папок, которые не могут быть удалены» – если включена эта опция, подавляются любые сообщения об ошибках, возникающие из-за невозможности удаления файлов или папок. Если эта опция не включена, возвращается ошибка, если совершается попытка удалить непустую папку, открытый файл, файл или папку, для которых пользователь не имеет разрешений или любой другой файл или папку, которые не могут быть удалены.

Примечание. Атрибуты «Архивный», «Скрытый» и «Только для чтения» применимы только для Windows систем.

Все настройки политики для управления каталогами хранятся в файлах:

```
{GUID GPT}/Machine/Preferences/Folders/Folders.xml
{GUID GPT}/User/Preferences/Folders/Folders.xml
```

Пример файла Folders.xml:

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<Folders clsid="{77CC39E7-3D16-4f8f-AF86-EC0BBEE2C861}">
  <Folder clsid="{07DA02F5-F9CD-4397-A550-4AE21B6B4BD3}"
    name="MyDir"
    status="MyDir"
    image="2"
    bypassErrors="1"
    changed="2020-10-27 11:49:19"
    uid="{57F41C87-4A65-4561-BFFF-4219149DCBF7}">
  <Properties
    action="U"
    path="%DesktopDir%\MyDir"
```

```

        readOnly="0"
        archive="1"
        hidden="0"/>
    </Folder>
</Folders>

```

10.4.6.5.3. Управление INI-файлами

Групповая политика «Управление ini-файлами» позволяет:

- добавить свойство в файл параметров конфигурации (.ini);
- заменить свойство в INI-файле;
- удалить свойство из INI-файла;
- удалить раздел из INI-файла;
- удалить INI-файл.

В разделах INI-файлов используется следующий формат:

```

[sectionA]
var01=value01

[sectionB]
var01=value01
var02=value02

```

Для настройки этой политики следует перейти в «Компьютер»/«Пользователь» → «Настройки» → «Настройки системы» → «Ini файлы». В контекстном меню свободной области выбрать пункт «Новый» → «Ini файл» (рис. 416).

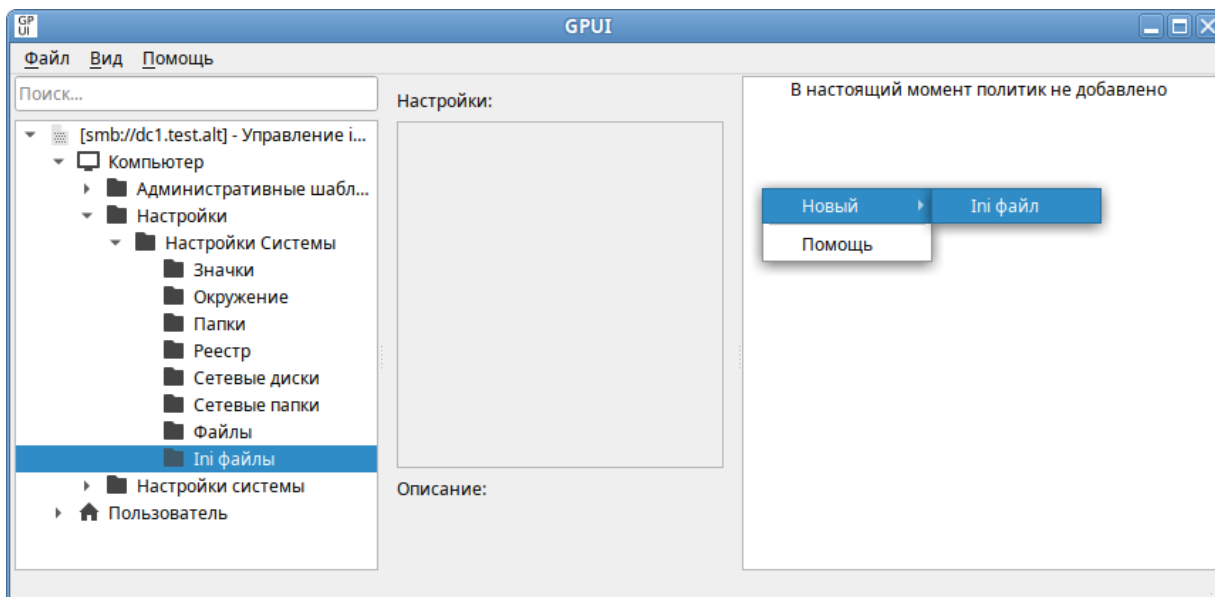


Рис. 416 – Создание новой политики «INI файл»

В открывшемся диалоговом окне «Диалог настроек» задать настройки политики (рис. 417).

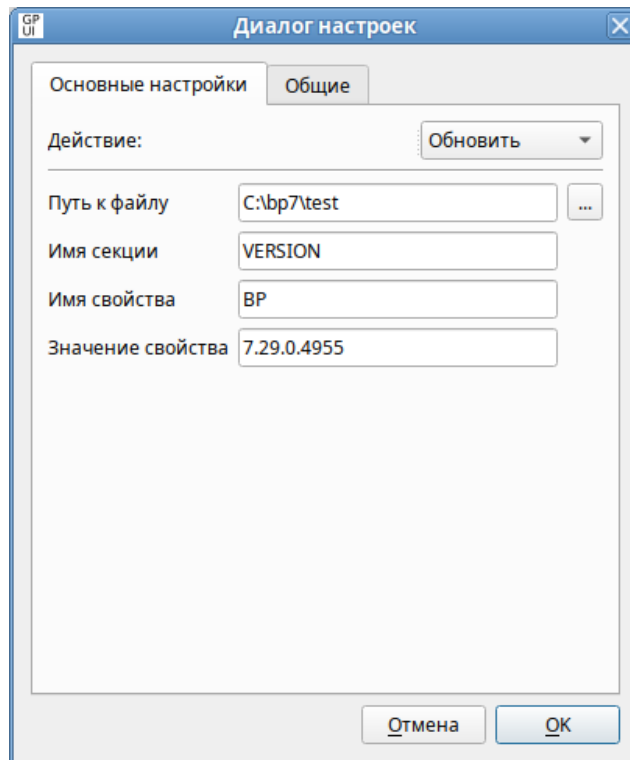


Рис. 417 – Настройки политики «INI файл»

Опции доступные на вкладке «Основные настройки»:

1) «Действие» – действие, которое будет выполняться для INI-файла:

- «Создать» – добавление свойства в INI-файл. Если файл не существует, он будет создан;
- «Удалить» – удаление свойства или раздела из INI-файла (либо удаление INI-файла);
- «Заменить» – удаление и повторное создание свойства в INI-файле (суммарный итог действия «Заменить» – переопределение свойства. Если свойство не существует, действие «Заменить» создаст его);
- «Обновить» – удаление и повторное создание свойства в INI-файле (аналогично действию «Заменить»);

2) «Путь к файлу» – путь к INI-файлу с точки зрения клиента (путь не должен включать кавычки). Если файл и родительские папки не существуют, они будут созданы;

- 3) «Имя секции» – имя раздела в файле, свойство которого нужно настроить или удалить. Чтобы удалить INI-файл целиком, следует оставить это поле пустым;
- 4) «Имя свойства» – имя свойства, которое нужно настроить или удалить. Чтобы удалить целиком раздел файла или весь файл, следует оставить это поле пустым;
- 5) «Значение свойства» – значение свойства. Значения могут содержать символы кавычек, которые, однако, при чтении значений приложением или операционной системой обычно удаляются. Все значения воспринимаются как текст. Если данное поле оставлено пустым, свойству присваивается пустое значение, что воспринимается как отсутствие свойства. Этот параметр доступен, если выбрано действие «Создать», «Заменить» или «Обновить».

Политики управления INI-файлами относятся к экспериментальным, поэтому на машинах с ОС Альт СП где они применяются должны быть включены экспериментальные групповые политики (подробнее см. п. 10.4.6.4.7).

Все настройки политики управления INI-файлами хранятся в файлах:

```
{GUID GPT}/Machine/Preferences/Inifiles/Inifiles.xml
{GUID GPT}/User/Preferences/Inifiles/Inifiles.xml
```

Пример файла Inifiles.xml:

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<IniFiles clsid="{694C651A-08F2-47fa-A427-34C4F62BA207}">
  <Ini changed="2022-11-21 09:13:44"
    clsid="{EEFACE84-D3D8-4680-8D4B-BF103E759448}"
    image="3"
    name="version.ini"
    status="version.ini"
    uid="{ADAA9BCF-C2EA-4004-980F-CEDA823E3B91}"
    bypassErrors="1">
    <Properties
      path="C:\tmp\version.ini"
      section=""
      value=""
      property="BP"
      action="D"/>
  </Ini>
</IniFiles>
```

10.4.6.5.4. Управление переменными среды

Групповая политика «Управление переменными среды» позволяет централизованно для компьютеров или пользователей:

- 1) создать постоянные пользовательские или системные переменные среды;
- 2) удалить переменные среды;
- 3) изменить переменные среды, например:
 - изменить приглашение командной строки (системная переменная PROMPT для Windows или PS1 для Linux (BASH));
 - изменить расположение папки временных файлов (системная переменная TEMP для Windows или TMPDIR для Linux);
 - заменить значение всей переменной PATH;
 - добавить сегменты в переменную PATH (разделенные точкой с запятой для Windows или двоеточием для Linux);
 - удалить сегменты из переменной PATH.

Для настройки этой политики следует перейти в «Компьютер»/«Пользователь» → «Настройки» → «Настройки системы» → «Окружение». В контекстном меню свободной области выбрать пункт «Новый» → «Переменные окружения» (рис. 418).

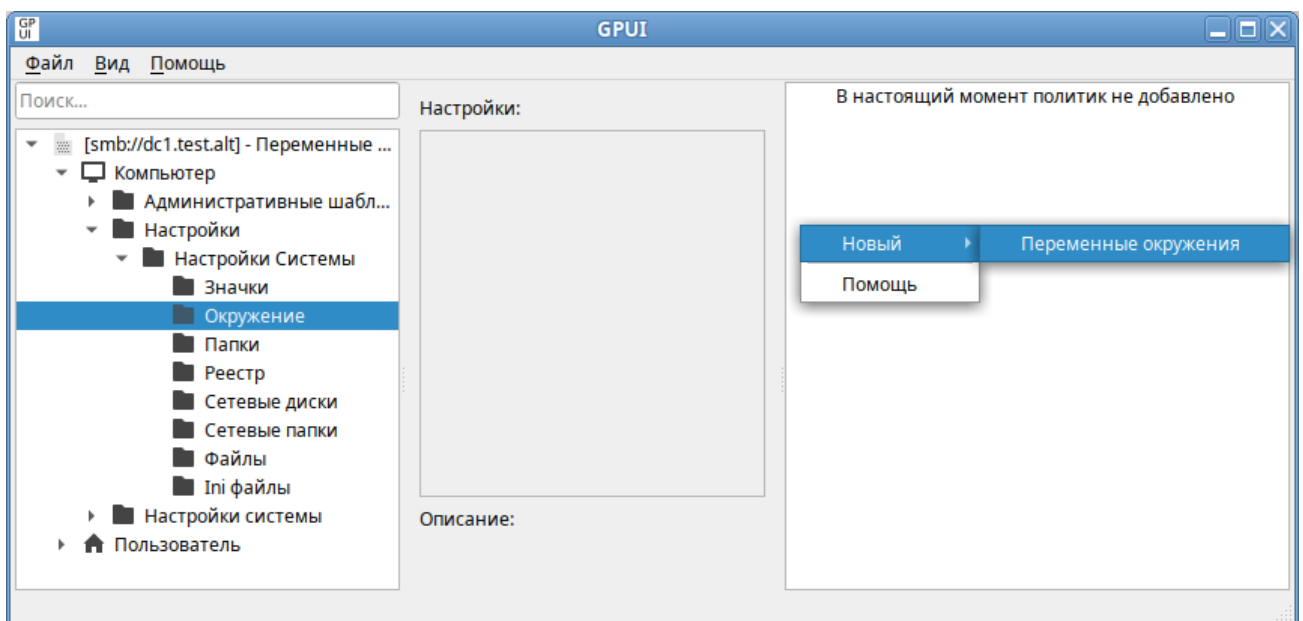


Рис. 418 – Новая политика «Переменные окружения»

В открывшемся диалоговом окне «Диалог настроек» задать настройки политики (рис. 419).

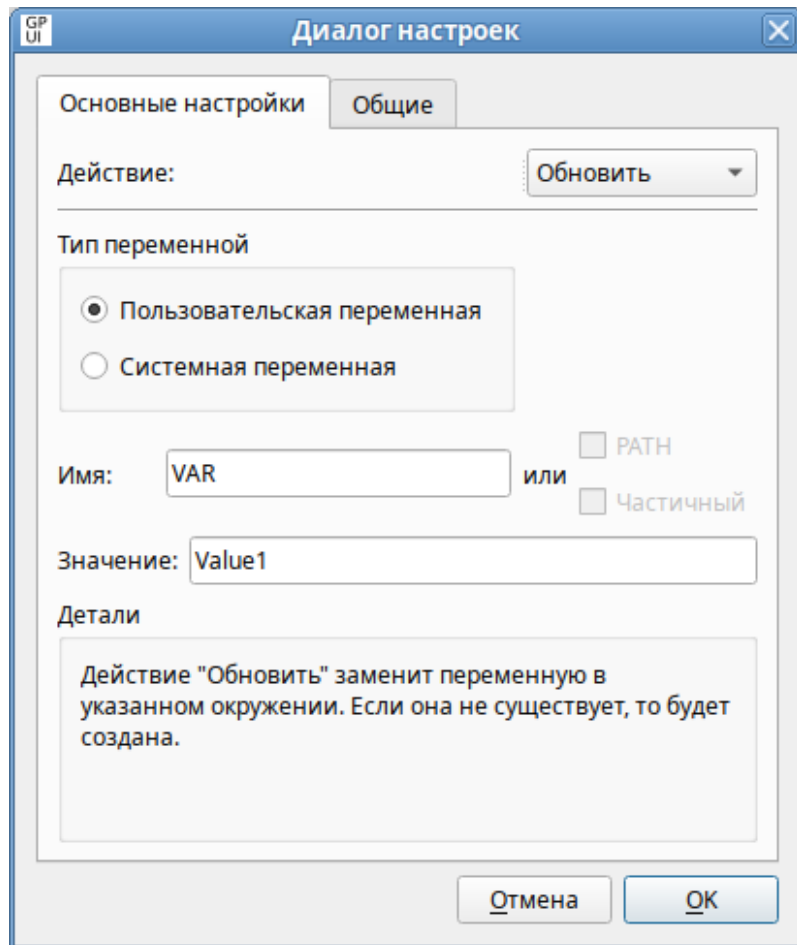


Рис. 419 – Настройки политики «Переменные окружения»

Опции доступные на вкладке «Основные настройки»:

- 1) «Действие» – действие, которое будет выполняться для переменной среды:
 - «Создать» – создание новой переменной среды (если переменная среды с таким именем уже есть, например, создана локально, то ее значение изменено не будет);
 - «Удалить» – удаление переменной среды;
 - «Заменить» – удаление и повторное создание переменной среды (если переменная среды с таким именем не существует, то это действие создает новую переменную среды);
 - «Обновить» – изменение параметров существующей переменной среды. Если переменная среды с таким именем не существует, то это действие

создает новую переменную среды (фактически это действие полностью аналогично действию «Заменить»). Применение этого действия к сегменту переменной PATH не имеет практического эффекта; в этом сегменте возможно только изменение регистра текста;

2) «Пользовательская переменная»:

- параметр для переменной среды в разделе «Конфигурация пользователя» – влияние переменной среды будет для каждого пользователя независимым. Переменная среды хранится в разделе реестра HKEY_CURRENT_USER;
- параметр для переменной среды в разделе «Конфигурация компьютера» – переменная среды будет влиять только на пользователя компьютера по умолчанию;

3) «Системная переменная» – переменная среды будет влиять на всех пользователей компьютера. Переменная среды будет храниться в реестре в разделе HKEY_LOCAL_MACHINE;

4) «Имя» – имя переменной среды, к которой применяется действие. Чтобы выбрать переменную PATH, следует оставить это поле пустым;

5) «Значение» – значение переменной среды. В это поле можно вводить переменные;

6) «PATH» – действие будет применяться к переменной PATH: можно создать/заменить значение переменной PATH или добавить/удалить сегмент значения переменной PATH. В поле «Имя» будет отмечено значение «PATH» и оно не будет доступно для редактирования. Эта опция доступна только в том случае, если выбран параметр «Системная переменная»;

7) «Частичный» – добавить или удалить один сегмент переменной PATH. Эта опция доступна только в том случае, если выбраны «Системная переменная» и «PATH».

Все настройки политики управления INI-файлами хранятся в файлах:

```
{GUID GPT}/Machine/Preferences/EnvironmentVariables/EnvironmentVariables.xml  
{GUID GPT}/User/Preferences/EnvironmentVariables/EnvironmentVariables.xml
```

Пример файла EnvironmentVariables.xml:

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<EnvironmentVariables          clsid="{BF141A63-327B-438a-B9BF-
2C188F13B7AD}">
  <EnvironmentVariable        clsid="{78570023-8373-4a19-BA80-
2F150738EA19}"
    name="VAR"
    status="VAR = value_1"
    image="0"
    changed="2020-06-05 12:16:20"
    uid="{6738058D-5455-4D9A-9B84-78E87DDD18D7}"
    desc="environment variable example"
    bypassErrors="1">
    <Properties
      action="C"
      name="VAR"
      value="value_1"
      user="1"
      partial="0"/>
  </EnvironmentVariable>
  <EnvironmentVariable        clsid="{78570023-8373-4a19-BA80-
2F150738EA19}"
    name="PATH"
    status="PATH = value_2"
    image="2"
    changed="2020-06-05 12:16:48"
    uid="{15E854D6-C338-4AD2-BF8D-72292B364BA3}">
    <Properties
      action="U"
      name="PATH"
      value="value_2"
      user="0"
      partial="1"/>
  </EnvironmentVariable>
</EnvironmentVariables>
```

Примечание. Для того чтобы политики применились (под доменным пользователем) нужно перелогиниться. Проверить наличие переменных окружения можно, выполнив команду:

```
$ env |grep имя_переменной
```

Просмотреть все переменные, назначенные с помощью групповой политики, можно в файле /etc/gpupdate/environment:

```
TEMP_DEFAULT="C:\tmp"
Var_DEFAULT="Value1"
HTTPS_PROXY_DEFAULT=https://10.0.66.52:3128
```

10.4.6.5.5. Управление файлами

Групповая политика «Файлы» позволяет проводить операции с файлами: копировать файлы в нужное расположение, удалять, заменять, обновлять атрибуты файлов.

Для компьютеров или пользователей эта политика предоставляет возможность:

- копировать файл (или несколько файлов из одного каталога) в новое место, а затем настроить атрибуты этих файлов;
- удалить файл (или несколько файлов в одном каталоге);
- удалить файл (или несколько файлов в одном каталоге) и заменить его копией файла из исходного каталога;
- изменить атрибуты файла (или нескольких файлов в одном каталоге);
- изменить атрибуты, заменить или удалить все файлы с определенным расширением в одном каталоге;
- изменить атрибуты, заменить или удалить все файлы в определенном каталоге.

Примечание. В групповой политике «Файлы» нет встроенной возможности скопировать целиком каталог со всем содержимым. Вместо этого можно использовать политику «Папки», которая позволяет создавать каталоги на компьютере, а для копирования файлов использовать групповую политику «Файлы».

Для настройки этой политики следует перейти в «Компьютер»/«Пользователь» → «Настройки» → «Настройки системы» → «Файлы». В контекстном меню свободной области выбрать пункт «Новый» → «Файл» (рис. 420).

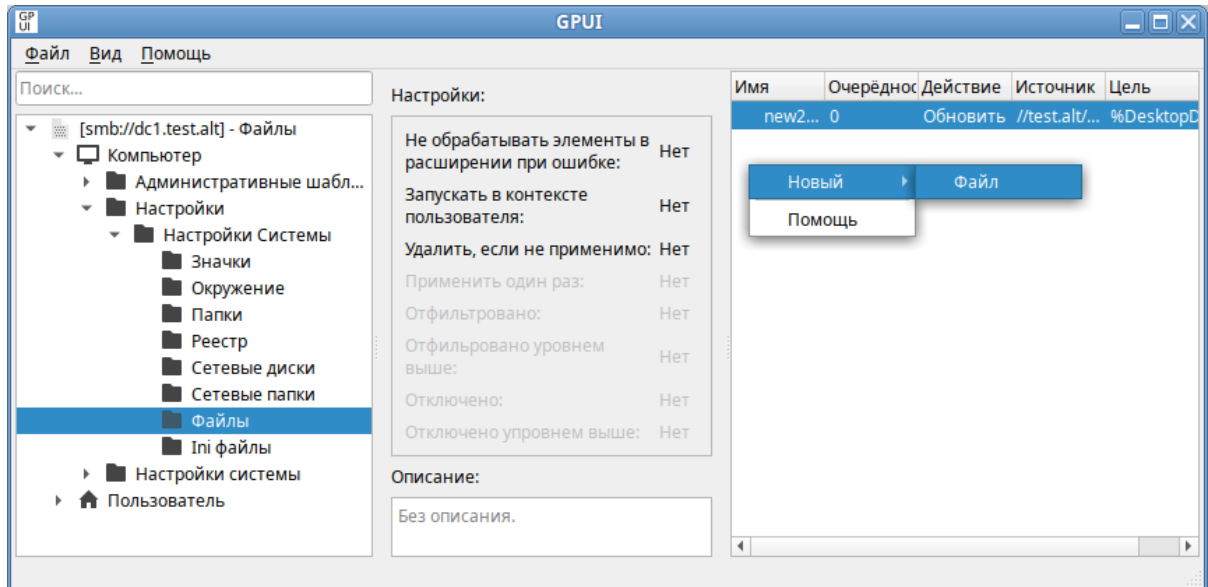


Рис. 420 – Создание новой политики «Файл»

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 421).

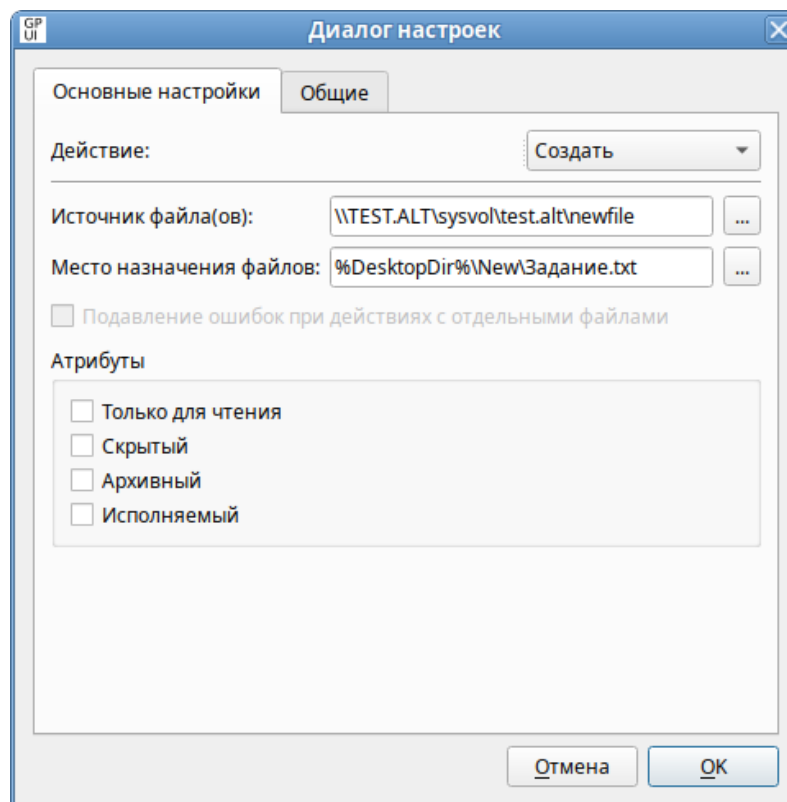


Рис. 421 – Настройки политики «Файл»

Опции доступные на вкладке «Основные настройки»:

1) «Действие» – действие, которое будет выполняться для файла(ов):

- «Создать» – копирование файла (или нескольких файлов из одного каталога) из исходного местоположения в конечное, если файл еще не существует в местоположении назначения, и настройка атрибутов этих файлов;
- «Удалить» – удаление файла (или нескольких файлов в одной папке);
- «Заменить» – удаление файла (или нескольких файлов в одной папке), замена его другим файлом и настройка атрибутов этих файлов. Конечным результатом действия «Заменить» будет перезапись файлов в местоположении назначения. Если файл не существует в месте назначения, действие «Заменить» копирует его из исходного местоположения в место назначения;
- «Обновить» – изменение параметров существующего файла (или нескольких файлов в одной папке). Это действие отличается от действия «Заменить» тем, что только обновляет атрибуты файла, определенные в элементе предпочтений. Все остальные атрибуты файла не изменяются. Если файл не существует, действие «Обновить» копирует его из исходного местоположения в место назначения;

2) «Источник файла(ов)» – местоположение (с точки зрения клиента), из которого требуется скопировать исходные файлы. Это местоположение может представлять полный путь UNC, или локальный путь, или сопоставленный диск со стороны клиента. Это поле может содержать переменные. Поле может содержать подстановочные знаки одного (?) или нескольких (*) символов, позволяя копировать или изменять несколько файлов (только для работы с файлами в ОС Windows). Поле недоступно для действия «Удалить».

Примечание. В настоящее время в ОС Альт СП можно использовать подстановочный знак (*) только для копирования всех файлов из папки (рис. 422).

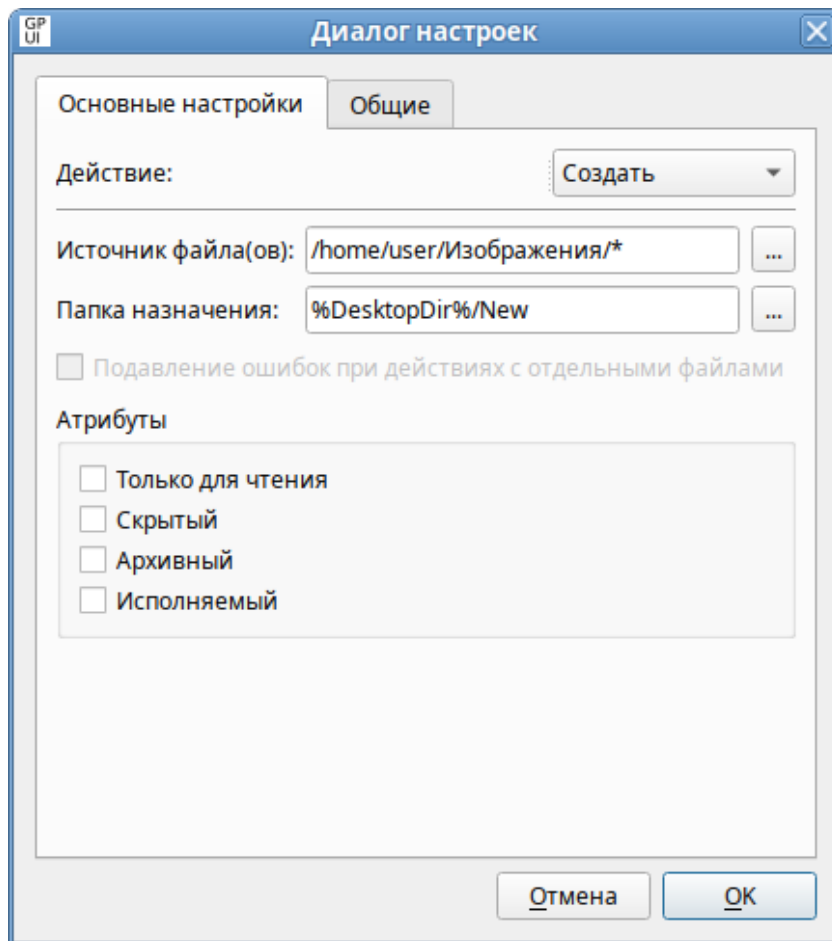


Рис. 422 – Копирование всех файлов из папки

- 3) «Место назначения файлов» – местоположение папки (с точки зрения клиента), в которую требуется скопировать файлы, или местоположение файлов, которые требуется изменить. Это местоположение может представлять полный путь UNC, или локальный путь, или сопоставленный диск со стороны клиента. Родительские папки создаются по мере необходимости. Нужно включить имя файла, которое затем можно будет изменить, указав другое имя в поле Исходные файлы. Это поле может содержать переменные. Этот параметр доступен, если выбрано действие «Создать», «Заменить» или «Обновить», а поле «Источник файла(ов)» не содержит подстановочные знаки;
- 4) «Папка назначения» – место назначения копирования файла или местоположение файла (с точки зрения клиента), который требуется изменить. Это местоположение может представлять полный путь UNC, или

локальный путь, или сопоставленный диск со стороны клиента. Родительские папки создаются по мере необходимости. Это поле может содержать переменные. Этот параметр доступен, если выбрано действие «Создать», «Заменить» или «Обновить», а поле «Источник файла(ов)» включает подстановочные знаки;

- 5) «Удалить файл(ы)» – путь к файлу (с точки зрения клиента), который требуется удалить. Чтобы удалить несколько файлов из одной папки нужно включить в имя файла подстановочные знаки одного (?) или нескольких (*) символов (только для удаления файлов в ОС Windows). Этот параметр доступен, только если выбрано действие «Удалить» (рис. 423).

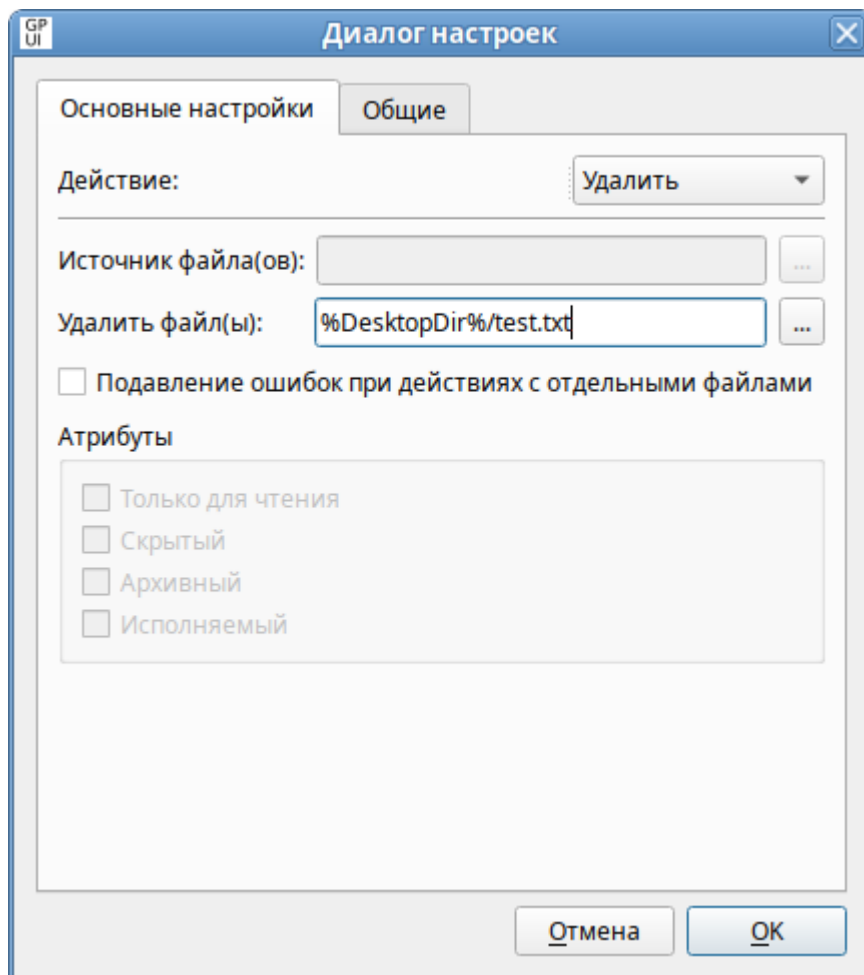


Рис. 423 – Настройка политики «Удаление файла»

- 6) «Подавление ошибок при действиях с отдельными файлами» – разрешить передачу одного или нескольких файлов даже в случае сбоя передачи

отдельных файлов. Не отображаются только ошибки, связанные с попыткой замены, удаления или настройки атрибутов файла. Такие ошибки могут быть вызваны тем, что файл используется, был отказ в доступе или исходный файл не найден. Если этот параметр включен, такие ошибки могут быть обнаружены только в файле трассировки. Этот параметр отличается от параметра пропуска ошибок предпочтений по умолчанию, который можно изменить на вкладке «Общее»;

7) «Атрибуты» – атрибуты файловой системы для папки (недоступны для действия «Удалить»):

- «Только для чтения»;
- «Скрытый»;
- «Архивный»;
- «Исполняемый».

Примечание. Атрибуты «Архивный», «Скрытый» и «Только для чтения» применимы только для Windows систем.

Политики управления файлами относятся к экспериментальным, поэтому на машинах с ОС Альт СП где они применяются должны быть включены экспериментальные групповые политики (подробнее см. п. 10.4.6.4.7).

Опционально можно включить политику «Настройка механизма копирования файлов». Данная политика конфигурирует механизм «копирования файлов», формируя список суффиксов (расширений), идентифицирующих файл как исполняемый, (например, .sh) и список целевых путей копирования.

Для включения политики «Настройка механизма копирования файлов» следует в разделе «Компьютер» → «Административные шаблоны» → «Система ALT» → «Групповые политики» выбрать пункт «Настройка механизма копирования файлов». В открывшемся окне установить отметку в поле «Включено» (рис. 424).

Для задания списка суффиксов (расширений), идентифицирующих файл как исполняемый, в поле «Список суффиксов файлов» нажать кнопку «Редактировать» и в открывшемся окне ввести список суффиксов, по одному на каждой строке (рис. 425).

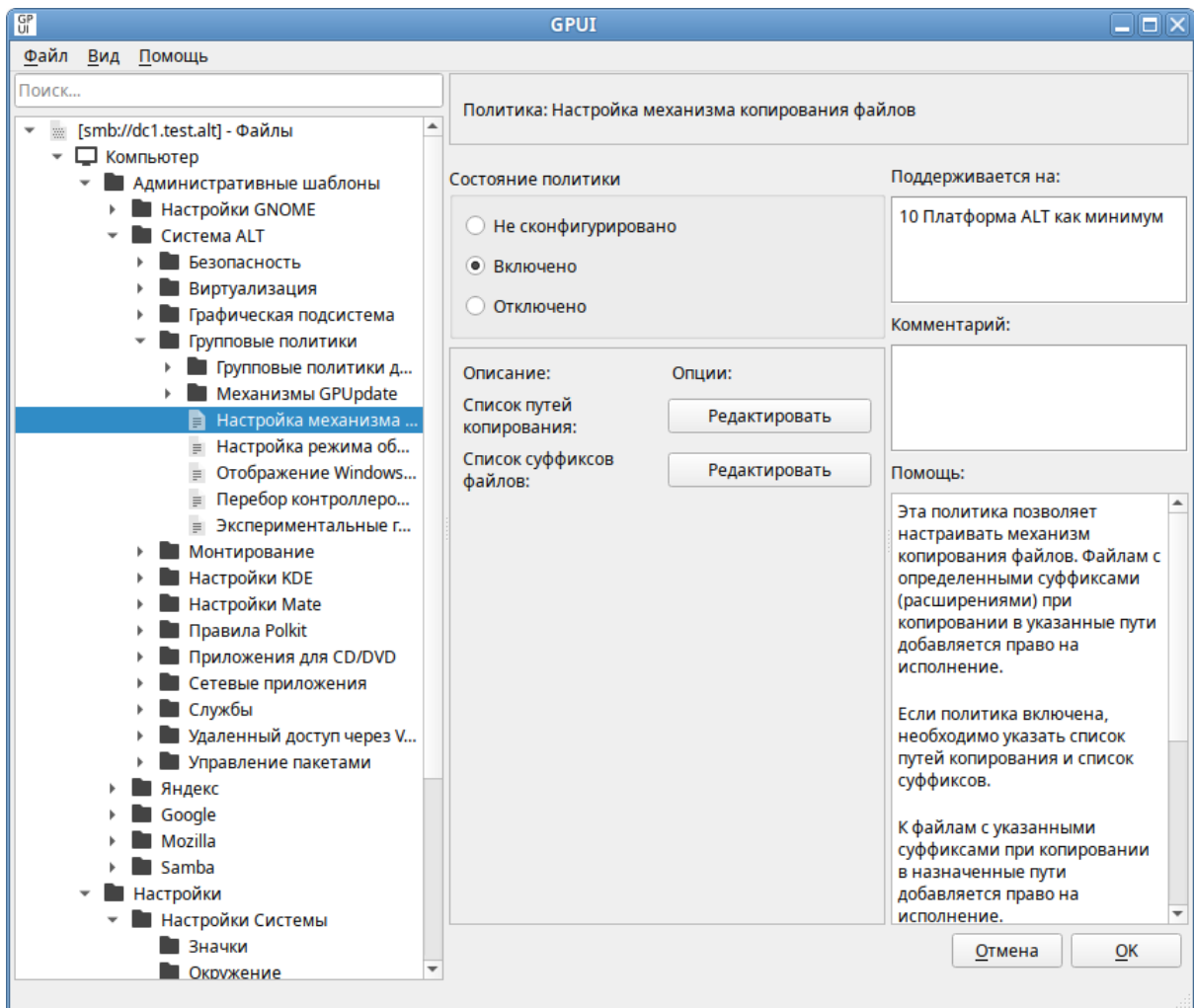


Рис. 424 – Политика «Настройка механизма копирования файлов»

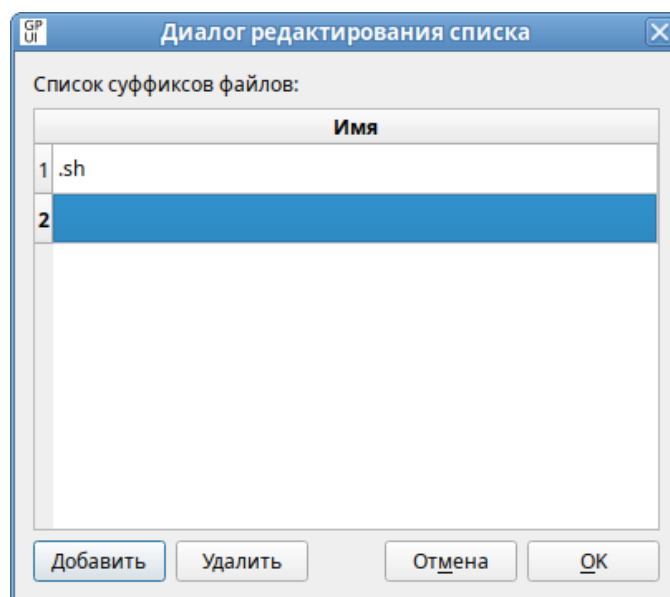


Рис. 425 – Список суффиксов файлов

Для задания списка целевых путей копирования в поле «Список путей копирования» нажать кнопку «Редактировать» и в открывшемся окне ввести список путей, по одному на каждой строке (рис. 426).

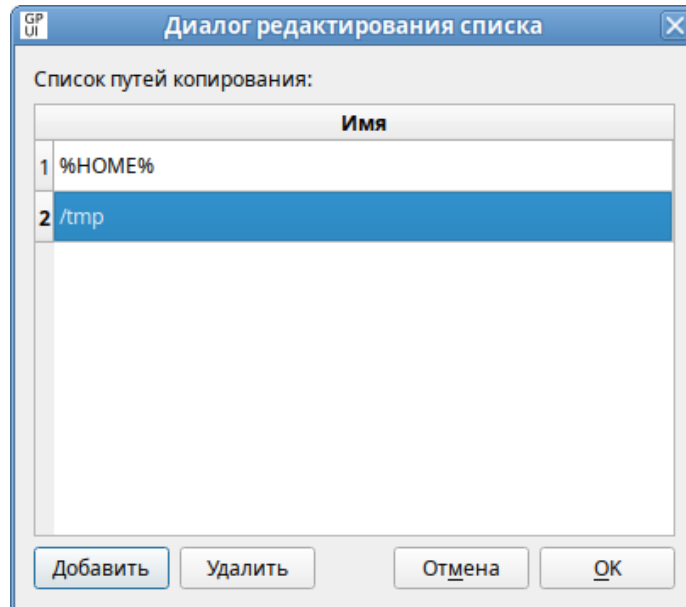


Рис. 426 – Список путей копирования

В результате применения данной политики при копировании файлов с указанными суффиксами в назначенные пути, этим файлам будет задано право на выполнение (chmod +x).

Все настройки политики управления файлами хранятся в файлах:

```
{GUID GPT}/Machine/Preferences/Files/Files.xml
{GUID GPT}/User/Preferences/Files/Files.xml
```

Пример файла Files.xml:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<Files clsid="{215B2E53-57CE-475c-80FE-9EEC14635851}">
  <File bypassErrors="0"
    changed="2023-08-20 13:18:25"
    clsid="{50BE44C8-567A-4ed1-B1D0-9234FE1F38AF}"
    desc="Файл с сервера"
    image="0"
    name="Задание.txt"
    removePolicy="0"
    status=""
    uid="{cd0d3cba-8698-4612-9c76-5e21da62cc48}"
    userContext="0">
  <Properties
```

```
    action="C"  
    archive="0"  
    executable="0"  
    fromPath="\\TEST.ALT\sysvol\test.alt\newfile"  
    hidden="0"  
    readOnly="0"  
    suppress="0"  
    targetPath="%DesktopDir%\New\Задание.txt"/>  
</File>  
</Files>
```

10.4.6.5.6. Управление общими каталогами

Групповая политика «Управление общими каталогами» позволяет:

- 1) создать общие ресурсы и настроить их свойства;
- 2) изменить путь к папке общего ресурса путем замены ресурса;
- 3) удалить (вывести из общего доступа) или изменить лимит пользователей, функцию перечисления на основе доступа и комментариев для следующих объектов:
 - общий ресурс;
 - все общие ресурсы, кроме скрытых;
 - все скрытые ресурсы, кроме административных общих ресурсов с присвоением буквы диска;
 - все административные общие ресурсы с присвоением буквы диска;
 - все общие ресурсы.

Примечание. Для создания общего сетевого ресурса, папка, используемая при их создании, должна существовать на всех компьютерах, к которым применяется объект групповой политики. Вместе с удалением сетевого ресурса удаляется ссылка на папку, но не сама папка и ее содержимое.

Примечание. Для поддержки общих сетевых ресурсов с помощью политик на клиенте должны быть выполнены следующие условия:

- установлен пакет `samba-usershares`;
- `control smb-conf-usershares` установлен в `enabled`;
- в файле `/etc/samba/smb.conf` в секции `[global]` подключен файл `/etc/samba/usershares.conf`:

```
include = /etc/samba/usershares.conf
```

Примечание. Для создания или удаления папок с помощью групповой политики можно использовать предпочтение «Папки».

Для настройки этой политики следует перейти в «Компьютер»/«Пользователь» → «Настройки» → «Настройки системы» → «Сетевые папки». В контекстном меню свободной области выбрать пункт «Новый» → «Сетевая папка» (рис. 427).

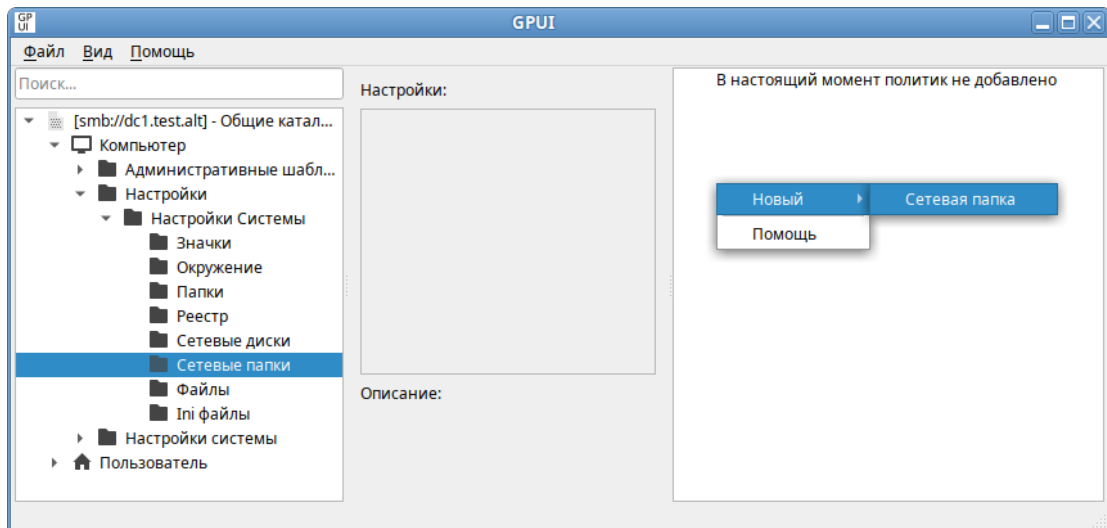


Рис. 427 – Создание новой политики «Сетевая папка»

В диалоговом открывшемся окне «Диалог настроек» задать настройки политики (рис. 428).

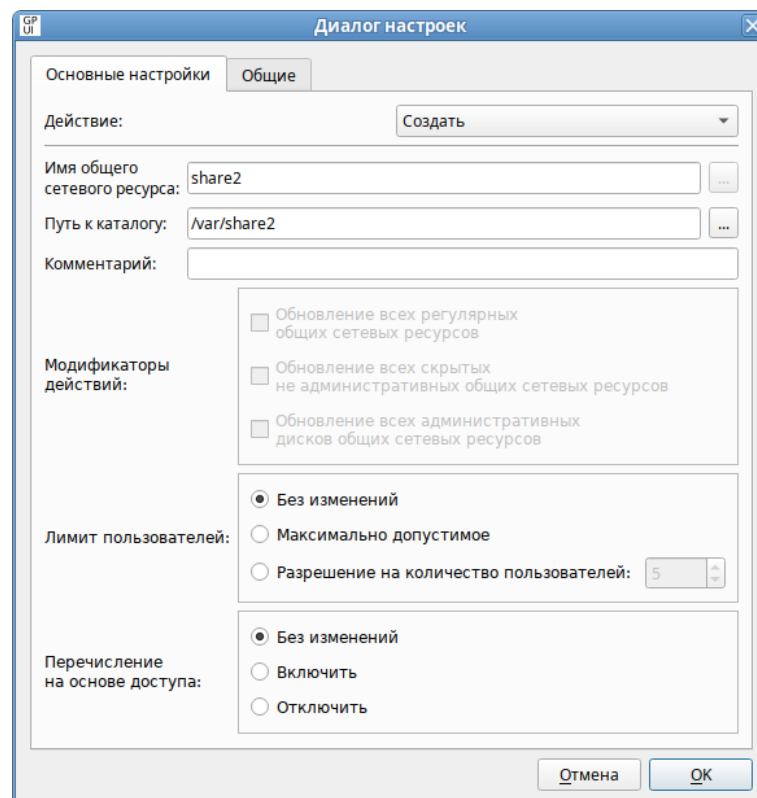


Рис. 428 – Настройки политики «Сетевая папка»

Опции доступные на вкладке «Основные настройки»:

- 1) «Действие» – действие, которое будет выполняться для общего сетевого ресурса:
 - «Создать» – создание нового сетевого ресурса;
 - «Удалить» – удаление общего ресурса;
 - «Заменить» – удаление и повторное создание сетевого ресурса. Суммарный итог действия «Заменить» – переопределение всех существующих параметров, связанных с общим ресурсом. Если сетевого ресурса не существует, то это действие создает новый сетевой ресурс;
 - «Обновить» – изменение параметров существующего сетевого ресурса. Если сетевого ресурса не существует, то это действие создает сетевой ресурс. Это действие отличается от «Заменить» тем, что не удаляет сетевой ресурс, а только обновляет параметры сетевого ресурса, определенные в элементе настройки;
- 2) «Имя общего сетевого ресурса» – имя общего ресурса. В этом поле можно указывать переменные;
- 3) «Путь к каталогу» – путь к существующей папке, на которую будет указывать общий ресурс. В этом поле можно указывать переменные;
- 4) «Комментарий» – текст для отображения в поле «Примечание» общего ресурса. Если выбрано действие «Обновить», общий ресурс уже существует и данное поле оставлено пустым, существующий комментарий будет оставлен без изменений. В этом поле можно указывать переменные. Этот параметр доступен, если выбрано действие «Создать», «Заменить» или «Обновить»;
- 5) «Модификаторы действий» – изменять и удалять общие ресурсы конкретного типа можно не только индивидуально, но и все вместе. Эти параметры доступны, если выбранное действие – «Обновить» или «Удалить»:
 - «Обновление всех регулярных общих сетевых ресурсов» – изменение или удаление всех общих ресурсов, которые не являются скрытыми

(с именами, оканчивающимися на \$) или специальными (SYSVOL или NETLOGON);

- «Обновление всех скрытых не административных общих сетевых ресурсов» – изменение или удаление всех скрытых общих ресурсов, за исключением административных общих ресурсов с буквенным обозначением дисков, ADMIN\$, FAX\$, IPC\$ и PRINT\$;
- «Обновление всех административных дисков общих сетевых ресурсов» – изменение или удаление всех административных общих ресурсов с буквенным обозначением дисков (в их именах после буквы диска следует \$);

6) «Лимит пользователей» – настройка числа пользователей, которым можно одновременно подключаться к общему ресурсу:

- «Без изменений» – не изменять допустимое число пользователей при обновлении общего ресурса (если этот параметр выбран при создании или замене общего ресурса, число пользователей будет настроено на максимально допустимое);
- «Максимально допустимое» – неограниченное число пользователей;
- «Разрешение на количество пользователей» – ограничить число пользователей (следует ввести допустимый максимум пользователей);

7) «Перечисление на основе доступа» – настройка видимости папок общего ресурса:

- «Без изменений» – не изменять видимость папок общего ресурса при обновлении общего ресурса;
- «Включить» – сделать папки общего ресурса видимыми только при наличии доступа на чтение;
- «Отключить» – сделать папки общего ресурса видимыми для всех пользователей.

Политики управления общими каталогами относятся к экспериментальным, поэтому на машинах с ОС Альт СП где они применяются должны быть включены экспериментальные групповые политики (подробнее см. п. 10.4.6.4.7).

Все настройки политики управления общими каталогами хранятся в файлах:

```
{GUID GPT}/Machine/Preferences/NetworkShares/NetworkShares.xml
{GUID GPT}/User/Preferences/NetworkShares/NetworkShares.xml
```

Пример файла NetworkShares.xml:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<NetworkShareSettings clsid="{520870D8-A6E7-47e8-A8D8-
E6A4E76EAEC2}">
  <NetShare changed="2022-11-21 13:03:10"
    clsid="{2888C5E7-94FC-4739-90AA-2C1536D68BC0}"
    image="0"
    name="share2"
    status=""
    uid="{cd0d3cba-8698-4612-9c76-5e21da62cc48}"
    userContext="0"
    removePolicy="0">
    <Properties
      action="C"
      name="share2"
      path="/var/share2"
      comment=""
      limitUsers="NO_CHANGE"
      abe="NO_CHANGE"/>
    </NetShare>
</NetworkShareSettings>
```

10.4.6.5.7. Подключение сетевых дисков

Групповая политика «Подключение сетевых дисков» позволяет осуществлять доступ к сетевым общим каталогам как к каталогам в локальной файловой системе. Политика служит для создания, замены, обновления и удаления сопоставленных дисков и их свойств.

Точки монтирования для отображения общих ресурсов на машинах ОС Альт СП:

- /media/gpupdate/drives.system – для системных ресурсов;
- /media/gpupdate/.drives.system – для скрытых системных ресурсов;
- /run/media/USERNAME/drives – для общих ресурсов пользователя;

- /run/media/USERNAME/.drives – для скрытых общих ресурсов пользователя.

Для настройки этой политики следует перейти в «Компьютер»/«Пользователь» → «Настройки» → «Настройки системы» → «Сетевые диски». В контекстном меню свободной области выбрать пункт «Новый» → «Сетевой диск» (рис. 429).

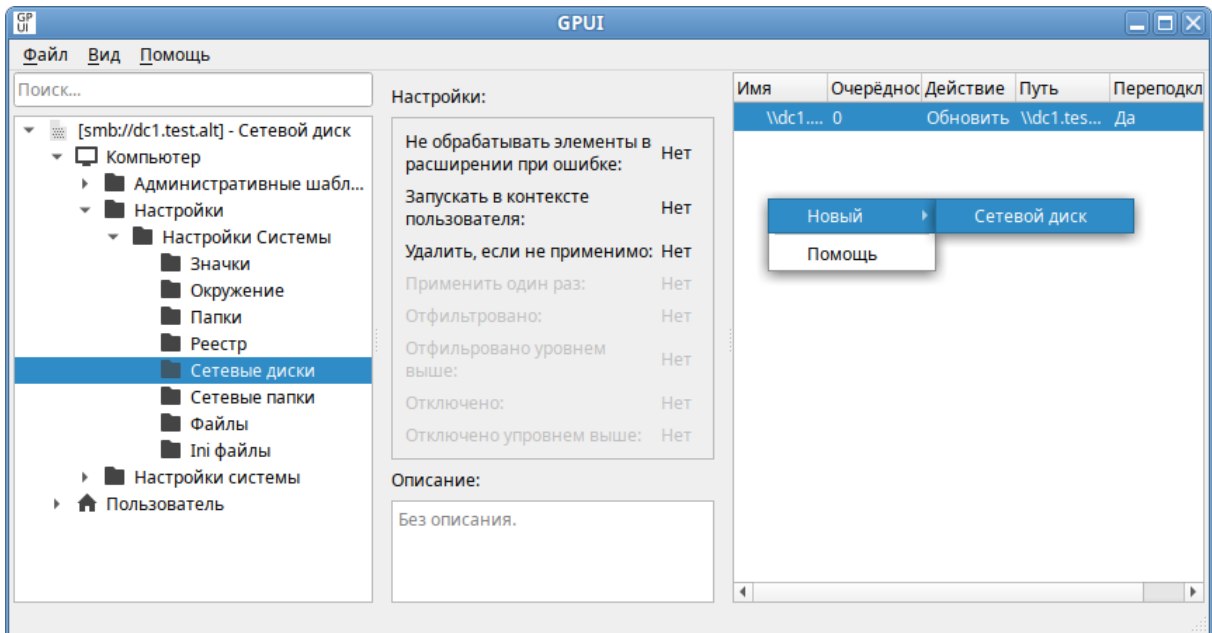


Рис. 429 – Создание новой политики «Сетевой диск»

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 430).

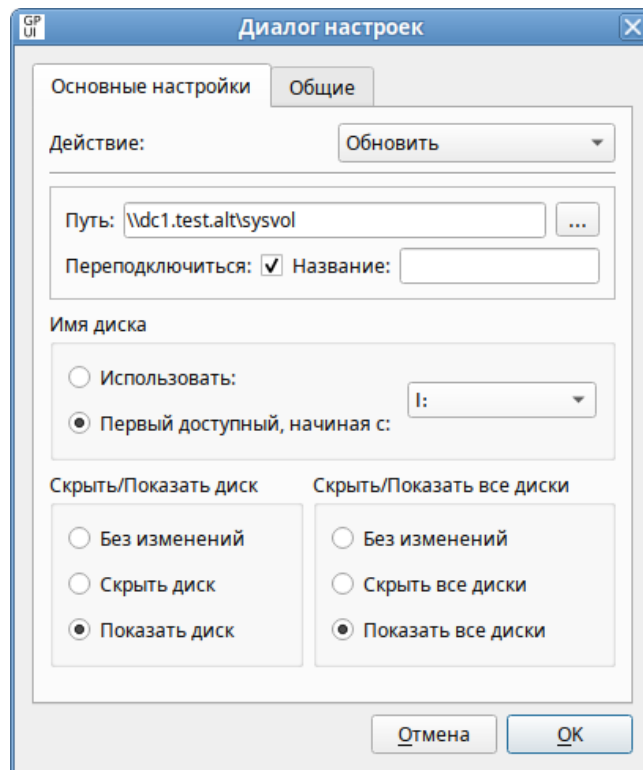


Рис. 430 – Настройки политики «Сетевой диск»

Опции доступные на вкладке «Основные настройки»:

- 1) «Действие» – поведение элемента настройки зависит от выбранного действия и от того, существует ли уже выбранная буква диска:
 - «Создать» – создание нового сетевого диска;
 - «Удалить» – удаление сетевого диска. Нельзя удалить локальный диск рабочей станции (жесткий диск, CD-Drive);
 - «Заменить» – удаление и повторное создание сетевого диска. Если диск до этого не был создан, то будет создан новый диск. Нельзя заменить локальный диск рабочей станции (жесткий диск, CD-Drive);
 - «Обновить» – изменение параметров существующего сетевого диска или создание нового, если диска с заданной буквой не существует. Это действие отличается от «Заменить» тем, что оно не удаляет диск, а только обновляет настройки (кроме пути к общей папке и буквы);
- 2) «Путь» – путь к общей папке или диску, который нужно отобразить (полный UNC-путь к сетевому общему ресурсу, например, \\server\sharename, \\server\hiddenshare\$ или

\\server\sharename\foldername). Это поле может содержать переменные. Чтобы изменить существующий сетевой диск (определяемый по букве диска), следует оставить это поле пустым;

- 3) «Переподключиться» – сохранять подключенный диск в настройках пользователя и повторно подключать его при каждом входе в систему;
- 4) «Название» – пользовательское имя для диска (можно оставить это поле пустым);

Примечание. Название должно представлять собой одно слово, состоящее только из латинских букв, цифр и символа подчеркивания, иначе монтирование не произойдет.

- 5) «Имя диска» – буква, на которую будет назначен диск:

- чтобы назначить сетевому диску первую доступную букву диска, следует выбрать «Первый доступный, начиная с», а затем выбрать букву диска, с которой начинать проверку доступности букв;
- чтобы назначить сетевому диску определенную букву, следует выбрать «Использовать», а затем выбрать букву диска (если рабочая станция уже использует выбранную здесь букву, сопоставление дисков групповой политики завершится неудачно);
- чтобы изменить существующее сопоставление диска (определяемое буквой диска), следует выбрать «Использовать», а затем выбрать букву диска;
- чтобы удалить все сопоставления дисков, начиная с определенной буквы, следует выбрать «Удалить, начиная с», а затем выбрать букву диска, с которой следует начать удаление сопоставлений дисков. Физические диски пропускаются без ошибок. Данный параметр доступен только при выбранном действии «Удалить»;
- чтобы удалить определенный сопоставленный диск, следует выбрать «Удалить», а затем выбрать букву диска. Данный параметр доступен только при выбранном действии «Удалить»;

б) параметры «Скрыть»/«Показать» – настройка отображения сопоставленного диска (параметры «Скрыть»/«Показать диск» имеют приоритет над параметрами «Скрыть»/«Показать все диски»):

- «Без изменений» – оставить отображение сопоставленного диска неизменным;
- «Скрыть диск» – скрыть диск в окне файлового менеджера;
- «Показать диск» – отобразить диск в окне файлового менеджера.

Примечание. Пункт «Имя диска» совместно с «Первый доступный, начиная с» рекомендуется использовать для дисков, которые должны подключаться в ОС Windows. Так как если будет создано несколько дисков с данными параметрами, то в ОС Альт СП будет отображаться только один диск (последний).

При выборе параметра «Показать диск» к точке монтирования (файл `/etc/auto.master.gpupdate.d/<имя>.autofs`) добавляется опция `--browse`. В этом случае для данной точки монтирования будет создан пустой каталог, независимо от того, смонтирована ли какая-либо файловая система в него или нет. Это удобно так как доступные автоматически монтируемые файловые системы будут показаны как существующие каталоги, даже если их файловые системы в данный момент не смонтированы.

При выборе параметра «Скрыть диск» необходимо запомнить название каталога, так как доступ к этому каталогу можно получить только при непосредственном обращении к нему. Каталог будет создан и файловая система будет смонтирована только при попытке доступа к нему. Незадействованный ресурс по истечении таймаута (по умолчанию 120 секунд) будет отмонтирован, а каталог удален.

Политики подключения сетевых дисков относятся к экспериментальным, поэтому на машинах с ОС Альт СП где они применяются должны быть включены экспериментальные групповые политики (подробнее см. п. 10.4.6.4.7).

Если необходимо, можно включить отображение ссылок (`symlink`) на соответствующий сетевой ресурс в домашнем каталоге пользователя (чтобы можно было очевидно наблюдать смонтированные ресурсы). Для этого следует включить политики монтирования «Отображение сетевых дисков пользователя в домашнем

каталоге» и (или) «Отображение сетевых дисков машины в домашнем каталоге». Политики монтирования находятся в разделе «Пользователь» → «Административные шаблоны» → «Система ALT» → «Монтирование» (рис. 431).

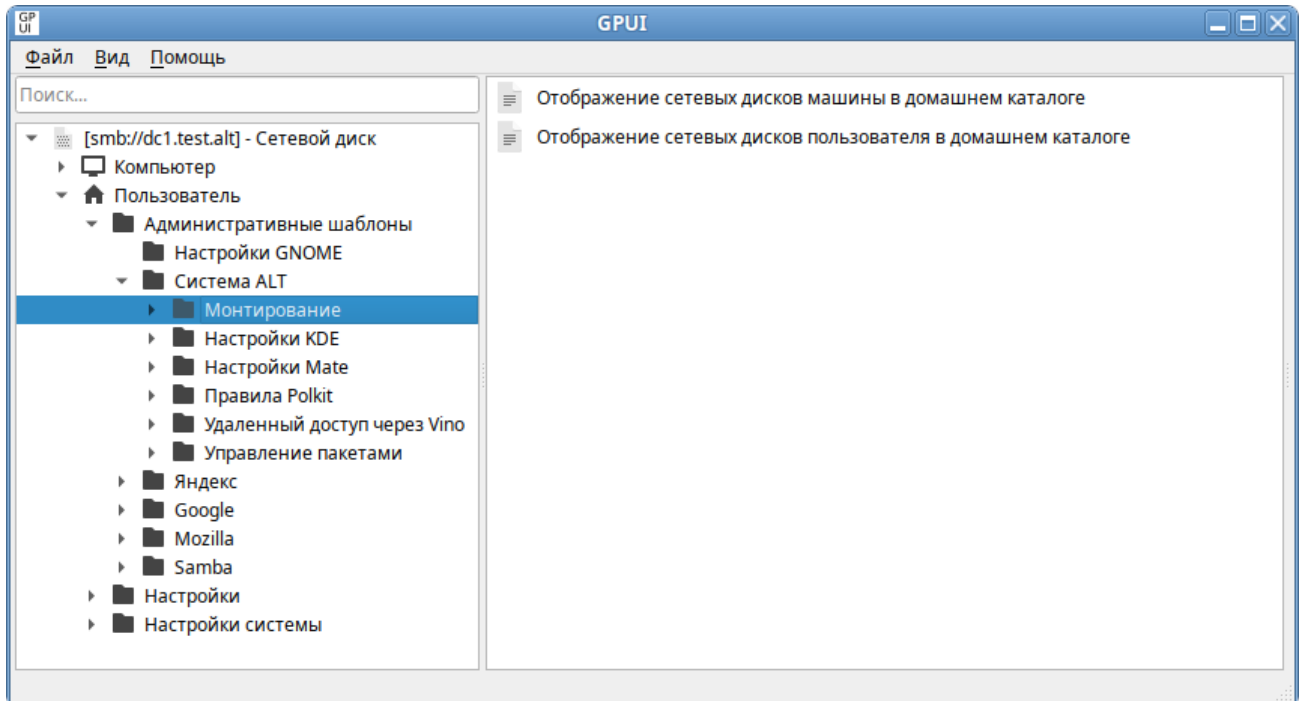


Рис. 431 – Раздел «Монтирование»

Для включения политики монтирования нужно щелкнуть на нужной политике, в открывшемся окне установить отметку в поле «Включено» и нажать кнопку «ОК» (рис. 432).

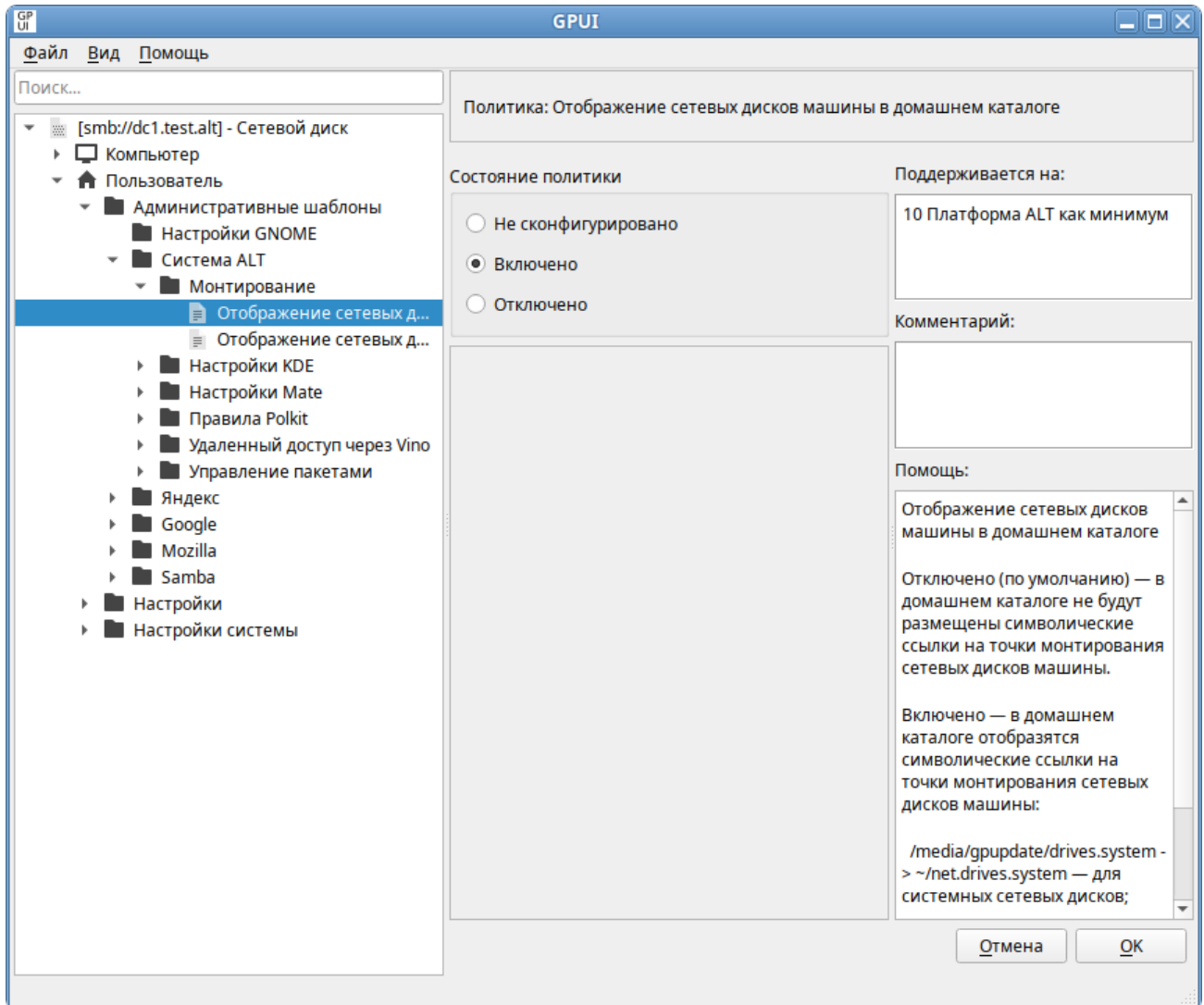


Рис. 432 – Включение политики монтирования

После обновления политик в сессии пользователя будет подключен сетевой диск, доступный из файлового менеджера и других программ (рис. 433, рис. 434).

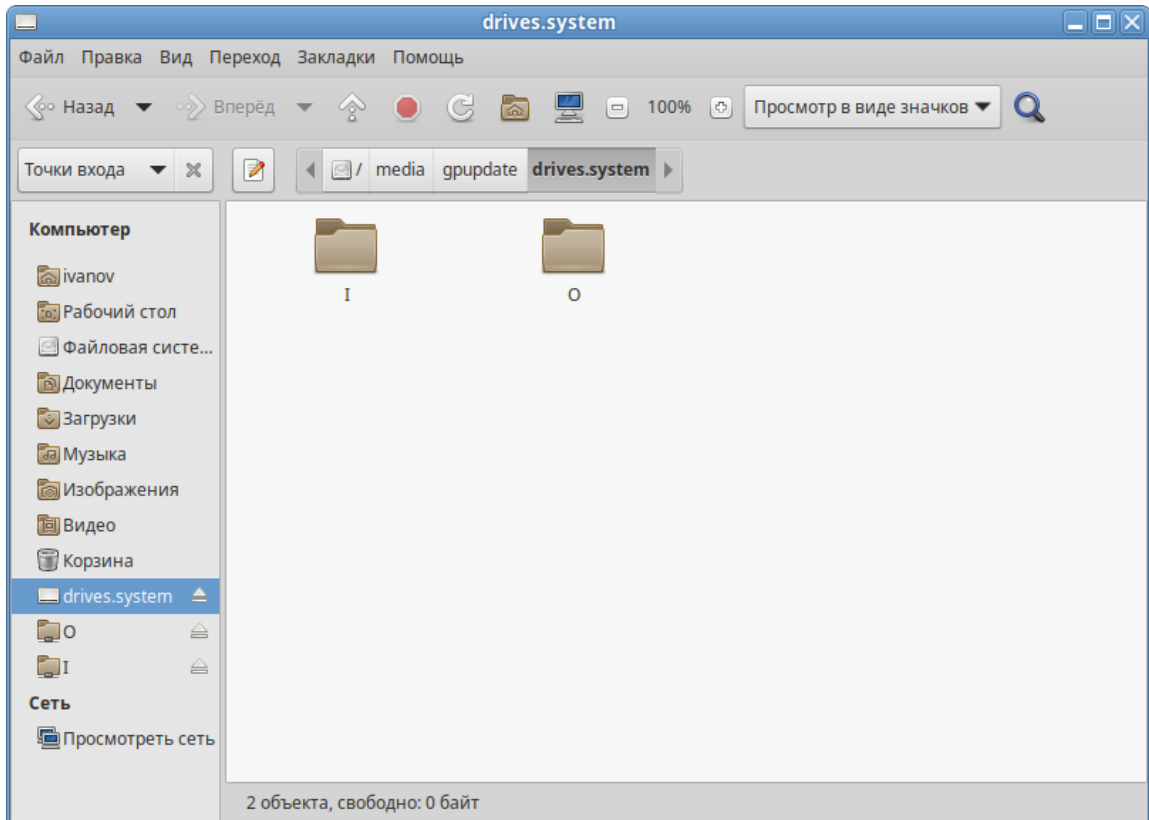


Рис. 433 – Сетевые диски в файловом менеджере Caja

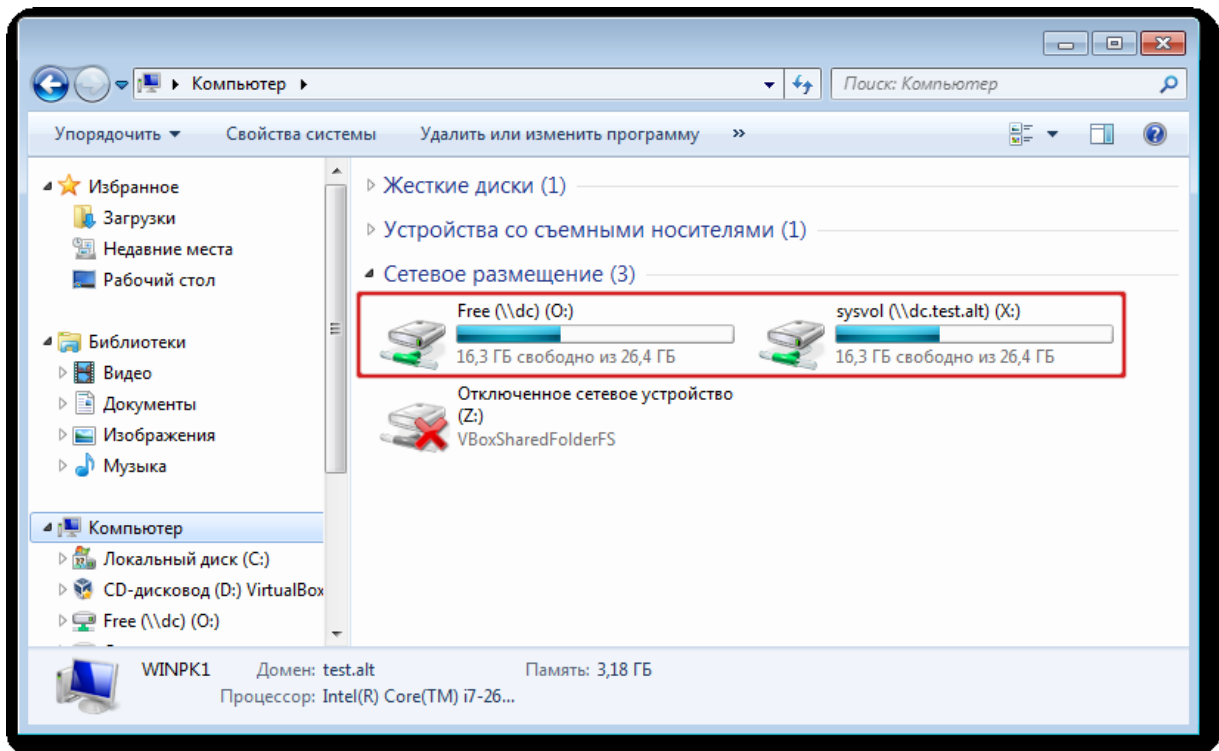


Рис. 434 – Сетевые диски в проводнике Windows

Если включены политики монтирования, в домашнем каталоге пользователя появятся ссылки:

- ~/net.drives.system – ссылка на /media/gpupdate/drives.system;
- ~/.net.drives.system – ссылка на /media/gpupdate/.drives.system;
- ~/net.drives – ссылка на /run/media/USERNAME/drives;
- ~/.net.drives – ссылка на /run/media/USERNAME/.drives.

Все настройки политики управления файлами хранятся в файлах:

```
{GUID GPT}/Machine/Preferences/Drives/Drives.xml
{GUID GPT}/User/Preferences/Drives/Drives.xml
```

В одном GPO возможно задать подключение более одного сетевого диска.

Пример файла Drives.xml:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<Drives clsid="{8FDDCC1A-0C3C-43cd-A6B4-71A6DF20DA8C}">
  <Drive bypassErrors="0"
    changed="2022-11-29 16:28:32"
    clsid="{935D1B74-9CB8-4e3c-9914-7DD559B7A417}"
    desc=""
    image="2"
    name="//dc1.test.alt\Free"
    removePolicy="0"
    status="O:"
    uid="{D070D4D6-DEB5-4DDE-9A53-6AB33C90352A}"
    userContext="0">
    <Properties
      action="U"
      allDrives="SHOW"
      cpassword=""
      label=""
      letter="O"
      path="//dc\Free"
      persistent="1"
      thisDrive="SHOW"
      useLetter="1"
      userName=""/>
  </Drive>
</Drives>
```

10.4.6.5.8. Настройка реестра

Групповая политика «Настройка реестра» позволяет управлять настройками реестра Windows.

Для настройки этой политики следует перейти в «Компьютер/Пользователь» → «Настройки» → «Настройки системы» → «Реестр». В контекстном меню свободной области выбрать пункт «Новый» → «Значение реестра» (рис. 435).

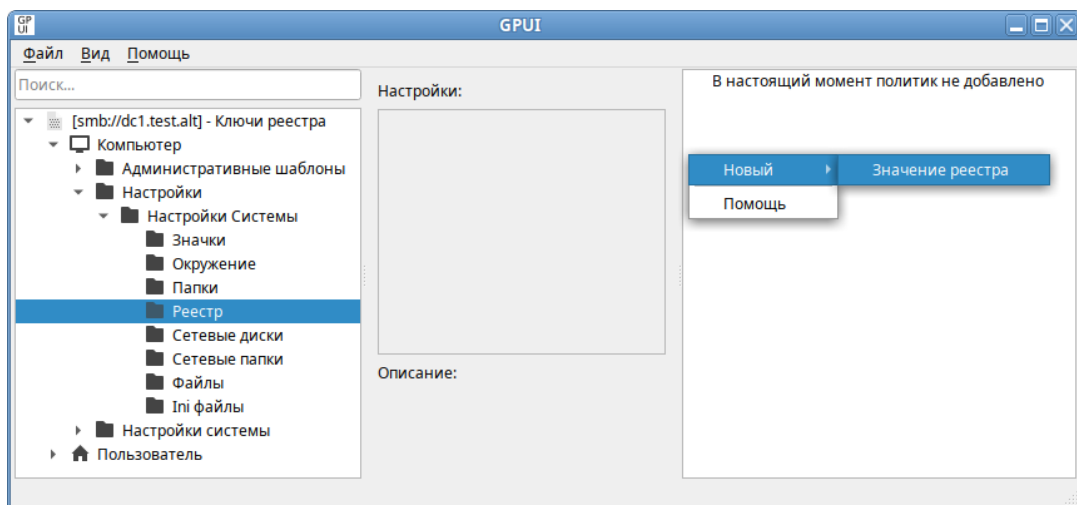


Рис. 435 – Создание политики «Значение реестра»

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 436).

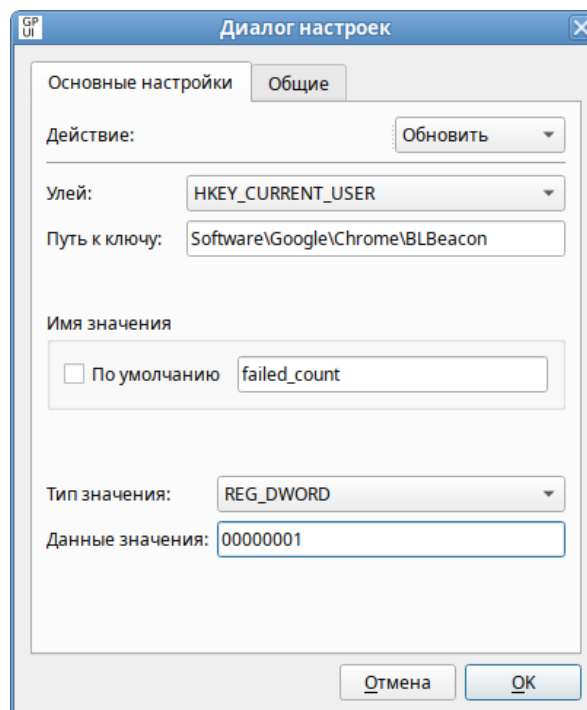


Рис. 436 – Настройки политики «Значение реестра»

Опции доступные на вкладке «Основные настройки»:

1) «Действие» – действие, которое будет выполняться для элемента реестра:

- «Создать» – создание нового значения или раздела, которое будет выполняться для элемента реестра;
- «Удалить» – удаление, которое будет выполняться для элемента реестра, всех его значений и подразделов;
- «Заменить» – удаление и повторное создание значения или раздела реестра. Если целевым объектом является значение реестра, то конечным результатом действия будет перезапись всех существующих параметров, сопоставленных данному значению реестра. Если целевым объектом является раздел реестра, то конечным результатом будет удаление всех значений и подразделов реестра, и останется только имя значения по умолчанию без данных. Если значение или раздел реестра не существует, то действие «Заменить» приведет к созданию нового значения или раздела;
- «Обновить» – изменение параметров существующего значения или раздела реестра. Это действие отличается от «Заменить» тем, что оно обновляет только параметры, определенные в элементе настройки. Все остальные параметры значения или раздела реестра остаются прежними. Если значение или раздел реестра не существует, то действие «Обновить» приведет к созданию нового значения или раздела;

2) «Улей» – улей (куст) для раздела реестра:

- «HKEY_CLASSES_ROOT» – информация о зарегистрированных в Windows типах файлов (это псевдоним для HKEY_LOCAL_MACHINE\Software\Classes);
- «HKEY_CURRENT_USER» – настройки пользователя, вошедшего в Windows (это псевдоним для HKEY_USERS\куст текущего пользователя). HKEY_USERS\.Default используется в том случае, когда HKEY_CURRENT_USER настроен в разделе конфигурации компьютера;

- «HKKEY_LOCAL_MACHINE» – настройки, относящиеся к компьютеру (параметр по умолчанию для политики компьютера). Эти параметры применяются ко всем пользователям компьютера;
 - «HKKEY_USERS» – настройки для всех пользователей (параметр по умолчанию для политики пользователя). Эти параметры применяются к отдельным пользователям;
 - «HKKEY_CURRENT_CONFIG» – сведения о настройках оборудования (это псевдоним для HKKEY_LOCAL_MACHINE\System\CurrentControlSet\Hardware Profiles\Current).
- 3) «Путь к ключу» – путь к ключу. Не нужно указывать улей и вводить косую черту до или после пути. Это поле воспринимает переменные процесса настройки;
- 4) «Имя значения» – для настройки значения следует установить, либо отметку в пункте «По умолчанию», чтобы принять значение раздела по умолчанию, либо ввести имя настраиваемого значения. Чтобы настроить только раздел, следует оставить это поле пустым. В этом поле можно указать переменные;
- 5) «Тип значения» – тип значения. Данный параметр доступен только при выбранном действии «Создать», «Заменить» или «Обновить», и введенном значении «Имя значения»;
- 6) «Данные значения» – значения реестра. Чтобы настроить только раздел, следует оставить это поле пустым. В этом поле можно указать переменные. Данный параметр доступен только при выбранном действии «Создать», «Заменить» или «Обновить» и введенном значении «Имя значения».

Все настройки политики управления файлами хранятся в файлах:

```
{GUID GPT}/Machine/Registry/Registry.xml  
{GUID GPT}/User/Registry/Registry.xml
```

Пример файла Registry.xml:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<RegistrySettings clsid="{A3CCFC41-DFDB-43a5-8D26-0FE8B954DA51}">
  <Registry changed="2022-11-21 18:36:20"
    clsid="{9CD4B2F4-923D-47f5-A062-E897DD1DAD50}"
    image="12"
    name="failed_count"
    status="failed_count"
    uid="{D5855321-D2BA-4595-BD28-4DF452BFF65F}"
    bypassErrors="1">
    <Properties
      action="U"
      displayDecimal="0"
      hive="HKEY_CURRENT_USER"
      key="Software\Google\Chrome\BLBeacon"
      name="failed_count"
      type="REG_DWORD"
      value="00000001">
      <SubProp id="" mask="0" value="0"/>
    </Properties>
  </Registry>
</RegistrySettings>
```

10.4.6.5.9. Указание прокси-сервера

С помощью групповых политик можно указать прокси-сервер.

Примечание. Если прокси-сервер был настроен в модуле «Прокси-сервер» ЦУС, предварительно нужно удалить эти настройки и в файле /etc/sysconfig/network удалить строки:

```
HTTP_PROXY=
HTTPS_PROXY=
FTP_PROXY=
NO_PROXY=
```

Для настройки этой политики используется политика управления переменными среды (см. п. 10.4.6.5.4).

Настройка политики для указания прокси-сервера – настроить групповую политику управления переменными окружения (рис. 437):

- в поле «Действие» выбрать пункт «Заменить»;
- в поле «Имя» указать имя переменной: HTTPS_PROXY;
- в поле «Значение» указать адрес и порт прокси-сервера, также при необходимости аутентификационные данные, в формате http://username:password@address:port

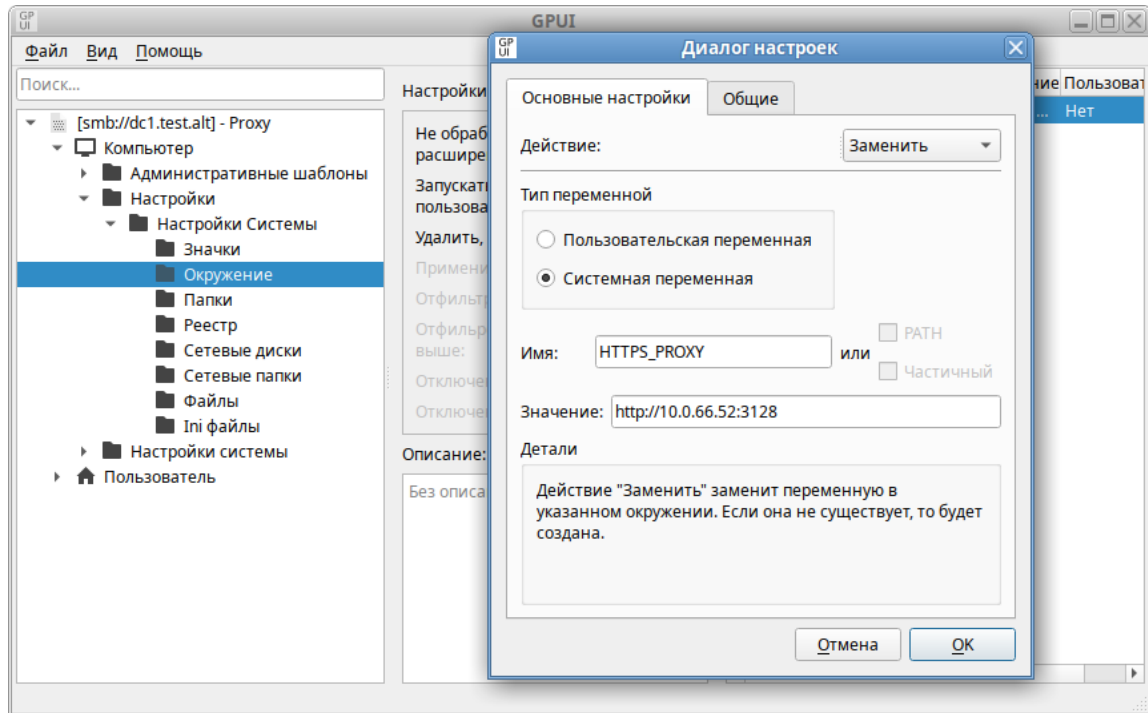


Рис. 437 – Настройка политики для указания прокси-сервера

Аналогичным способом создать настройки окружения для переменных HTTP_PROXY и FTP_PROXY (в поле «Имя» указывать соответственно HTTP_PROXY, FTP_PROXY).

Проверка применения политики:

- применить групповые политики на целевом компьютере, выполнив команду:

```
$ gpupdate
```

- повторно авторизоваться на целевом компьютере;

- проверить наличие переменных окружения, выполнив команду:

```
$ env |grep PROXY
HTTP_PROXY=http://10.0.66.52:3128
HTTPS_PROXY=http://10.0.66.52:3128
FTP_PROXY=http://10.0.66.52:3128
```

- запустить веб-браузер, убедиться, что сайты открываются через прокси-сервер.

10.4.6.5.10. Настройка периодичности запроса конфигураций

Для изменения периодичности запроса конфигураций можно создать файлы:

- /etc/systemd/user/gpupdate-user.timer.d/override.conf – изменение пользовательского таймера;

- /etc/systemd/system/gpupdate.timer.d/override.conf – изменение системного таймера.

С указанием периодичности запроса конфигураций, например:

```
[Timer]
OnUnitActiveSec = 10min
```

где 10min – периодичность запроса конфигураций.

Периодичность запроса конфигураций (запроса gpupdate) можно установить с помощью групповых политик.

Для настройки этой политики используются политика управления каталогами (см. п. 10.4.6.5.2) и политика управления INI-файлами (см. п. 10.4.6.5.3).

Настройка политики задания периодичности запроса конфигураций:

1) настроить групповую политику создания каталога (рис. 438):

- в поле «Действие» выбрать пункт «Создать»;
- в поле «Путь» указать /etc/systemd/system/gpupdate.timer.d;

2) настроить групповую политику создания INI-файла (рис. 439):

- в поле «Действие» выбрать пункт «Обновить»;
- в поле «Путь» к файлу указать /etc/systemd/system/gpupdate.timer.d/override.conf;
- в поле «Имя секции» указать «Timer»;
- в поле «Имя свойства» указать OnUnitActiveSec;
- в поле «Значение свойства» указать периодичность запроса, в данном примере 10 минут: 10min.

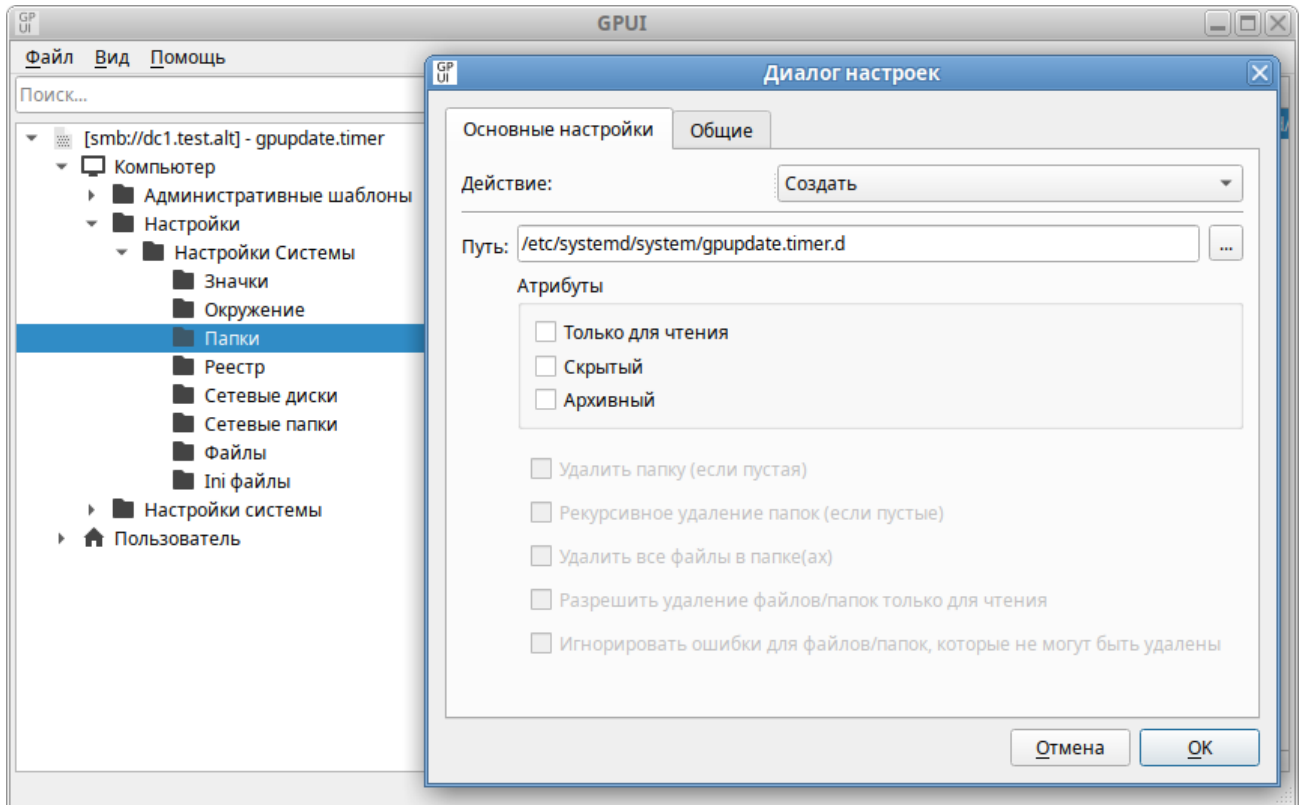


Рис. 438 – Создание каталога для настроек таймера

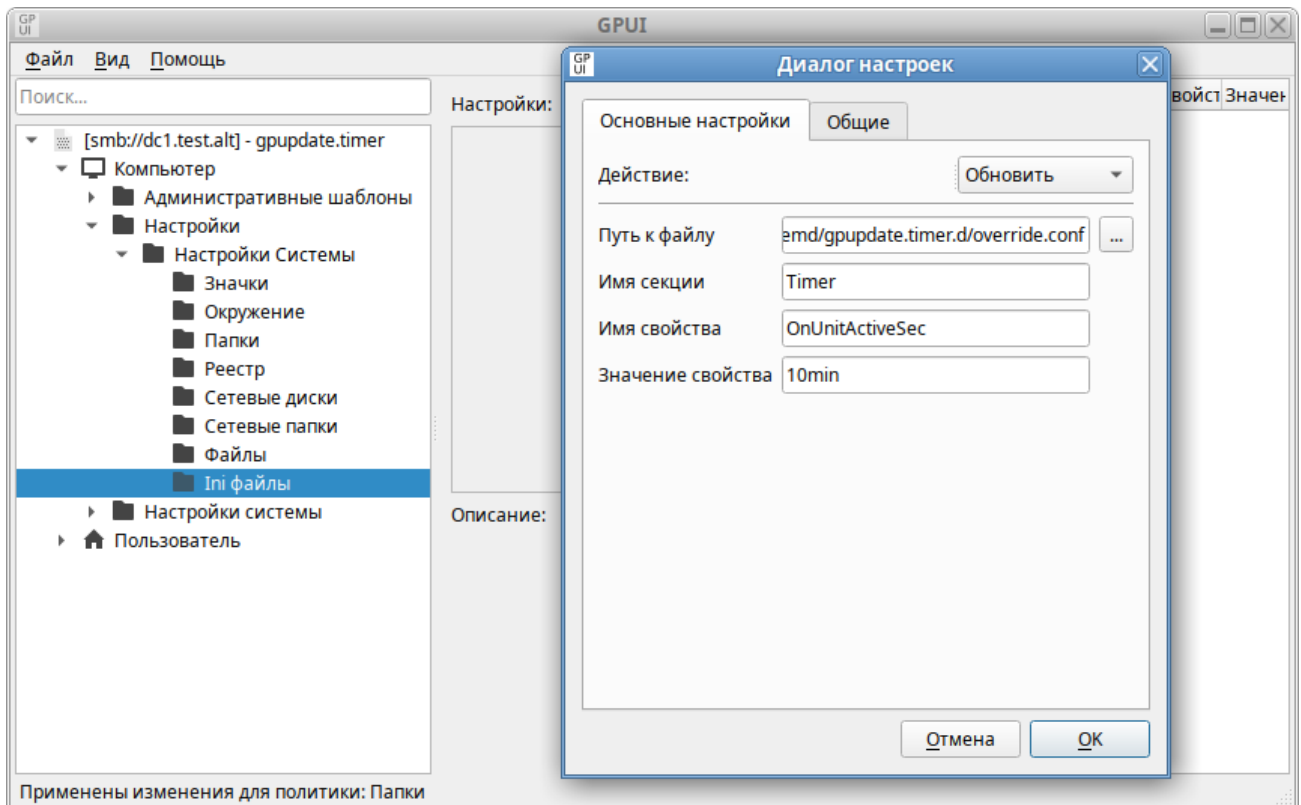


Рис. 439 – Настройка периодичности запроса конфигураций

Проверка применения политики:

- 1) применить групповые политики на целевом компьютере, выполнив команду:

```
$ gpupdate
```

- 2) выполнить команду (или перезагрузить компьютер):

```
# systemctl daemon-reload
```

- 3) убедиться, что политика применилась, выполнив команды:

```
$ cat /etc/systemd/system/gpupdate.timer.d/override.conf
```

```
[Timer]
```

```
OnUnitActiveSec = 10min
```

```
$ systemctl status gpupdate.timer
```

```
...
```

```
Active: active (waiting) since Mon 2024-06-10 16:29:23 EET; 44s ago
```

```
Trigger: Mon 2024-06-10 16:39:25 EET; 9min left
```

Примечание. Файл `override.conf` подменяет настройки системной библиотеки в файле `/lib/systemd/system/gpupdate.timer` только если значение секции `Timer` в файле `override.conf` меньше, чем значение аналогичной секции в `gpupdate.timer`.

Примечание. Применить пользовательские настройки можно, выполнив команду:

```
$ systemctl --user daemon-reload
```

10.4.6.6. Управление logon-скриптами

Групповые политики позволяют запускать сценарии запуска и завершения работы компьютера, входа и выхода из системы пользователя. Возможно связать один или несколько файлов сценариев (scripts) с четырьмя иницируемыми событиями:

- 1) для машины:

- запуск компьютера (Startup);
- выключение компьютера/завершение работы (Shutdown);

- 2) для пользователя:

- вход пользователя (Logon);
- выход пользователя (Logoff).

Система выполняет сценарии на языках, которые поддерживает клиентский компьютер. В среде Windows эту задачу выполняет Windows Script Host (WSH), который поддерживает языки сценариев, включая bat, cmd, VBScript и Jscript. В случае если указано более одного сценария, они будут выполняться согласно перечню в списке.

Примечание. В сценариях, запускаемых на машинах на базе ОС ALT, нужно в первой строке указывать шебанг, например, `#!/usr/bin/env bash`

Примечание. Если сценарии (scripts) хранятся в SYSVOL, они реплицируются между контроллерами домена. SYSVOL доступен всем членам домена, что гарантирует запуск сценария.

10.4.6.6.1. Сценарии для входа/выхода пользователя

Для удобства можно скопировать нужные сценарии в каталог User\Scripts\Logon (например, `\\test.alt\sysvol\test.alt\Policies\{20DDB816-421B-4861-8AC5-007E56CB67D0}\User\Scripts\Logon`) или User\Scripts\Logoff соответствующей политики.

Для настройки политики следует перейти в «Пользователь» → «Настройки системы» → «Скрипты». Щелкнуть левой кнопкой мыши на политике «Вход в систему» или «Выход из системы» (рис. 440).

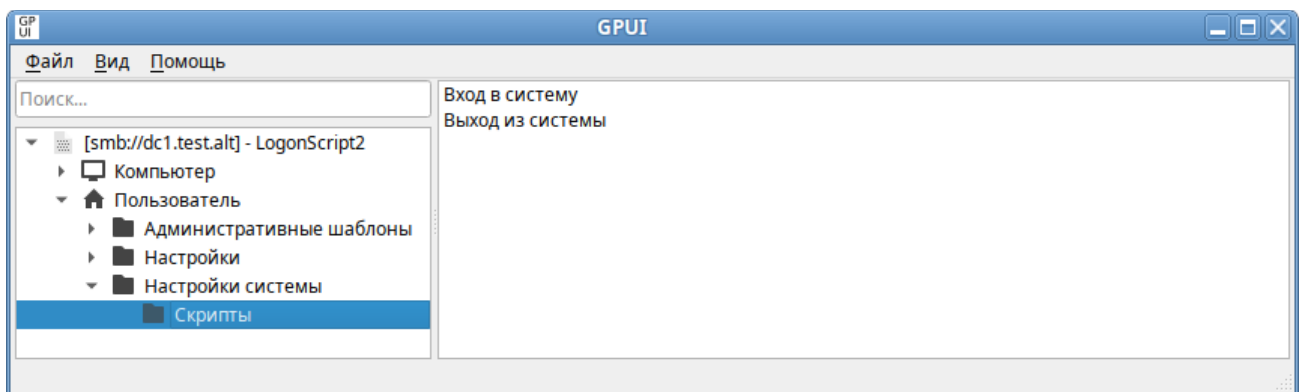


Рис. 440 – Политика «Вход в систему» или «Выход из системы»

В диалоговом окне свойств политики нажать кнопку «Добавить» (рис. 441).

В диалоговом окне «Добавить скрипт» в поле «Имя сценария» ввести путь к сценарию, в поле «Параметры сценария» ввести параметры аналогично вводу этих параметров в командной строке (рис. 442). Нажать кнопку «ОК».

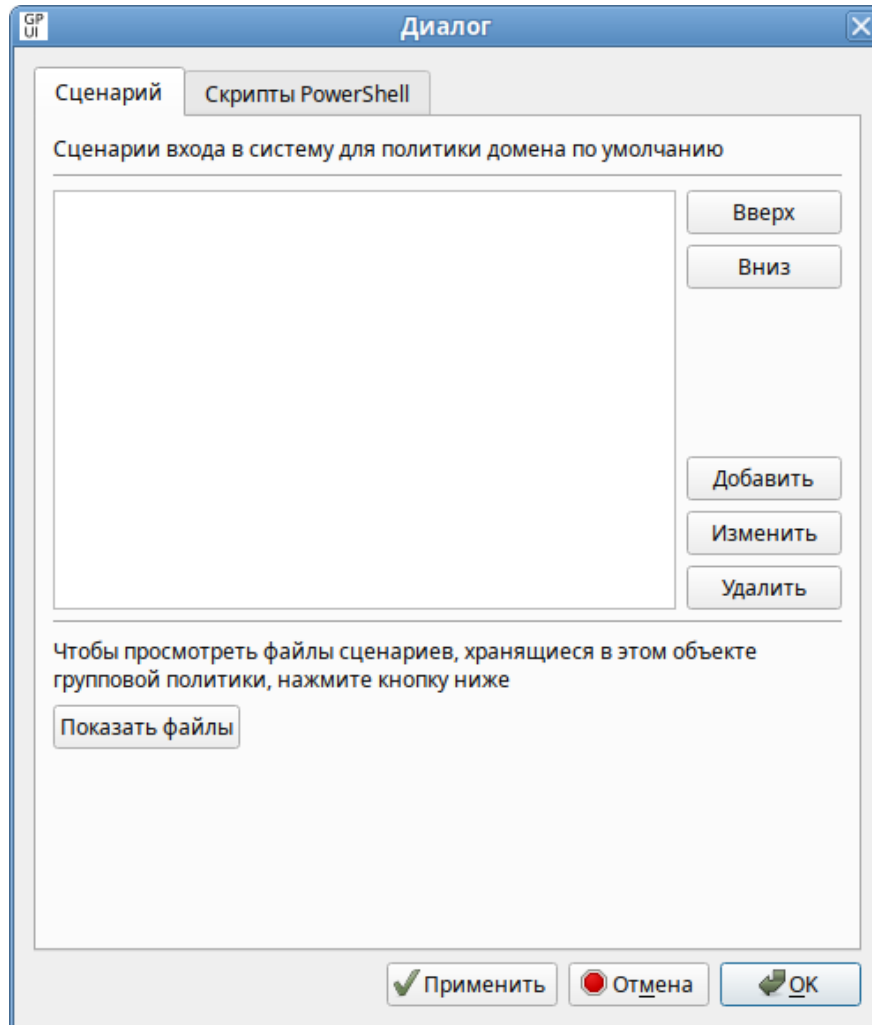


Рис. 441 – Диалоговое окно свойств политики «Вход в систему»

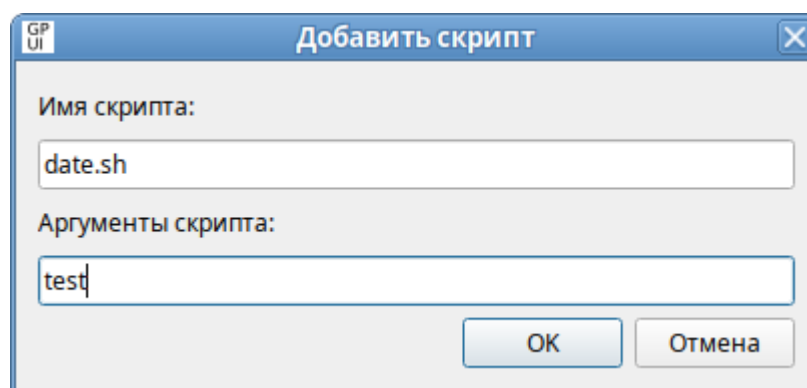


Рис. 442 – Пример добавления сценария для ОС Альт СП

Примечание. Применение локальных скриптов реализовано в механизме `groupdate` версии 0.9.11. В версиях ниже скрипты для ОС Альт СП должны находиться в GPT настраиваемого объекта групповой политики.

В сценариях для ОС Windows можно указать локальный скрипт на компьютере клиента (рис. 443).

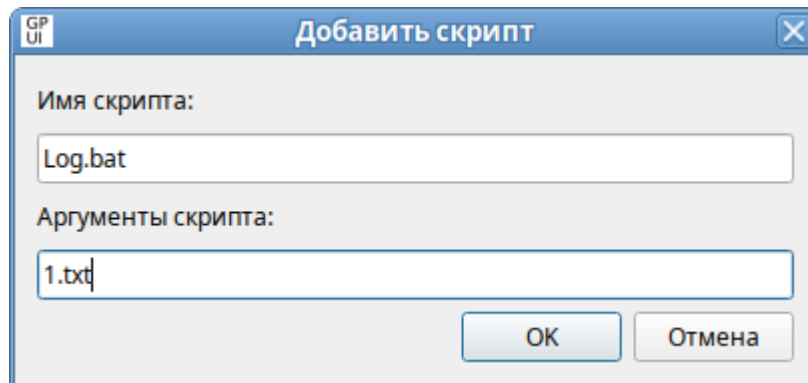


Рис. 443 – Пример добавления сценария для ОС Windows

При назначении нескольких сценариев они будут применяться в заданном порядке. Чтобы переместить сценарий в списке вверх/вниз, следует выбрать его в списке и нажать кнопку «Вверх»/«Вниз» (рис. 444).

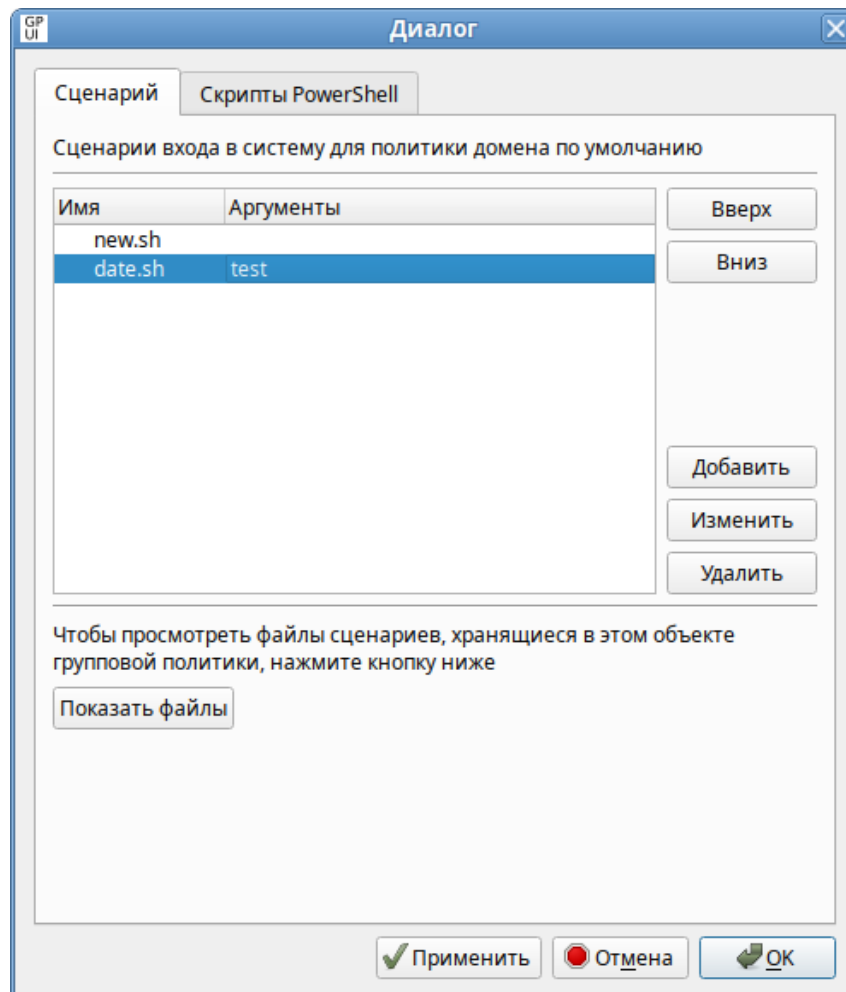


Рис. 444 – Список сценариев

Для того чтобы изменить параметры сценария, нужно выбрать его в списке и нажать кнопку «Изменить». Кнопка «Удалить» предназначена для удаления сценария из списка.

На вкладке «Скрипты PowerShell» можно добавить сценарии с расширением *.ps1.

10.4.6.6.2. Сценарии для автозагрузки или завершения работы компьютера

Для удобства можно скопировать нужные сценарии в каталог Machine\Scripts\Startup (например, \\test.alt\sysvol\test.alt\Policies\{20DDB816-421B-4861-8AC5-007E56CB67D0}\Machine\Scripts\Startup) или Machine\Scripts\Shutdown соответствующей политики.

Для настройки политики следует перейти в «Компьютер» → «Настройки системы» → «Скрипты». Щелкнуть левой кнопкой мыши на политике «Запуск» или «Завершение работы» (рис. 445).

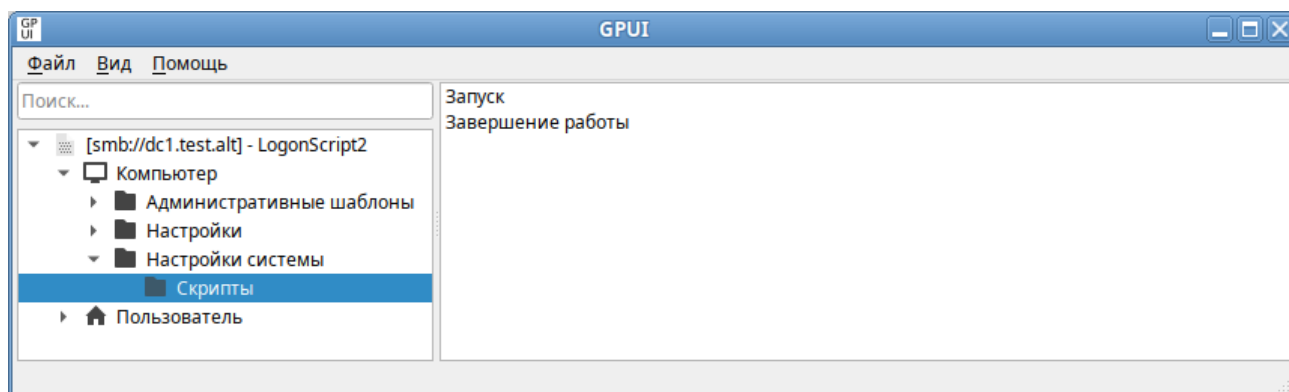


Рис. 445 – Сценарии для автозагрузки или завершения работы компьютера

В диалоговом окне свойств политики нажать кнопку «Добавить» (рис. 441).

В диалоговом окне «Добавить скрипт» в поле «Имя сценария» ввести путь к сценарию, в поле «Параметры сценария» ввести параметры аналогично вводу этих параметров в командной строке (рис. 442). Нажать кнопку «ОК».

Примечание. Применение локальных скриптов реализовано в механизме groupdate версии 0.9.11. В версиях ниже скрипты для ОС Альт СП должны находиться в GPT настраиваемого объекта групповой политики.

При назначении нескольких сценариев они будут применяться в заданном порядке. Чтобы переместить сценарий в списке вверх/вниз, следует выбрать его в

списке и нажать кнопку «Вверх»/«Вниз». Для того чтобы изменить параметры сценария, нужно выбрать его в списке и нажать кнопку «Изменить». Кнопка «Удалить» предназначена для удаления сценария из списка.

На вкладке «Скрипты PowerShell» можно добавить сценарии с расширением *.ps1.

10.4.6.6.3. Включение экспериментальных групповых политик

Политики управления logon-скриптами относятся к экспериментальным, поэтому на машинах с ОС Альт СП где они применяются должны быть включены экспериментальные групповые политики (подробнее см. п. 10.4.6.4.7).

Включить/отключить механизм групповых политик управления logon-скриптами также можно, включив/отключив политики «Модуль выполнения сценариев для компьютеров» или «Модуль выполнения сценариев для пользователей» («Компьютер» → «Административные шаблоны» → «Система ALT» → «Групповые политики» → «Механизмы GPOupdate») (рис. 446).

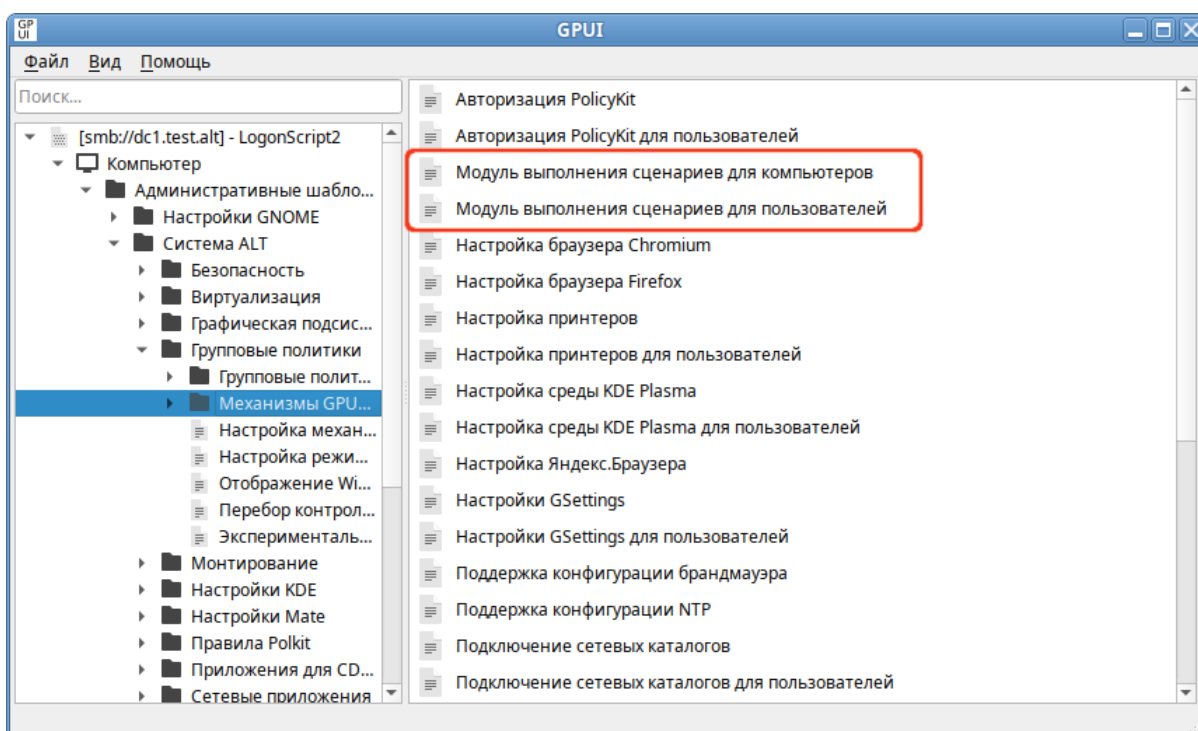


Рис. 446 – Механизмы GPOupdate управления logon-скриптами

10.4.6.6.4. Файлы настроек политики

Файлы сценариев входа и выхода пользователя (за исключением локальных) хранятся в каталогах: {GUID GPT}\User\Scripts\Logon и {GUID GPT}\User\Scripts\Logoff. Настройки политики для сценариев входа и выхода пользователя хранятся в файле {GUID GPT}\User\Scripts\scripts.ini.

В файле scripts.ini перечисляются все скрипты, выполняемые в сценариях входа и выхода пользователя из системы. Сценарии входа начинаются с преамбулы [Logon], сценарии выхода начинаются с преамбулы [Logoff].

Пример файла scripts.ini:

```
[Logon]
0CmdLine=date.sh
0Parameters=test
1CmdLine=test.sh
1Parameters=new
[Logoff]
0CmdLine=touch.sh
0Parameters=
1CmdLine=Logoff.bat
1Parameters=1.txt
2CmdLine=C:\share\Logon.bat
2Parameters=
```

Файлы сценариев запуска и завершения работы компьютера (за исключением локальных) хранятся в каталогах: {GUID GPT}\Machine\Scripts\Shutdown и {GUID GPT}\Machine\Scripts\Startup. Настройки политики для сценариев входа и выхода пользователя хранятся в файле {GUID GPT}\User\Scripts\scripts.ini.

В файле scripts.ini перечисляются все скрипты, выполняемые в сценариях запуска и завершения работы компьютера. Сценарии запуска компьютера начинаются с преамбулы [Startup], сценарии завершения работы начинаются с преамбулы [Shutdown].

Пример файла scripts.ini:

```
[Startup]
0CmdLine=hello.bat
0Parameters=
1CmdLine=notescript.vbs
1Parameters=
2CmdLine=notescript2.vbs
2Parameters=
3CmdLine=touch.bat
```



```
3Parameters=  
[Shutdown]  
0CmdLine=touch.bat  
0Parameters=
```

Файл `scripts.ini` закодирован в формате UTF-16LE (little-endian).

Настройки политики для скриптов PowerShell хранятся в файлах `{GUID GPT}/User/Scripts/pgscripts.ini` (для сценариев входа и выхода пользователя) и `{GUID GPT}/Machine/Scripts/pgscripts.ini` (для запуска и завершения работы компьютера).

10.4.7. Расширение возможностей ГП

10.4.7.1. Схема административных шаблонов ADMX

Административные шаблоны представляют собой два типа XML-файлов:

- независимый от языка файл (ADMX), описывающий структуру категорий и параметры политики административных шаблонов, отображаемых в редакторе управления групповыми политиками;
- набор зависящих от языка файлов (ADML), которые предоставляют локализованные части, отображаемые в редакторе управления групповыми политиками. Каждый ADML-файл представляет один язык, для которого требуется поддержка.

Каждому ADMX-файлу должен соответствовать свой ADML-файл с таким же именем.

10.4.7.1.1. Структура ADMX-файла

ADMX-файл состоит из семи разделов (рис. 447):

- XML-объявление – XML-объявлением является заголовок файла, который не рассматривается в качестве фрагмента ADMX-документа, но является его необходимой частью и помещается в начале файла для того, чтобы указать на то, что это XML-документ;
- `policyDefinitions` – элемент, который содержит все остальные элементы ADMX-файла;
- `policyNamespaces` – этот элемент определяет уникальное пространство имен для данного ADMX-файла. Данный элемент также обеспечивает

- сопоставление с пространствами имен во внешних файлах, если ADMX-файл ссылается на элементы `category`, определенные в другом ADMX-файле;
- `resources` – определяет требования к ресурсам определенного языка и минимальную необходимую версию связанного ADML-файла;
 - `supportedOn` – определяет ссылки на локализованные текстовые строки, определяющие ОС или приложения, на которые влияет определенный параметр политики;
 - `categories` – содержит список категорий, в которых параметр политики текущего ADMX-файла будет отображаться в редакторе объектов групповой политики;
 - `policies` – содержит определения отдельных параметров политики.

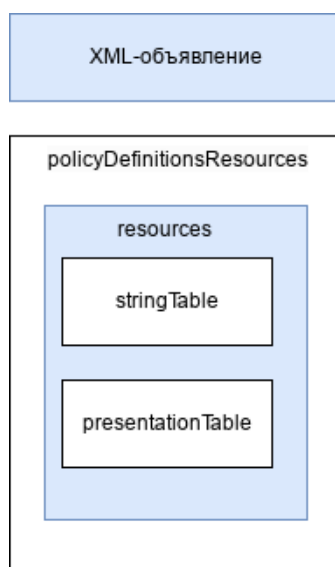


Рис. 447 – Структура ADMX-файла

XML-объявление не считается частью документа ADMX. Однако рекомендуется начинать файл ADMX с объявления XML.

Синтаксис XML-объявления:

```
<?xml version="<версия>" encoding="<кодировка"?">
```

где:

- `version` – версия XML, используемая в документе (обязательный атрибут).

В настоящее время поддерживается только версия 1.0;

- `encoding` – информация о кодировке символов, используемая анализаторами XML-документов. ADMX-файлы всегда имеют кодировку UTF-8.

Примечание. XML-объявление не должно предваряться комментариями, пробелами или другими инструкциями по обработке XML.

Элемент `policyDefinitions` – это элемент документа для ADMX-файла, который определяет набор параметров политики реестра. Элемент `policyDefinitions` также объявляет пространство имен по умолчанию для всех элементов в ADMX-файле.

Синтаксис элемента `policyDefinitions`:

```
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
revision="<MajorVersion.MinorVersion>"
schemaVersion="<MajorVersion.MinorVersion>"
xmlns="
http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinition
s" >
<policyNamespaces> ... </policyNamespaces>
<supersededAdm> ... </supersededAdm>
<resources> ... </resources>
<supportedOn> ... </supportedOn>
<categories> ... </categories>
<policies> ... </policies>
</policyDefinitions>
```

Атрибуты элемента `policyDefinitions` описаны в таблице 55.

Т а б л и ц а 55 – Атрибуты элемента `policyDefinitions`

Атрибут	Обязательный	Описание
<code>xmlns:xsd</code>	Нет	Обозначение элементов и типов данных, используемых в схеме пространства имен
<code>xmlns:xsi</code>	Нет	Обозначение пространства имен экземпляра XML-схемы, предоставленной в самом пространстве имен
<code>revision</code>	Да	Версия ADMX-файла, которая в большинстве случаев предназначена для отслеживания внесенных изменений. Синтаксис: <code>revision="<MajorVersion.MinorVersion>"</code> где <code>MajorVersion</code> и <code>MinorVersion</code> являются номерами версии, например, <code>revision="1.0"</code>
<code>schemaVersion</code>	Да	Указывает версию схемы, используемую средствами работы с ГП для определения того, поддерживается ли ими формат конкретных ADMX-файлов. Синтаксис этой команды идентичен синтаксису <code>revision</code>
<code>xmlns</code>	Нет	Пространство имен схемы ГП

Примечание. Инструменты ГП успешно используют файлы ADMX-файлы, которые не содержат атрибутов `xmlns`. Но эти атрибуты должны входить в состав ADMX-файла, так как, в противном случае, он может не пройти проверку на правильность формата XML-файла.

Дочерние элементы `policyDefinitions` описаны в таблице 56.

Т а б л и ц а 56 – Дочерние элементы `policyDefinitions`

Элемент	Обязательный	Описание
<code>policyNamespaces</code>	Да	<p>Определяет уникальное имя пространства имен политики в файле ADMX, а также любых пространств имен, на которые оно ссылается в других файлах ADMX.</p> <p>Синтаксис: <code><policyNamespaces></code> <code><target> ... </target></code> <code><using> ... </using></code> <code></policyNamespaces></code></p> <p>где</p> <ul style="list-style-type: none"> - <code>target</code> – определяет уникальное имя пространства имен политики в ADMX-файле (обязательный элемент); - <code>using</code> – ссылается на существующую категорию или имя <code>supportOn</code> из другого пространства имен политики
<code>supersededAdm</code>	Нет	<p>Данный элемент ссылается на имя ADM-файла, заменяемого ADMX-файлом</p>
<code>resources</code>	Да	<p>Определяет требования для ресурсов определенного языка и минимальную необходимую версию связанного ADML-файла.</p> <p>Синтаксис: <code><resources</code> <code>minRequiredRevision="<MajorVersion.MinorVersion>"</code> <code>fallbackCulture="<language name>"/></code></p> <p>где</p> <ul style="list-style-type: none"> - <code>minRequiredRevision</code> – минимальный уровень версии соответствующего ADML-файла; - <code>fallbackCulture</code> – язык, который будет использоваться, если ни в одном расположении не будет найден соответствующий ADML-файл. Если этот атрибут не указан будет использоваться английский язык
<code>supportedOn</code>	Нет	<p>Определяет сопоставление ссылки на локализованные строки текста с ОС или приложениями, на которые влияют конкретные параметры политики.</p> <p>Синтаксис: <code><supportedOn></code> <code><definitions> ... </definitions></code> <code></supportedOn></code></p> <p>Элементы <code>definitions</code> содержат информацию о поддерживаемой версии</p>

Окончание таблицы 56

Элемент	Обязательный	Описание
categories	Нет	Содержит список категорий, в которых параметр политики текущего ADMX-файла будет отображаться в редакторе управления групповыми политиками. Синтаксис: <categories> <category ... </category> </categories> Элемент category указывает имя уникальной категории, которая будет отображаться в редакторе объектов групповой политики
policies	Нет	Содержит список определений параметров политики. Синтаксис: <policies> <policy> ... </policy> </policies> Дочерний элемент policy соответствует одному параметру групповой политики, отображаемому в редакторе объектов групповой политики. Элемент policy описывает всю информацию о параметре политики, но включает ссылку на определение параметра

Синтаксис элемента category:

```
<category name="<logical or friendly name>"
  displayName="$ (string.<category text>)"
  explainText="$ (string.<help text>)"
  <parentCategory> ... </parentCategory>
  <seeAlso> ... </seeAlso>
  <keywords> ... </keywords>
</category>
```

Атрибуты элемента category описаны в таблице 57. Дочерние элементы category описаны в таблице 58.

Т а б л и ц а 57 – Атрибуты элемента category

Атрибут	Обязательный	Описание
name	Да	Имя, которое будет использоваться для конкретного поддерживаемого приложения и версии
displayName	Да	Ссылка на текстовую строку категории, расположенную в таблице строк ADML-файла
explainText	Нет	Текст объяснения или справки, связанный с конкретной категорией

Т а б л и ц а 58 – Дочерние элементы элемента category

Элемент	Обязательный	Описание
parentCategory	Да	Ссылка на родительскую категорию
seeAlso	Нет	Ссылка на другой элемент, который может быть связан с этим. Этот элемент не поддерживается и будет игнорироваться текущей ГП
keywords	Нет	Содержит индексные слова, которые можно использовать для поиска элементов. Этот элемент не поддерживается и будет игнорироваться текущей ГП

Синтаксис элемента policy:

```
<policy name="<logical or friendly name>"
class="Machine|User|Both"
displayName="$ (string.<category text>)"
explainText="$ (string.<help text>)"
presentation="$ (presentation.<parameter>)"
key="<registry key>"
valueName="<registry valuename>"
<parentCategory> ... </parentCategory>
<supportedOn> ... </supportedOn>
<enabledValue> ... </enabledValue>
<disabledValue> ... </disabledValue>
<enabledList> ... </enabledList>
<disabledList> ... </disabledList>
<elements> ... </elements>
</policy>
```

Атрибуты элемента policy описаны в таблице 59. Дочерние элементы policy описаны в таблице 60.

Т а б л и ц а 59 – Атрибуты элемента policy

Атрибут	Обязательный	Описание
name	Да	Уникальное имя элемента политики (строка без пробелов и специальных символов)
class	Да	Определяет, где в каком разделе редактора ГП будет размещен элемент политики: компьютере, пользователе или в обоих узлах. Может принимать значения: «User», «Machine» или «Both»
displayName	Да	Имя, отображаемое в GUI или оснастке консоли управления ГП. Ссылка на строку, расположенную в ADML-файле
explainText	Нет	Текст объяснения или справки, связанный с элементом политики. Ссылка на строку, расположенную в ADML-файле
presentation	Нет	Подписи параметров политики. Ссылка на строки, расположенные в ADML-файле
key	Да	Местоположение ключа реестра, в котором будет создан параметр реестра
valueName	Нет	Значение реестра, которое будет настроено для этого конкретного элемента политики

Т а б л и ц а 60 – Дочерние элементы элемента policy

Элемент	Обязательный	Описание
parentCategory	Да	Ссылка на родительскую категорию (раздел, в котором будет отображаться политика)
supportedOn	Нет	Логическое имя supportOn, определенное в элементе supportOn для этого файла (ссылка на поддерживаемые продукты)
enabledValue	Нет	Значение, которое раздел реестра примет, если политика включена. Синтаксис: <enabledValue> <delete /> <decimal> ... </decimal> <string> ... </string> </enabledValue> где: - delete – удалить значение или ключ реестра; - decimal – десятичное беззнаковое число; - string – строка, ограничена 255 символами
disabledValue	Нет	Значение, которое раздел реестра примет, если политика отключена. См. описание элемента enabledValue
enabledList	Нет	Набор значений и ключей реестра, представляющих включенное состояние элемента политики. Синтаксис: <enabledList defaultKey="<registry subkey>"> <item> ... </item> </enabledList> где: - атрибут defaultKey – подраздел реестра по умолчанию для всех элементов; - item – подраздел реестра со связанным значением
disabledList	Нет	Набор значений и ключей реестра, представляющих отключенное состояние элемента политики. См. описание элемента enabledList
elements	Нет	Один из пяти типов параметров (см.ниже), которые можно задать в настройке политики

Синтаксис элемента elements:

```
<elements>
<boolean> ... </boolean>
<decimal> ... </decimal>
<text> ... </text>
<enum> ... </enum>
<list> ... </list>
</elements>
```

Дочерние элементы elements описаны в таблице 61.

Т а б л и ц а 61 – Дочерние элементы elements

Элемент	Обязательный	Описание
boolean	Нет	<p>Представляет логический элемент в политике.</p> <p>Синтаксис:</p> <pre><boolean id="<ID>" clientExtension="<GUID>" key="<RegKey>" valueName="<Name>" <trueValue> ... </trueValue> <falseValue> ... </falseValue> <trueList> ... </trueList> <falseList> ... </falseList> </boolean></pre> <p>где:</p> <ul style="list-style-type: none"> - атрибут <code>id</code> – сопоставление с элементом (обязательный); - атрибут <code>clientExtension</code> – клиентское расширение, которое будет обрабатывать на клиентском компьютере конкретные настройки, представленные элементом; - атрибут <code>key</code> – местоположение ключа реестра, под которым будет создан параметр реестра; - атрибут <code>valueName</code> – значение реестра, которое будет настроено для этого конкретного элемента политики (обязательный); - <code>trueValue</code> – устанавливает значение на основе истинного условия; - <code>falseValue</code> – устанавливает значение на основе ложного условия; - <code>trueList</code> – устанавливает значения на основе истинного состояния; - <code>falseList</code> – устанавливает значения на основе ложного состояния. <p>Пример:</p> <pre><boolean id="OrgXfceThunar_blocker" key="Software\BaseALT\Policies\PolkitLocks" valueName="org.xfce.thunar"> <trueValue> <decimal value="1" /> </trueValue> <falseValue> <decimal value="0" /> </falseValue> </boolean></pre> <p>Для элемента <code>boolean</code> из ADMX-файла требуется элемент <code>checkbox</code> с соответствующим идентификатором в ADML-файле</p>
decimal	Нет	<p>Представляет числовой/десятичный элемент в политике. Число может быть определено для хранения в виде числового или строкового репрезентативного значения.</p> <p>Синтаксис:</p> <pre><decimal id="<ID>" clientExtension="<GUID>" key="<RegKey>" valueName="<Name>" required="true false" minValue="<MinValue>" maxValue="<MaxValue>"</pre>

Продолжение таблицы 61

Элемент	Обязательный	Описание
		<p>storeAsText="true false" soft="true false" /> где:</p> <ul style="list-style-type: none"> - атрибут id – сопоставление с элементом (обязательный); - атрибут clientExtension – клиентское расширение, которое будет обрабатывать на клиентском компьютере конкретные настройки, представленные элементом; - атрибут key – местоположение ключа реестра, под которым будет создан параметр реестра; - атрибут valueName – значение реестра, которое будет настроено для этого конкретного элемента политики (обязательный); - атрибут required – требует ввести значение в поле параметра; - атрибут minValue – минимально допустимое значение; - атрибут maxValue – максисмально допустимое значение; - атрибут soft – следует ли перезаписывать существующий подраздел; - атрибут storeAsText – если true, сохранить десятичное значение как значение реестра REG_SZ. <p>Пример: <decimal id="OrgMateSessionIdleDelay_setter" valueName="org.mate.session.idle-delay" minValue="1" maxValue="2147483647" /> Для элемента decimal требуется элемент decimalTextBox с соответствующим идентификатором в ADML-файле</p>
text	Нет	<p>Представляет текстовый элемент в политике. Синтаксис: <text id="<ID>" clientExtension="<GUID>" key="<RegKey>" valueBame="<Name>" required="true false" maxLength="<maxLength>" expandable="true false" soft="true false" / > где:</p> <ul style="list-style-type: none"> - атрибут id – сопоставление с элементом (обязательный); - атрибут clientExtension – клиентское расширение, которое будет обрабатывать на клиентском компьютере конкретные настройки, представленные элементом; - атрибут key – местоположение ключа реестра, под которым будет создан параметр реестра; - атрибут valueName – значение реестра, которое будет настроено для этого конкретного элемента политики (обязательный); - атрибут required – требует ввести значение в поле параметра; - атрибут maxLength – максисмально допустимое количество символов;

Продолжение таблицы 61

Элемент	Обязательный	Описание
		<p>- атрибут <code>expandable</code> – если <code>true</code>, значение подраздела реестра будет создано как расширяемый строковый тип (<code>REG_EXPAND_SZ</code>) вместо строкового типа (<code>REG_SZ</code>);</p> <p>- атрибут <code>soft</code> – следует ли перезаписывать существующий подраздел.</p> <p>Пример: <code><text id="OrgMateFilename_setter" valueName="org.mate.background.picture-filename" /></code> Элемент <code>text</code> допускает строковые значения длиной до 1023 символов. Для элемента <code>text</code> требуется соответствующий элемент <code>textBox</code> или <code>comboBox</code> с соответствующим идентификатором в ADML-файле</p>
enum	Нет	<p>Представляет элемент перечисления.</p> <p>Синтаксис: <code><enum id="<ID>" clientExtension="<GUID>" key="<RegKey>" valueName="<Name>" required="true false"></code> <code><item> ... </item></code> <code></enum></code></p> <p>где:</p> <ul style="list-style-type: none"> - атрибут <code>id</code> – сопоставление с элементом (обязательный); - атрибут <code>clientExtension</code> – клиентское расширение, которое будет обрабатывать на клиентском компьютере конкретные настройки, представленные элементом; - атрибут <code>key</code> – местоположение ключа реестра, под которым будет создан параметр реестра; - атрибут <code>valueName</code> – значение реестра, которое будет настроено для этого конкретного элемента политики (обязательный); - атрибут <code>required</code> – требует ввести значение в поле параметра; - <code>item</code> – представляет набор отображаемых имен с одним значением или набор значений подразделов реестра. синтаксис элемента <code>item</code>: <code><item displayName="\$(string.<placeholder for text>)"></code> <code><item> ... </item></code> <code></item></code> <ul style="list-style-type: none"> - где <code>displayName</code> – ссылка на отображаемую строку, расположенную в таблице строк ADML-файла. <p>Пример: <code><enum id="OrgMateColorShadingType_setter" required="true" valueName="org.mate.background.color-shading-type"></code> <code><item displayName="\$(string.org-mate-background-color-shading-type-horizontal-gradient)"></code> <code><value></code> <code><string>horizontal-gradient</string></code> <code></value></code> <code></item></code> <code><item displayName="\$(string.org-mate-background-color-shading-type-vertical-gradient)"></code> <code><value></code></p>

Окончание таблицы 61

Элемент	Обязательный	Описание
		<pre data-bbox="563 304 1433 600"><string>vertical-gradient</string> </value> </item> <item displayName="\$(string.org-mate-background-color- shading-type-solid)"> <value> <string>solid</string> </value> </item> </enum></pre> <p data-bbox="563 607 1398 674">Элемент <code>enum</code> обычно связан с элементом раскрывающегося списка в редакторе объектов групповой политики.</p> <p data-bbox="563 680 1321 748">Для элемента <code>enum</code> требуется элемент <code>dropdownList</code> с соответствующим идентификатором в ADML-файле</p>
list	Нет	<p data-bbox="563 757 1136 790">Представляет элемент списка в политике.</p> <p data-bbox="563 797 719 824">Синтаксис:</p> <pre data-bbox="563 831 1015 1066"><list id="<ID>" clientExtension="<GUID>" key="<RegKey>" valuePrefix="<Name>" additive="true false" expandable="true false" explicitValue="true false" > </ list></pre> <p data-bbox="563 1072 619 1099">где:</p> <ul data-bbox="584 1115 1477 1883" style="list-style-type: none"> - атрибут <code>id</code> – сопоставление с элементом (обязательный); - атрибут <code>clientExtension</code> – клиентское расширение, которое будет обрабатывать на клиентском компьютере конкретные настройки, представленные элементом; - атрибут <code>key</code> – местоположение ключа реестра, под которым будет создан параметр реестра; - атрибут <code>valuePrefix</code> – префикс, добавляемый к увеличенному целому числу, создает подраздел реестра, используемый при настройке значений политики (обязательный); - атрибут <code>additive</code> – если для этого параметра указано значение <code>true</code>, существующие подразделы не удаляются, а значения, установленные в списке, добавляются к существующим подразделам; - атрибут <code>explicitValue</code> – если для этого параметра указано значение <code>true</code>, пользователь должен указать значение подраздела реестра и имя подраздела реестра. В списке отображаются два столбца: один для имени и один для данных; - атрибут <code>expandable</code> – если <code>true</code>, значение подраздела реестра будет создано как расширяемый строковый тип (<code>REG_EXPAND_SZ</code>) вместо строкового типа (<code>REG_SZ</code>). <p data-bbox="563 1890 679 1917">Пример:</p> <pre data-bbox="563 1924 1334 2007"><list id="InstallPackagesList" key="Software\BaseALT\Policies\Packages\Install" additive="true"/></pre> <p data-bbox="563 2013 1289 2080">Для элемента <code>list</code> требуется элемент <code>listBox</code> с соответствующим идентификатором в ADML-файле</p>

Примечание. Если элемент `elements` определен, он должен содержать хотя бы один дочерний элемент. Количество и тип элементов, определенных в ADMX-файле, должны соответствовать элементам `presentation`, определенным в соответствующем ADML-файле.

10.4.7.1.2. Структура ADML-файла

ADML-файл состоит из пяти разделов (рис. 448):

- XML-объявление – XML-объявлением является заголовок файла, который не рассматривается в качестве фрагмента ADML-документа, но является его необходимой частью и помещается в начале файла для того, чтобы указать на то, что это XML-документ;
- `policyDefinitionResources` – элемент, который содержит все остальные элементы ADML-файла;
- `resources` – содержит элементы `stringTable` и `presentationTable` для указанного языка. Эти два элемента должны быть определены в ADML-файле в определенном порядке: элемент `stringTable`, за которым следует элемент `presentationTable`, как того требует схема ADMX;
- `stringTable` – используя этот элемент ADML-файла, можно указать заголовок параметра ГП, текст с описанием, текст со ссылкой на поддержку, названия категорий, а также подписи для параметров. Элемент `stringTable` нельзя объявлять более одного раза. Данный элемент включает в себя вложенные элементы `string`, позволяющие определить все указанные выше данные;
- `presentationTable` – представляет собой структуру дочерних элементов управления параметрами отдельных параметров ГП, включая всевозможные флаги, переключатели, подписи, подсказки и прочее. Дочерними элементами являются элементы `presentation`, которые представляют собой отображаемые сведения параметров для параметров политики.

Элемент `policyDefinitionResources` – это элемент документа для ADMX-файла, который определяет набор параметров политики реестра. Элемент `policyDefinitions` также объявляет пространство имен по умолчанию для всех элементов в ADMX-файле.

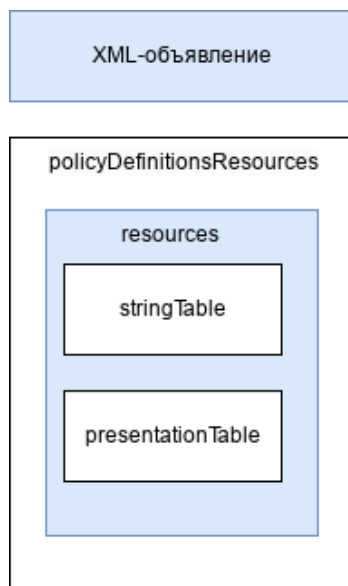


Рис. 448 – Структура ADML-файла

Синтаксис элемента `policyDefinitionResources`:

```

<policyDefinitionResources
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
revision="<MajorVersion.MinorVersion>"
schemaVersion="<MajorVersion.MinorVersion>"
xmlns="
http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinition
s" >
<displayName> ... </displayName>
<description> ... </description>
<annotation> ... </annotation>
<resources> ... </resources>
</policyDefinitionResources>
  
```

Дочерние элементы `policyDefinitionResources` описаны в таблице 62.

Атрибуты элемента `policyDefinitionResources` описаны в таблице 63.

Т а б л и ц а 62 – Дочерние элементы `policyDefinitionResources`

Элемент	Обязательный	Описание
<code>displayName</code>	Да	Название политики, содержащееся в ADML-файле
<code>description</code>	Нет	Описание параметров политики, содержащееся в ADML-файле
<code>annotation</code>	Да	Локализованный комментарий
<code>resources</code>	Нет	Содержит элементы <code>stringTable</code> и <code>presentationTable</code> для указанного языка.

Т а б л и ц а 63 – Атрибуты элемента `policyDefinitionResources`

Атрибут	Обязательный	Описание
<code>xmlns:xsd</code>	Нет	Обозначение элементов и типов данных, используемых в схеме пространства имен
<code>xmlns:xsi</code>	Нет	Обозначение пространства имен экземпляра XML-схемы, предоставленной в самом пространстве имен
<code>revision</code>	Да	Версия ADMX-файла. Синтаксис: <code>revision="<MajorVersion.MinorVersion>"</code> где <code>MajorVersion</code> и <code>MinorVersion</code> являются номерами версии, например, <code>revision="1.0"</code>
<code>schemaVersion</code>	Да	Указывает версию схемы, используемую средствами работы с ГП для определения того, поддерживается ли ими формат конкретных ADMX-файлов. Синтаксис этой команды идентичен синтаксису <code>revision</code>
<code>xmlns</code>	Нет	Пространство имен схемы ГП

Синтаксис элемента `resources`:

```
<resources>
<stringTable> ... </stringTable>
<presentationTable> ... </presentationTable>
</resources>
```

Дочерние элементы `resources` описаны в таблице 64.

Т а б л и ц а 64 – Дочерние элементы `resources`

Элемент	Обязательный	Описание
<code>stringTable</code>	Нет	Содержит отображаемые строки для следующих видов информации: <ul style="list-style-type: none"> - заголовок параметра групповой политики; - описание групповой политики; - определения поддерживаемых продуктов (<code>SupportedOn</code>); - названия категорий и описание категории; - подписи для параметров. Синтаксис: <pre><stringTable> <string> ... </string> </stringTable></pre> Элемент <code>stringTable</code> нельзя объявлять более одного раза.
<code>presentationTable</code>	Нет	Таблица элементов представления, представляющая структуру элементов управления параметрами для отдельных параметров групповой политики. Расположение элементов управления параметрами включает в себя: тип элемента ввода параметров (поле редактирования, ползунок, выпадающий список, флаги, переключатели); подписи и текст подсказки для ввода параметров; а также значения по умолчанию и диапазон возможных значений для каждого параметра. Синтаксис: <pre><presentationTable> <presentation> ... </presentation> </presentationTable></pre> Если в ADML-файле нет элементов представления, элемент <code>PresentationTable</code> можно опустить.

Окончание таблицы 64

Элемент	Обязательный	Описание
		Если элемент PresentationTable включен в ADML-файл, необходимо определить хотя бы один элемент представления. Элемент PresentationTable определяется в ADML-файле не более одного раза.

Синтаксис элемента presentation:

```
<presentation id="<logical or friendly name">
<text> ... </text>
<decimalTextBox> ... </decimalTextBox>
<textBox> ... </textBox>
<checkBox> ... </checkBox>
<comboBox> ... </comboBox>
<dropdownList> ... </dropdownList>
<listBox> ... </listBox>
</presentation>
```


Атрибут элемента presentation описаны в таблице 65.

Дочерние элементы presentation описаны в таблице 66.

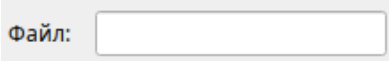
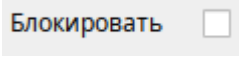
Т а б л и ц а 65 – Атрибут элемента presentation

Атрибут	Обязательный	Описание
id	Да	Указывает логическое имя при ссылке на информацию о представлении для определенного параметра политики

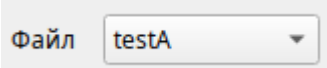
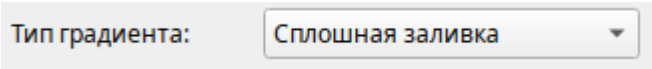
Т а б л и ц а 66 – Дочерние элементы resources

Элемент	Обязательный	Описание
text	Да	Локализованная строка. Используется для определения текста, расположенного выше и ниже поля ввода параметра. Синтаксис: <text>Локализованная строка</text>
decimalTextBox	Нет	Текстовое поле с элементом управления прокруткой или без него для ввода десятичных чисел в качестве параметра настройки политики. Должен быть связан с элементом decimal, определенным в элементе elements. Синтаксис: <decimalTextBox refId="Sample_NumericTextLabel">Метка</decimalTextBo x> где: - атрибут refId – сопоставление с элементом. Пример: <decimalTextBox refId="OrgMateScreensaverLockDelay_setter"defaultVal ue="3">Скорость повтора</decimalTextBox> 

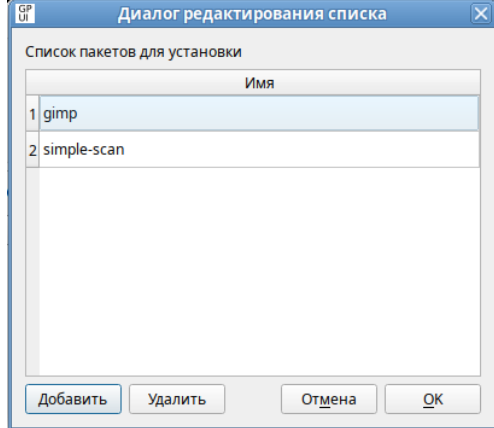
Продолжение таблицы 66

Элемент	Обязательный	Описание
textBox	Нет	<p>Текстовое поле. Этот элемент должен быть связан с элементом text, определенным в elements.</p> <p>Синтаксис: <code><textBox refId="<ID>"></code> <code><label> ... </label></code> <code><defaultValue> ... </defaultValue></code> <code></textBox></code></p> <p>где:</p> <ul style="list-style-type: none"> - атрибут refId – сопоставление с элементом; - label – подпись для параметра текстового поля (обязательный); - defaultValue – строка, по умолчанию отображаемая в текстовом поле. <p>Пример: <code><textBox refId="OrgMateFilename_setter"></code> <code><label>Файл:</label></code> <code></textBox></code></p> 
checkBox	Нет	<p>Элемент флага. Должен быть связан с элементом boolean, определенным в элементе elements.</p> <p>Синтаксис: <code><checkBox refId="<ID></code> <code>defaultChecked="true false"></code> Label: <code></checkBox></code></p> <p>где:</p> <ul style="list-style-type: none"> - атрибут refId – сопоставление с элементом (обязательный); - атрибут defaultChecked – значение по умолчанию. Если не указано, атрибуту defaultChecked будет присвоено значение false. <p>Пример: <code><checkBox refId="OrgXfceThunar_blocker"></code> Блокировать</checkBox></p> 
comboBox	Нет	<p>Поле со списком со значениями по умолчанию или предлагаемыми записями. Должно быть связано с элементом text, определенным в элементе elements.</p> <p>Синтаксис: <code><comboBox refId="<ID></code> <code>noSort="true false"></code> <code><label> ... </label></code> <code><default> ... </default></code> <code><suggestion> ... </suggestion></code> <code></comboBox></code></p> <p>где:</p> <ul style="list-style-type: none"> - атрибут refId – сопоставление с элементом (обязательный);

Продолжение таблицы 66

Элемент	Обязательный	Описание
		<p>- атрибут <code>noSort</code> – если <code>true</code>, отображать предлагаемые значения в определенном порядке элементов предложения; в противном случае отсортировать предлагаемые значения в алфавитном порядке. Если не указано, атрибуту <code>noSort</code> будет присвоено значение <code>false</code>;</p> <p>- <code>label</code> – подпись для параметра (обязательный);</p> <p>- <code>default</code> – строка, по умолчанию отображаемая в параметре;</p> <p>- <code>suggestion</code> – строка раскрывающегося списка.</p> <p>Пример:</p> <pre><comboBox refId="OrgMateFilename_setter"> <label>Файл</label> <default>None</default> <suggestion>testA</suggestion> <suggestion>testB</suggestion> <suggestion>testC</suggestion> </comboBox></pre> 
dropdownList	Нет	<p>Раскрывающийся список, с помощью которого пользователь может выбрать одну из отображаемых записей. Должен быть связан с элементом <code>enum</code>, определенным в элементе <code>elements</code>.</p> <p>Синтаксис:</p> <pre><dropdownList refId="<ID>" noSort="true false"> defaultItem="<NumericValue>" Placeholder label: </dropdownList></pre> <p>где:</p> <ul style="list-style-type: none"> - атрибут <code>refId</code> – сопоставление с элементом (обязательный); - атрибут <code>noSort</code> – если <code>true</code>, создать элемент <code>spin</code>; в противном случае создать текстовое поле для ввода чисел. Если не указано, атрибуту <code>noSort</code> будет присвоено значение <code>true</code>; - атрибут <code>defaultItem</code> – числовое значение, определяющее выбор из списка элементов по умолчанию. Список элементов нумеруется, начиная с 0. <p>Пример:</p> <pre><dropdownList noSort="true" defaultItem="0" refId="OrgMateColorShadingType_setter">Тип градиента:</dropdownList></pre> 
listBox	Нет	<p>Представляет параметр списка с кнопками «Добавить» и «Удалить». Это единственный параметр, который можно использовать для управления несколькими значениями под одним ключом. Должен быть связан с элементом <code>list</code>, определенным в элементе <code>elements</code>.</p> <p>Синтаксис:</p> <pre><listBox refId="ID">Описание:</listBox></pre> <p>где:</p> <ul style="list-style-type: none"> - атрибут <code>refId</code> – сопоставление с элементом.

Окончание таблицы 66

Элемент	Обязательный	Описание
		<p>Пример:</p> <pre data-bbox="566 336 1452 392"><listBox refId="InstallPackagesList">Список пакетов для установки</listBox></pre> 

Дочерние элементы, указанные в элементе `presentation`, должны соответствовать элементам, определенным в элементе `elements` ADMX-файла.

10.4.7.2. Связывание информации из ADMX и ADML-файлов

В синтаксисе ADMX, элементы, управляющие представлением или локализованным отображением параметра, определяются в ADML-файле. Информация же, определяющая тип данных и значение параметра, задается в ADMX-файле. Различные элементы из этих двух файлов используются для создания определений параметров для настроек политики.

Ниже рассмотрен пример использования двух параметров `checkbox` для настройки одной политики.

Фрагмент XML из файла `example.admx` с элементом `policy`, который содержит два элемента флага (`checkbox`):

```
<policy name="Sample_Checkbox" class="User"
  displayName="$ (string.Sample_Checkbox) "
  explainText="$ (string.Sample_Checkbox_Help) "
  presentation="$ (presentation.Sample_Checkbox) "
  key="Software\BaseALT\Policies\gsettings">
  <parentCategory ref="system:ALT_Background_Mate" />
  <supportedOn ref="system:SUPPORTED_AltP9" />
  <elements>
    <boolean id="Checkbox_1" valueName="ExampleCheckbox1">
      <trueValue>
        <decimal value="1" />
      </trueValue>
```

```

    <falseValue>
      <decimal value="0" />
    </falseValue>
  </boolean>

  <boolean id="Checkbox_2" valueName="ExampleCheckbox2">
    <trueValue>
      <decimal value="0" />
    </trueValue>
    <falseValue>
      <decimal value="1" />
    </falseValue>
  </boolean>
</elements>
</policy>

```

Фрагмент XML из файла `example.admx` с элементом `policy`, который содержит два элемента флага (`checkbox`):

```

<presentation id="Sample_Checkbox">
  <checkbox refId="Checkbox_1">Первый параметр</checkbox>
  <checkbox refId="Checkbox_2" defaultChecked="true">Второй
параметр - отмечен по умолчанию</checkbox>
</presentation>

```

Примечание. Каждому ADMX-файлу должен соответствовать ADML-файл с тем же именем. Редактор объектов групповой политики отобразит сообщение об ошибке, если не сможет найти соответствующий ADML-файл для каждого прочитанного ADMX-файла.

Есть две области координации между файлами ADMX и ADML:

- 1) ссылка верхнего уровня между установкой политики и отображением ее параметров. Политика, определяемая с помощью элемента `policy` в ADMX-файле, ссылается на определенный элемент `presentation` в ADML-файле через атрибут `presentation` элемента `policy`. В данном примере атрибут `presentation` определен как `presentation="$ (presentation.Sample_Checkbox) "`. Текст `presentation.Sample_Checkbox` сообщает редактору объектов групповой политики сослаться на элемент `presentationTable` ADML-файла, используя атрибут `id`, для которого установлено значение `Sample_Checkbox`.

Количество типов данных, а также тип данных (`boolean`, `decimal`, `text`, `enum`, `item` и `list`), определенные в элементе `elements` в ADMX-файле,

должны соответствовать количеству и типу параметров, определенных в ADML-файле в элементе `presentation` (`checkbox`, `textBox`, `decimalTextBox`, `comboBox`, `dropdownList` и `listBox`);

- 2) ссылка между представлением типа данных в элементе `elements` и определением параметра в элементе `presentation`.

В примере выше элемент `elements` содержит два элемента `boolean`:

```
<elements>
<boolean id="Checkbox_1" valueName="ExampleCheckbox1">
...
</boolean>

<boolean id="Checkbox_2" valueName="ExampleCheckbox2">
...
</boolean>
</elements>
```

Элемент `presentation` содержит два элемента `checkbox`:

```
<presentation id="Sample_Checkbox">
<checkbox refId="Checkbox_1">...</checkbox>
<checkbox refId="Checkbox_2" defaultChecked="true">...</checkbox>
</presentation>
```

Атрибут `id` элемента `boolean` используется для соответствия связанному элементу `checkbox`, на который ссылается атрибут `refId`.

10.4.7.3. Рекомендации для создания ADMX-файлов

При создании ADMX-файлов следует придерживаться следующих рекомендаций:

- 1) чтобы избежать отображения повторяющихся узлов в редакторе объектов групповой политики, не следует использовать название категории, которое было ранее определено в родительской категории. Например, создание двух ADMX-файлов с одинаковой категорией приведет к тому, что редактор объектов групповой политики создаст два узла с одинаковым именем. Вместо этого следует создать собственный базовый файл (см. ниже), на который будут ссылаться все разрабатываемые ADMX-файлы;
- 2) чтобы избежать циклических ссылок, один ADMX-файл не должен ссылаться на элементы категории другого ADMX-файла. Вместо этого

базовую категорию компонента следует поместить в отдельный базовый файл;

- 3) каждое пространство имен политики для ADMX-файла должно быть уникальным. Пространство имен политики определяется в целевом элементе ADMX-файла.

Пример создания пользовательского базового файла:

- 1) создать ADMX-файл MyCompany.admx с определением категории MyCompany:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
revision="1.0" schemaVersion="1.0"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions">
<policyNamespaces>
<target prefix="mycompany"
namespace="MyCompany.Policies.MyCompany" />
</policyNamespaces>
<resources minRequiredRevision="1.0" />
<categories>
<category name="MyCompany"
displayName="$ (string.MyCompany) "
explainText="$ (string.MyCompany_Help) " />
</categories>
</policyDefinitions>
```

- 2) создать ADML-файл ru-RU/MyCompany.adml, который будет содержать локализованное название категории:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
revision="1.0" schemaVersion="1.0"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions">
<displayName>Определение базовой категории</displayName>
<description>Этот файл содержит определение базовой категории организации.
</description>
<resources>
<stringTable>
<string id="MyCompany">Моя организация</string>
<string id="MyCompany_Help">Содержит параметры конфигурации, специфичные для организации.</string>
</stringTable>
</resources>
</policyDefinitionResources>
```

Чтобы обратиться к базовому файлу `MyCompany`, следует включить атрибут `using` в элемент `policyNamespaces`. Атрибут пространства имен должен соответствовать пространству имен, определенному в пользовательском базовом файле (в примере `MyCompany.Policies.MyCompany`). Атрибутом префикса может быть любое имя, уникальное для ADMX-файла. Рекомендуется по возможности использовать строку атрибута префикса из пользовательского базового файла, чтобы избежать путаницы. Например, следующий фрагмент файла `example.admx` определяет пространство имен и ссылается на базовый файл `MyCompany` в элементе `policyNamespaces`:

```
<policyNamespaces>
<target prefix="example" namespace="MyCompany.Policies.Example"
/>
<using namespace="MyCompany.Policies.MyCompany" prefix="mycompany" />
</policyNamespaces>
```

10.4.7.4. Разработка новой политики

Программа `grpupdate` состоит из ряда механизмов, позволяющих обращаться к настройкам ОС Альт СП. Механизмы обращаются к интерфейсам системы или отдельных приложений через API. Через систему механизмов `grpupdate` пользователю доступно создание собственных ГП так, чтобы не менять содержимое пакетов `admx` и `grpupdate`. В этом случае при очередном обновлении пакетов в системе не нарушится работа ГП – базовых и собственных. Появляется возможность создать свой набор политик, необходимый для внутреннего использования.

Механизмы применения параметров, которые позволяют создавать собственные политики:

- `Systemd`. Управление запуском служб `Systemd`;
- `Polkit`. Механизм `Polkit` отвечает за безопасность и правяет разрешениями при обращении к системным процессам;
- `Gsettings`. Управление настройками системной базы реестра `dconf`;
- `Control`. Механизм `Control` управляет состоянием конфигурационных файлов;
- скрипты загрузки системы и авторизации пользователя (`logon/logoff/startup/shutdown`).

Примечание. Скрипты загрузки системы и авторизации пользователя (Logon/logoff/startup/shutdown) не связаны с подготовкой ADMX-файлов и формируются через раздел настроек системы.

Шаги создания новой политики:

- 1) подобрать механизм реализации политики – systemd, control, gsettings, polkit;
- 2) загрузить шаблоны ADMX-файлов для выбранного механизма;
- 3) описать в ADMX-файлах (admx + adml) структуру новой политики и ее описание на русском или английском языке;
- 4) проверить корректность кода в ADMX-файлах, открыв редактор групповых политик – GPUI в ОС Альт СП или RSAT в Windows;
- 5) загрузить собственный набор административных шаблонов групповых политик (admx) на контроллер домена в каталог Sysvol.

10.4.7.4.1. Пример для механизма Systemd

Подсистема инициализации и управления службами Systemd в ГП «Альт» может запускать или останавливать службы. Systemd позволяет задавать расписание запуска служб, выполнять монтирование и многое другое. Через ГП «Альт» возможно управление самостоятельно созданной пользовательской службой.

Примечание. Просмотреть список загруженных служб можно, выполнив команду:

```
$ systemctl list-units --type service --all
```

Получить список всех установленных файлов модулей можно, выполнив команду:

```
$ systemctl list-unit-files
```

Пример создания новой политики для веб-сервера Apache (служба httpd2):

- 1) создать файл MySystemd.admx:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
revision="1.0"
schemaVersion="1.0"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDef
initions">
<policyNamespaces>
<target                                prefix="systemdunits"
namespace="BaseALT.Policies.MySystemdUnits" />
<using prefix="system" namespace="BaseALT.Policies.System" />
```

```

</policyNamespaces>
<resources minRequiredRevision="1.0" />
<policies>
<policy class="Machine" displayName="$(string.httpd2_service)"
explainText="$(string.httpd2_service_help)"
key="Software\BaseALT\Policies\SystemdUnits"
valueName="httpd2.service" name="httpd2.service">
<parentCategory ref="system:ALT_Systemd"/>
<supportedOn ref="system:SUPPORTED_AltP9"/>
<enabledValue>
<decimal value="1"/>
</enabledValue>
<disabledValue>
<decimal value="0"/>
</disabledValue>
</policy>
</policies>
</policyDefinitions>

```

2) создать файл ru-RU/MySystemd.adml:

```

<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDef
initions"
revision="1.0" schemaVersion="1.0">
<displayName>Определения служб</displayName>
<description>Этот файл содержит дополнительные определения
systemd-служб</description>
<resources>
<stringTable>
<string id="httpd2_service">Веб-сервер Apache</string>
<string id="httpd2_service_help">Эта политика определяет, включен
ли systemd юнит веб-сервера Apache.
</string>
</stringTable>
</resources>
</policyDefinitionResources>

```

3) создать файл en-US/MySystemd.adml:

```

<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDef
initions"
revision="1.0" schemaVersion="1.0">
<displayName>Services definitions</displayName>
<description>This file contains the systemd services
definitions</description>
<resources>

```



```

<stringTable>
<string id="httpd2_service">Apache Web Server</string>
<string id="httpd2_service_help">This policy determines whether
the systemd unit of Apache Web Server is enabled.
</string>
</stringTable>
</resources>
</policyDefinitionResources>

```

4) скопировать обновленные файлы admx/adml на машину с Windows RSAT или GPOI.

В Windows RSAT:

- файл MySystemd.admx В каталог

\\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions;

- файл ru-RU/MySystemd.adml В каталог

\\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions\ru-RU;

- файл en-US/MySystemd.adml В каталог

\\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions\en-US;

- Windows RSAT автоматически проверит корректность этих файлов.

В GPOI:

- файл MySystemd.admx В каталог /usr/share/PolicyDefinitions;

- файл ru-RU/MySystemd.adml В каталог

/usr/share/PolicyDefinitions/ru-RU;

- файл en-US/MySystemd.adml В каталог

/usr/share/PolicyDefinitions/en-US;

5) проверить корректность кода, открыв редактор групповых политик – GPOI в ОС Альт СП (рис. 449) или RSAT в Windows;

6) если все корректно, скопировать обновленные файлы admx/adml на контроллер домена в сетевой каталог sysvol (/var/lib/samba/sysvol/<DOMAIN>/Policies/).

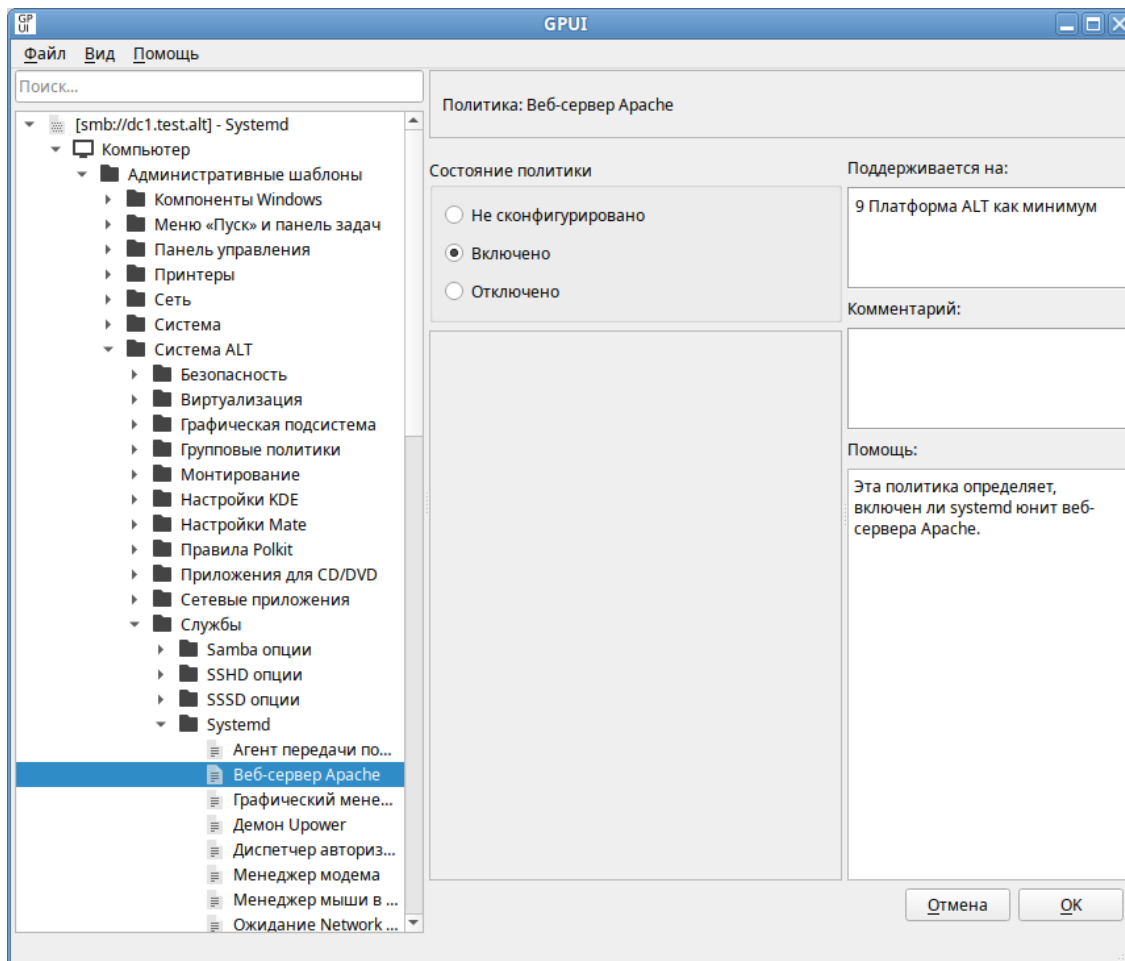


Рис. 449 – Проверка новой политики Systemd в GPUI

10.4.7.4.2. Пример для механизма Control

Подсистема Control в Linux-дистрибутивах является интерфейсом управления конфигурацией системы. Возможно написание собственных Control-интерфейсов для изменения системных или прикладных настроек, управляемых в дальнейшем через групповые политики.

Примечание. Просмотреть список опций Control можно, выполнив команду:

```
# control
```

Ниже рассмотрен пример создания admx для Control osec-send:

```
# control osec-send help
```

```
mail: Mail root
```

```
journal: Write to systemd journal
```

Пример создания новой политики для Control osec-send:

1) создать файл MyControl.admx:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
revision="1.0" schemaVersion="1.0"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDef
initions">
<policyNamespaces>
<target prefix="control" namespace="BaseALT.Policies.MyControl"
/>
<using prefix="system" namespace="BaseALT.Policies.System" />
</policyNamespaces>
<resources minRequiredRevision="1.0" />
<policies>
<policy class="Machine" displayName="$(string.osec-send)"
explainText="$(string.osec-send_help)"
key="Software\BaseALT\Policies\Control"
name="osec-send" presentation="$(presentation.osec-send)">
<parentCategory ref="system:ALT_Services"/>
<supportedOn ref="system:SUPPORTED_AltP9"/>
<elements>
<enum id="osec-send_setter" required="true" valueName="osec-
send">
<item displayName="$(string.osec-send_mail)">
<value>
<string>mail</string>
</value>
</item>
<item displayName="$(string.osec-send_journal)">
<value>
<string>journal</string>
</value>
</item>
</enum>
</elements>
</policy>
</policies>
</policyDefinitions>
```

2) создать файл ru-RU/MyControl.adml:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDef
initions"
revision="1.0" schemaVersion="1.0">
<displayName>Определения политик управления системными
компонентами</displayName>
```

ЛКНВ.11100-01 90 03

```
<description>Этот файл содержит определения политик управления
системными компонентами.</description>
```

```
<resources>
```

```
<stringTable>
```

```
<string id="osec-send">Отчет подсистемы osec</string>
```

```
<string id="osec-send_help">Политика позволяет определить куда
отправлять ежедневный отчет:
```

```
Почта - отправлять отчет на почтовый ящик пользователя root
```

```
Журнал - записывать отчет в системный журнал
```

```
</string>
```

```
<string id="osec-send_mail">Почта</string>
```

```
<string id="osec-send_journal">Журнал</string>
```

```
</stringTable>
```

```
<presentationTable>
```

```
<presentation id="osec-send">
```

```
<dropdownList noSort="true" defaultItem="0" refId="osec-
send_setter">Куда отправлять отчет:
```

```
</dropdownList>
```

```
</presentation>
```

```
</presentationTable>
```

```
</resources>
```

```
</policyDefinitionResources>
```

3) создать файл en-US/MyControl.adml:

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<policyDefinitionResources
```

```
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
```

```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDef
initions"
```

```
revision="1.0" schemaVersion="1.0">
```

```
<displayName>Control installed facilities
definitions</displayName>
```

```
<description>This file contains the control installed facilities
definitions.</description>
```

```
<resources>
```

```
<stringTable>
```

```
<string id="osec-send">Osec Subsystem Report</string>
```

```
<string id="osec-send_help">The policy allows you to determine
where to send the daily report:
```

```
Mail - Mail root
```

```
Journal - Write to systemd journal
```

```
</string>
```

```
<string id="osec-send_mail">Mail</string>
```

```
<string id="osec-send_journal">Journal</string>
```

```
</stringTable>
```

```
<presentationTable>
```

```
<presentation id="osec-send">
```

```

<dropdownList noSort="true" defaultItem="0" refId="osec-
send_setter">Where to send the report:
</dropdownList>
</presentation>
</presentationTable>
</resources>
</policyDefinitionResources>

```

4) скопировать обновленные файлы admx/adml на машину с Windows RSAT или GPOI.

В Windows RSAT:

```

- файл MyControl.admx В каталог
  \\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions;
- файл ru-RU/MyControl.adml В каталог
  \\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions\ru-RU;
- файл en-US/MyControl.adml В каталог
  \\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions\en-US.

```

Windows RSAT автоматически проверит корректность этих файлов.

В GPOI:

```

- файл MyControl.admx В каталог /usr/share/PolicyDefinitions;
- файл ru-RU/MyControl.adml В каталог
  /usr/share/PolicyDefinitions/ru-RU;
- файл en-US/MyControl.adml В каталог
  /usr/share/PolicyDefinitions/en-US.

```

5) проверить корректность кода, открыв редактор групповых политик – GPOI в ОС Альт СП (рис. 450) или RSAT в Windows;

6) если все корректно, скопировать обновленные файлы admx/adml на контроллер домена в сетевой каталог sysvol (/var/lib/samba/sysvol/<DOMAIN>/Policies/).

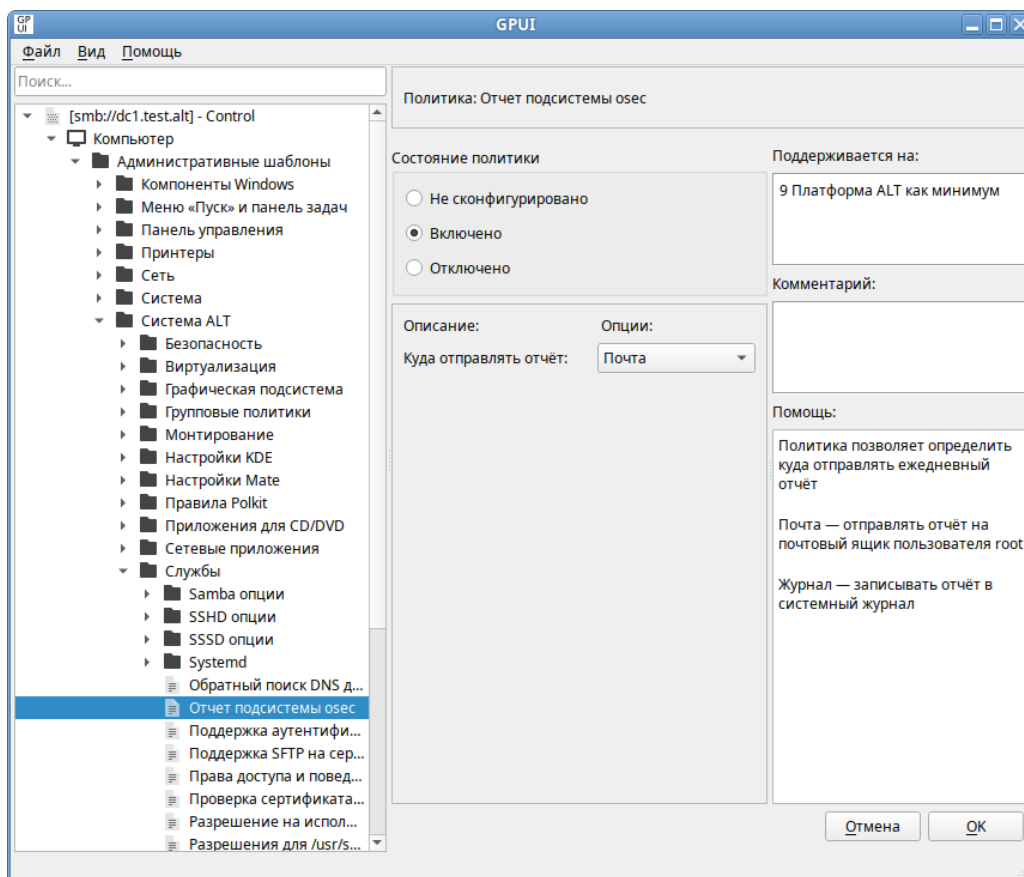


Рис. 450 – Проверка новой политики Control в GPUI

10.4.7.4.3. Пример для механизма Gsetting

Конфигурация DE Mate хранится в базе dconf, ключами которой управляет консольное приложение GSettings. Механизм gupdate управляет ключами GSettings и через них редактирует ключи dconf. На текущий день через ГП можно настраивать целый ряд параметров графической среды Mate – от фона рабочего стола до хранителя экрана. Можно также добавить новые политики для незадействованных ключей GSettings.

Примечание. Посмотреть все доступные схемы GSettings можно, выполнив команду:

```
$ gsettings list-schemas
```

Посмотреть все ключи GSettings можно, выполнив команду:

```
$ gsettings list-recursive
```

Ниже рассмотрен пример создания admx для ключа idle-delay схемы org.mate.session:

```
$ gsettings list-keys org.mate.session
gnome-compat-startup
show-hidden-apps
```

```
idle-delay
required-components-list
default-session
auto-save-session
logout-prompt
logout-timeout
session-start
```

```
$ gsettings get org.mate.session idle-delay
5
```

Ключ `idle-delay` позволяет управлять настройкой «Считать компьютер простаивающим через».

Пример создания новой политики для ключа `idle-delay` схемы `org.mate.session`:

1) создать файл `MyGsettings.admx`:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
revision="1.0" schemaVersion="1.0"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDef
initions">
<policyNamespaces>
<target prefix="gsettings"
namespace="BaseALT.Policies.MyGsettings" />
<using prefix="system" namespace="BaseALT.Policies.System" />
</policyNamespaces>
<resources minRequiredRevision="1.0" />
<policies>
<policy name="OrgMateSessionIdleDelayUser" class="User"
displayName="$(string.org-mate-session-idle-delay)"
explainText="$(string.org-mate-session-idle-delay_help)"
key="Software\BaseALT\Policies\gsettings"
presentation="$(presentation.OrgMateSessionIdleDelayUser-pr)">
<parentCategory ref="system:ALT_Screensaver_Mate" />
<supportedOn ref="system:SUPPORTED_AltP9" />
<elements>
<decimal id="OrgMateSessionIdleDelay_setter"
valueName="org.mate.session.idle-delay"
minValue="1" maxValue="2147483647" />
</elements>
</policy>
<policy name="OrgMateSessionIdleDelayMachine" class="Machine"
displayName="$(string.org-mate-session-idle-delay)"
explainText="$(string.org-mate-session-idle-delay_help)"
key="Software\BaseALT\Policies\gsettings"
presentation="$(presentation.OrgMateSessionIdleDelayMachine-pr)">
<parentCategory ref="system:ALT_Screensaver_Mate" />
<supportedOn ref="system:SUPPORTED_AltP9" />
<elements>
<decimal id="OrgMateSessionIdleDelay_setter"
valueName="org.mate.session.idle-delay"
```

```

minValue="1" maxValue="2147483647" />
<boolean          id="OrgMateSessionIdleDelay_setter_blocker"
key="Software\BaseALT\Policies\GSettingsLocks"
valueName="org.mate.session.idle-delay">
<trueValue>
<decimal value="1" />
</trueValue>
<falseValue>
<decimal value="0" />
</falseValue>
</boolean>
</elements>
</policy>
</policies>
</policyDefinitions>

```

2) создать файл ru-RU/MyGsettings.adml:

```

<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDef
initions"
revision="1.0" schemaVersion="1.0">
<displayName>Определения списка настроек рабочего окружения
МАТЕ</displayName>
<description>Этот файл содержит определения настроек рабочего
окружения МАТЕ.</description>
<resources>
<stringTable>
<string      id="org-mate-session-idle-delay">Считать      компьютер
простаивающим через</string>
<string      id="org-mate-session-idle-delay_help">Устанавливает
количество минут,
по истечении которых компьютер будет считаться простаивающим.
Опция «Блокировать» - (доступна только для машинной политики)
запрещает изменение
данной настройки пользователем. Блокировка политики делает ее
приоритетнее аналогичной политики для пользователя.
</string>
</stringTable>
<presentationTable>
<presentation id="OrgMateSessionIdleDelayUser-pr">
<text>Количество минут, по истечении которого компьютер будет
считаться простаивающим</text>
<decimalTextBox      refId="OrgMateSessionIdleDelay_setter"
defaultValue="1">Время в минутах</decimalTextBox>
</presentation>
<presentation id="OrgMateSessionIdleDelayMachine-pr">
<text>Количество минут, по истечении которого компьютер будет
считаться простаивающим</text>

```



```

<decimalTextBox                refId="OrgMateSessionIdleDelay_setter"
defaultValue="1">Время в минутах:</decimalTextBox>
<checkBox
refId="OrgMateSessionIdleDelay_setter_blocker">Блокировать</check
Box>
</presentation>
</presentationTable>
</resources>
</policyDefinitionResources>

```

3) создать файл en-US/MyGsettings.adml:

```

<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDef
initions"
revision="1.0" schemaVersion="1.0">
<displayName>MATE                desktop                configurations
definitions</displayName>
<description>This file contains the desktop MATE configurations
definitions.</description>
<resources>
<stringTable>
<string id="org-mate-session-idle-delay">Consider the computer
idle after</string>
<string id="org-mate-session-idle-delay_help">Sets the number of
minutes after which the computer will be considered idle.
The "Block" option - (available only for machine policy) prevents
the user
from changing this setting. Blocking a policy makes it a priority
over a similar policy for the user.
</string>
</stringTable>
<presentationTable>
<presentation id="OrgMateSessionIdleDelayUser-pr">
<text>Number of minutes after which the computer will be
considered idle</text>
<decimalTextBox                refId="OrgMateSessionIdleDelay_setter"
defaultValue="1">Time in minutes</decimalTextBox>
</presentation>
<presentation id="OrgMateSessionIdleDelayMachine-pr">
<text>Number of minutes after which the computer will be
considered idle</text>
<decimalTextBox                refId="OrgMateSessionIdleDelay_setter"
defaultValue="1">Time in minutes:</decimalTextBox>
<checkBox
refId="OrgMateSessionIdleDelay_setter_blocker">Блокировать</check
Box>
</presentation>
</presentationTable>
</resources>
</policyDefinitionResources>

```

- 4) скопировать обновленные файлы admx/adml на машину с Windows RSAT или GPUI.

В Windows RSAT:

- файл MyGsettings.admx в каталог
 \\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions;

- файл ru-RU/MyGsettings.adml в каталог
 \\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions\ru-RU;

- файл en-US/MyGsettings.adml в каталог
 \\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions\en-US.

Windows RSAT автоматически проверит корректность этих файлов.

В GPUI:

- файл MyGsettings.admx в каталог /usr/share/PolicyDefinitions;

- файл ru-RU/MyGsettings.adml в каталог /usr/share/PolicyDefinitions/ru-RU;

- файл en-US/MyGsettings.adml в каталог /usr/share/PolicyDefinitions/en-US;

- 5) проверить корректность кода, открыв редактор групповых политик – GPUI в ОС Альт СП (рис. 451) или RSAT в Windows;

- 6) если все корректно, скопировать обновленные файлы admx/adml на контроллер домена в сетевой каталог sysvol (/var/lib/samba/sysvol/<DOMAIN>/Policies/).

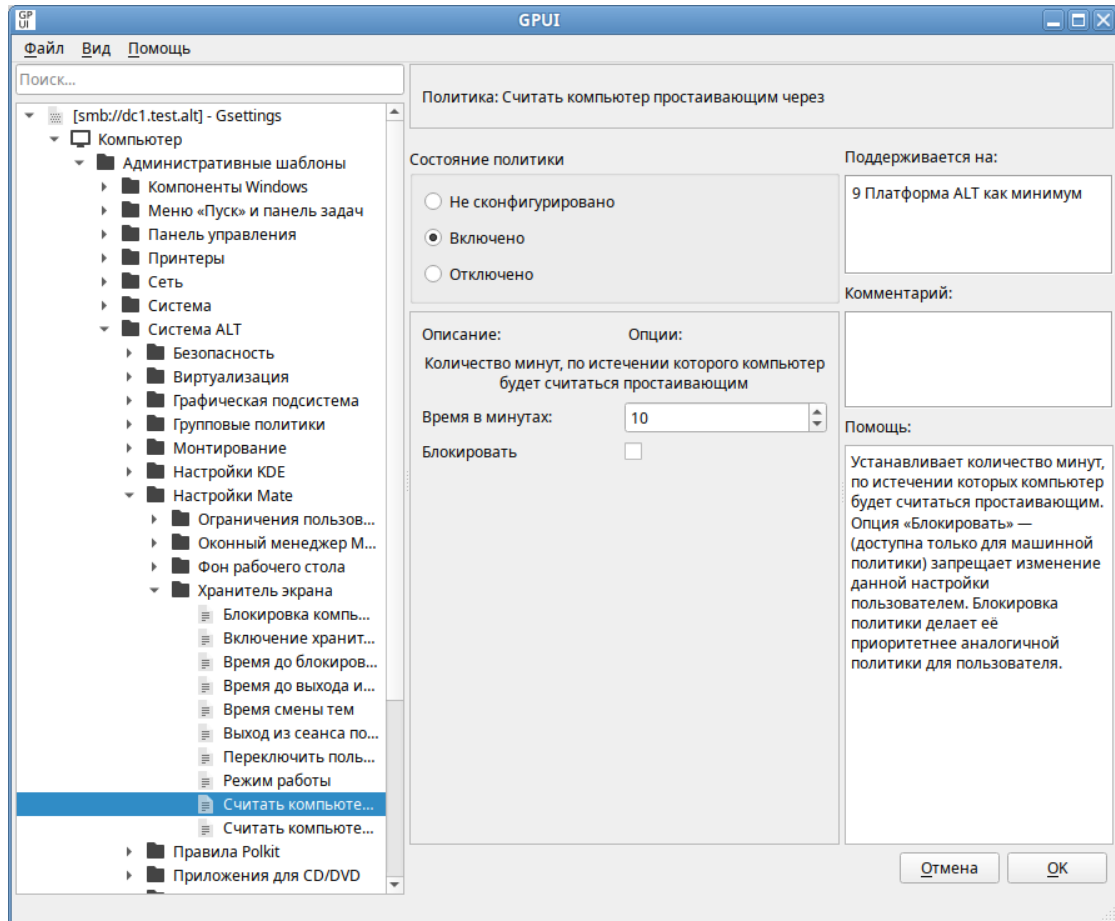


Рис. 451 – Проверка новой политики Gsetting в GPUI

10.4.7.4.4. Пример для механизма Polkit

Библиотека Polkit выполняет в ОС роль ограничителя действий приложений, преимущественно работающих на шине D-Bus. Polkit позволяет установить степень ограничений для непривилегированного процесса при обращении к привилегированному. Например, ограничить доступ пользователя к настройкам сети или монтированию блочного устройства (USB-накопителя) только для тех пользователей, которые знают пароль суперпользователя. Действия приложений, для которых заложены Polkit-ограничения, называются «actions». На основе указанных действий «actions» возможно формирование правил «polkit-rules», согласно которым в ОС и определится степень ограничений для программ и пользователей. Механизм `groupdate` умеет автоматически формировать polkit-правила. Благодаря этому возможно добавление новых групповых политик для polkit-правил.

Примечание. Все политики находятся в каталоге /usr/share/polkit-1/actions/ в формате *.policy Каждая политика представляет собой xml-файл, в котором описываются запросы к polkit.

Вывести список всех действий, определенных в /usr/share/polkit-1/actions/ можно, выполнив команду:

```
$ pkaction
```

Пример создания admx для действия org.xfce.thunar (запуск thunar от суперпользователя):

1) создать файл MyPolkit.admx:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"revision="1.0" schemaVersion="1.0"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDef
initions">
<policyNamespaces>
<target prefix="xfce" namespace="BaseALT.Policies.MyPolkit" />
<using prefix="system" namespace="BaseALT.Policies.System" />
</policyNamespaces>
<resources minRequiredRevision="1.0" />
<policies>
<policy class="Machine" displayName="$(string.org-xfce-thunar)"
explainText="$(string.org-xfce-thunar_help)"
key="Software\BaseALT\Policies\Polkit"
name="org.xfce.thunar"
valuename="org.xfce.thunar"
presentation="$(presentation.OrgXfceThunar-pr)">
<parentCategory ref="system:ALT_Polkit" />
<supportedOn ref="system:SUPPORTED_AltP10" />
<elements>
<enum id="OrgXfceThunar_setter" valueName="org.xfce.thunar"
required="true">
<item displayName="$(string.org-xfce-thunar-No)">
<value>
<string>No</string>
</value>
</item>
<item displayName="$(string.org-xfce-thunar-Yes)">
<value>
<string>Yes</string>
</value>
</item>
<item displayName="$(string.org-xfce-thunar-Auth-self)">
<value>
<string>Auth_self</string>
</value>
</item>
<item displayName="$(string.org-xfce-thunar-Auth-admin)">
<value>
```

```

<string>Auth_admin</string>
</value>
</item>
<item displayName="$ (string.org-xfce-thunar-Auth-self-keep) ">
<value>
<string>Auth_self_keep</string>
</value>
</item>
<item displayName="$ (string.org-xfce-thunar-Auth-admin-keep) ">
<value>
<string>Auth_admin_keep</string>
</value>
</item>
</enum>
<boolean                                id="OrgXfceThunar_blocker"
key="Software\BaseALT\Policies\PolkitLocks"
valueName="org.xfce.thunar">
<trueValue>
<decimal value="1" />
</trueValue>
<falseValue>
<decimal value="0" />
</falseValue>
</boolean>
</elements>
</policy>
</policies>
</policyDefinitions>

```

2) создать файл ru-RU/MyPolkit.adml:

```

<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDef
initions"
revision="1.0" schemaVersion="1.0">
<displayName>Определения политик Xfce</displayName>
<description>Этот файл содержит определения политик для
управления Xfce.</description>
<resources>
<stringTable>
<string id="org-xfce-thunar">Ограничение возможности запуска
Thunar от суперпользователя</string>
<string id="org-xfce-thunar_help">Политика управляет ограничением
возможности запуска Thunar от суперпользователя
Отключено/Не сконфигурировано - ограничения определяются
системными параметрами.
Включено - ограничение с установленными правами;
Возможные значения:
«No» - установить ограничение с запретом действия (пользователю
не разрешено выполнять действие);

```

ЛКНВ.11100-01 90 03

«Yes» - снять ограничение (пользователь может выполнять действие без какой-либо аутентификации);

«Auth_self» - пользователь должен ввести свой пароль для аутентификации.

Обратите внимание, этого уровня ограничения недостаточно для большинства

применений в многопользовательских системах, обычно рекомендуется «Auth_admin»;

«Auth_admin» - пользователь должен ввести пароль администратора при каждом запросе.

Требуется аутентификация пользователя с правами администратора;

«Auth_self_keep» - подобно «Auth_self», но авторизация сохраняется в течение

короткого периода времени (например, пять минут). Обратите внимание, этого уровня

ограничения недостаточно для большинства применений в многопользовательских системах, обычно рекомендуется

«Auth_admin_keep»;

«Auth_admin_keep» - аналогично «Auth_admin», но авторизация сохраняется в течение

короткого периода времени (например, пять минут);

Примечание: обладание административными правами в контексте PolicyKit определяются его правилами.

По умолчанию в Альт запрашивается пароль пользователя, находящегося в группе «wheel».

Опция «Блокировать» - запрещает изменение данной настройки пользователем.

Блокировка политики делает ее приоритетнее аналогичной политики для пользователя.

</string>

<string id="org-xfce-thunar-No">No</string>

<string id="org-xfce-thunar-Yes">Yes</string>

<string id="org-xfce-thunar-Auth-self">Auth_self</string>

<string id="org-xfce-thunar-Auth-admin">Auth_admin</string>

<string id="org-xfce-thunar-Auth-self-keep">Auth_self_keep</string>

<string id="org-xfce-thunar-Auth-admin-keep">Auth_admin_keep</string>

</stringTable>

<presentationTable>

<presentation id="OrgXfceThunar-pr">

<dropdownList noSort="true" defaultItem="1"

refId="OrgXfceThunar_setter">Варианты ограничений

на запуск Thunar от суперпользователя:</dropdownList>

<checkBox refId="OrgXfceThunar_blocker">Блокировать настройку ограничений</checkBox>

</presentation>

</presentationTable>

</resources>

</policyDefinitionResources>

3) создать файл en-US/MyPolkit.adml:

```

<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDef
initions"
revision="1.0" schemaVersion="1.0">
<displayName>ALT Xfce policies definitions</displayName>
<description>This file contains the Xfce service policies
definitions used by ALT operating system.</description>
<resources>
<stringTable>
<string id="org-xfce-thunar">Run Thunar as root</string>
<string id="org-xfce-thunar_help">This policy grants or restricts
permissions to run Thunar as root
Disabledd/Not configured - Permissions are determined by system
settings. Default is «Auth_admin»
Enabled - permission to mount with set rights;
Possible values:
"No" - block permissions (the user is not allowed to perform the
action);
"Yes" - grant permissions (the user can perform the action
without any authentication);
"Auth_self" - The user must enter their password to authenticate.
Note that this permission is not sufficient for most uses on
multi-user systems,
the "Auth_admin" permission is generally recommended;
"Auth_admin" - The user must enter an administrator password on
each request.
Requires user authentication with administrator rights;
"Auth_self_keep" - Similar to "Auth_self", but the authorization
is kept for
a short period of time (for example, five minutes). Note that
this permission
is not sufficient for most uses on multi-user systems, the
"Auth_admin_keep" permission is generally recommended;
"Auth_admin_keep" - similar to "Auth_admin", but the
authorization
is kept for a short period of time (for example, five minutes);
Note: the possession of administrative rights in the context of
PolicyKit
is determined by its rules. By default, Alt asks for the password
of the user in the "wheel" group.
The "Block" option prevents the user from changing this setting.
Blocking a policy makes it a priority over a similar policy for
the user.
</string>
<string id="org-xfce-thunar-No">No</string>
<string id="org-xfce-thunar-Yes">Yes</string>
<string id="org-xfce-thunar-Auth-self">Auth_self</string>
<string id="org-xfce-thunar-Auth-admin">Auth_admin</string>

```

```

<string id="org-xfce-thunar-Auth-self-keep">Auth_self_keep</string>
<string id="org-xfce-thunar-Auth-admin-keep">Auth_admin_keep</string>
</stringTable>
<presentationTable>
<presentation id="OrgXfceThunar-pr">
<dropdownList noSort="true" defaultItem="1"
refId="OrgXfceThunar_setter">Restriction options:</dropdownList>
<checkBox refId="OrgXfceThunar_blocker">Block</checkBox>
</presentation>
</presentationTable>
</resources>
</policyDefinitionResources>

```

4) скопировать обновленные файлы admx/adml на машину с Windows RSAT или GPUI.

В Windows RSAT:

- файл	MyPolkit.admx	В	каталог
	\\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions;		
- файл	ru-RU/MyPolkit.adml	В	каталог
	\\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions\ru-RU;		
- файл	en-US/MyPolkit.adml	В	каталог
	\\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions\en-US.		

Windows RSAT автоматически проверит корректность этих файлов.

В GPUI:

- файл MyPolkit.admx в каталог /usr/share/PolicyDefinitions;
- файл ru-RU/MyPolkit.adml в каталог /usr/share/PolicyDefinitions/ru-RU;
- файл en-US/MyPolkit.adml в каталог /usr/share/PolicyDefinitions/en-US;

5) проверить корректность кода, открыв редактор групповых политик – GPUI в ОС Альт СП (рис. 452) или RSAT в Windows;

6) если все корректно, скопировать обновленные файлы admx/adml на контроллер домена в сетевой каталог sysvol (/var/lib/samba/sysvol/<DOMAIN>/Policies/).

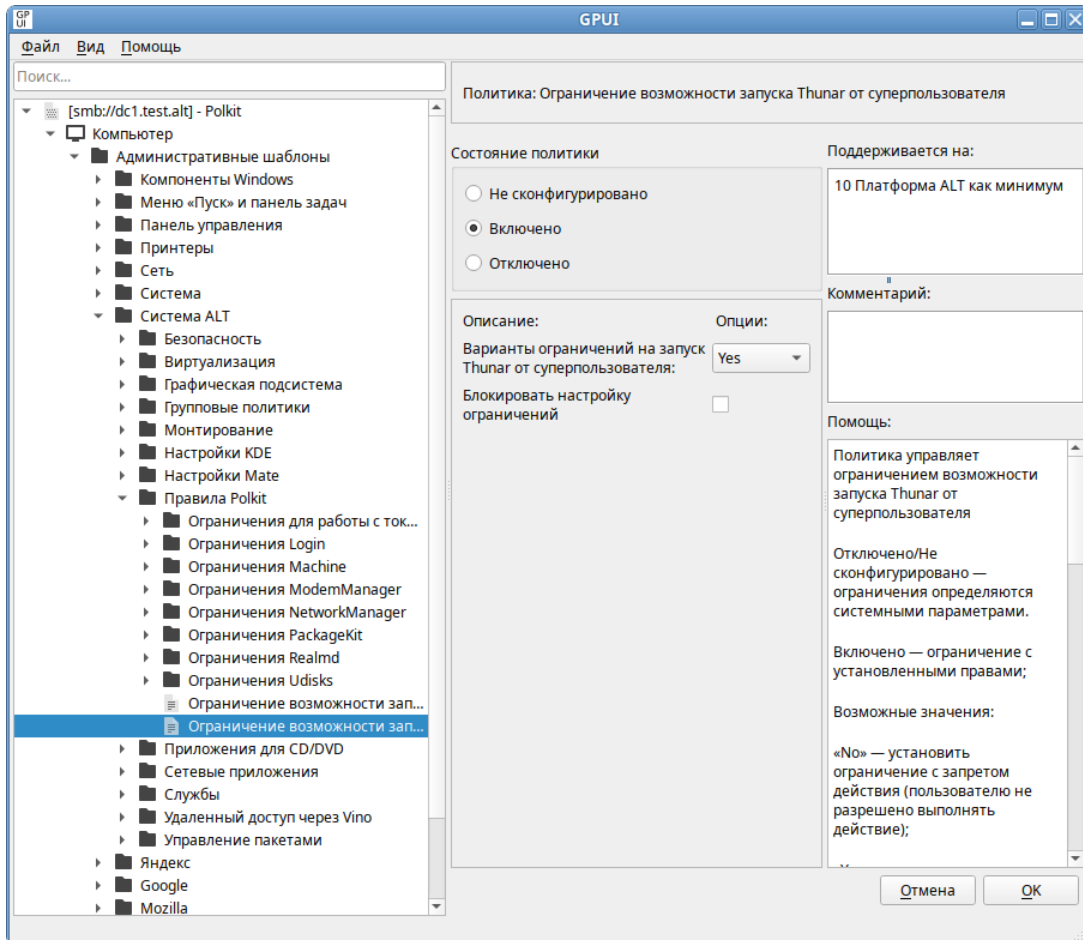


Рис. 452 – Проверка новой политики Polkit в GPUI

10.4.8. Решение проблем

Прежде чем разбираться, почему групповые политики не применяются, как ожидается, необходимо убедиться, что инфраструктура «Альт Домен» работает штатно. Работа групповых политик в домене зависит от корректности работы контроллеров домена и репликации между ними.

Не рекомендуется использовать сложную структуру групповых политик и создавать дополнительные политики без необходимости. Рекомендуется использовать единую схему наименования политик. Имя групповой политики должно давать однозначное понимание того, для чего она нужна.

10.4.8.1. Область действия и статус групповой политики

В каждой групповой политике есть два независимых раздела с настройками:

- «Компьютер» – параметры, применяемые к компьютеру;
- «Пользователь» – параметры пользователей.

Если параметр политики настраивается в секции «Компьютер», групповая политика должна быть привязана к OU с компьютерами. Соответственно, если настраиваемый параметр относится к конфигурации пользователя, нужно назначить политику на OU с пользователями. Также следует убедиться, что объект, к которому должна применяться политика находится в нужном OU с компьютерами или пользователями.

Примечание. Чтобы применить пользовательские настройки к компьютерам, нужно включить политику замыкания (см. п. 10.4.8.4).

Если ГП настраивает только параметры пользователя или только параметры компьютера, неиспользуемый раздел можно отключить. Это снизит трафик ГП и позволит уменьшить время обработки групповой политики на клиентах.

Статус групповой политики можно проверить в ADMC в свойствах подразделения на вкладке «Групповая политика» (рис. 453).

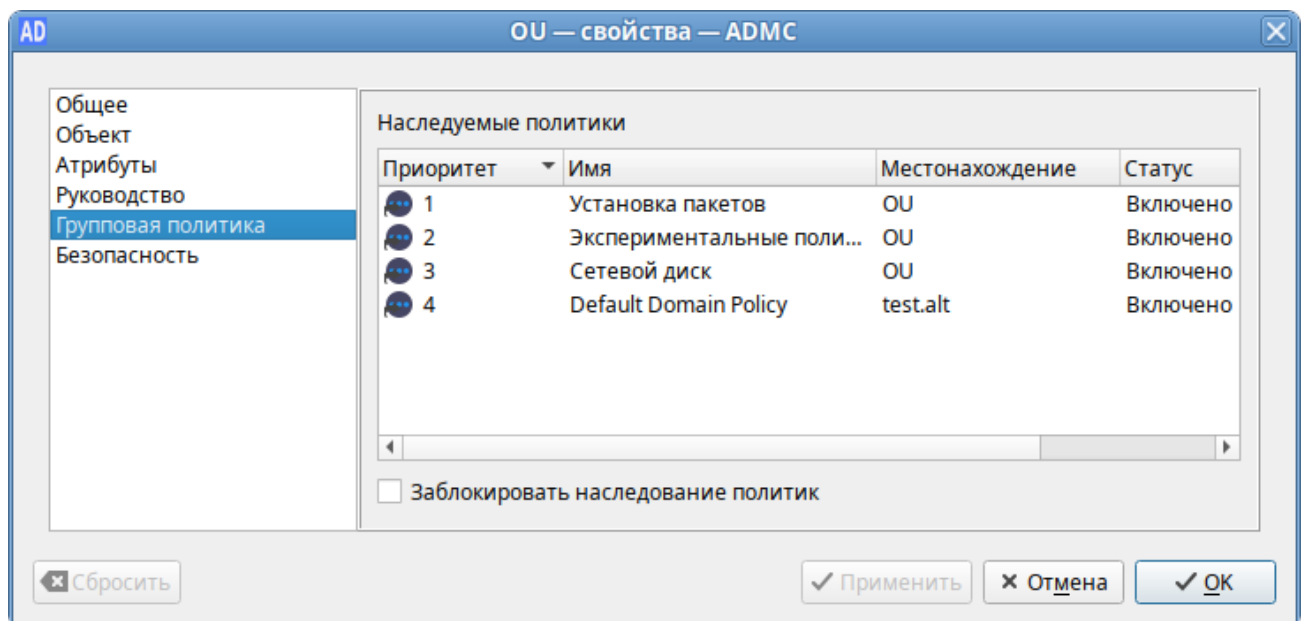


Рис. 453 – Статус групповых политик

Изменение статуса групповой политики возможно в свойствах на вкладке «Атрибуты» (рис. 454).

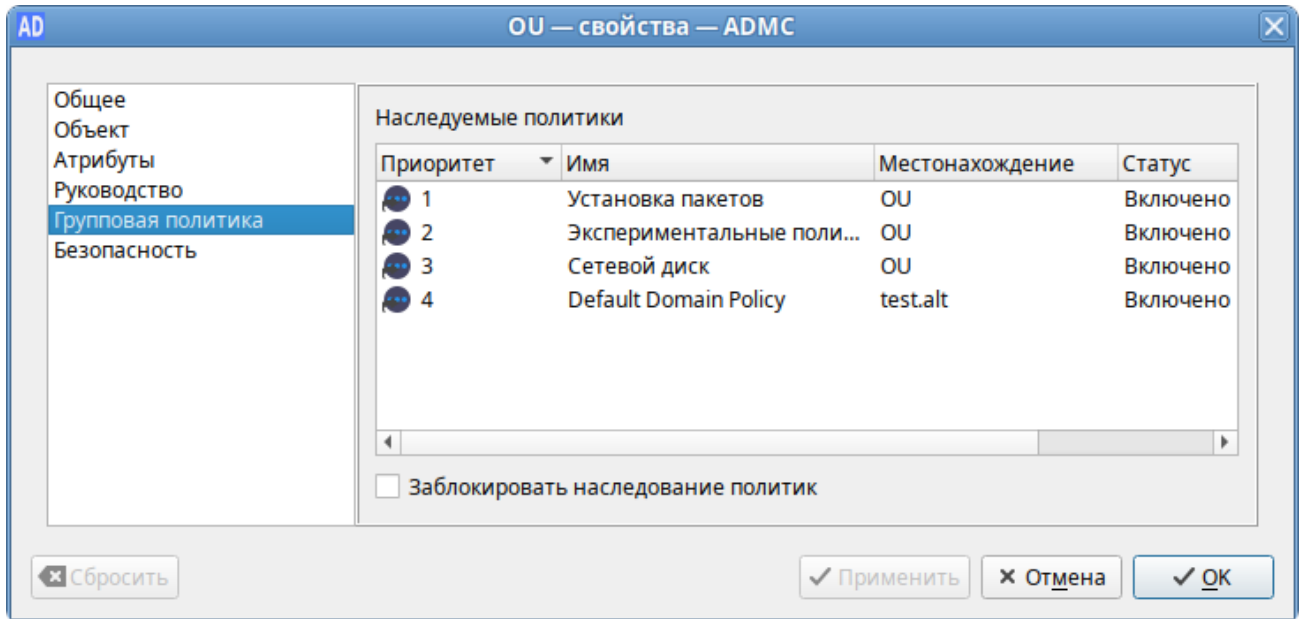


Рис. 454 – Атрибут «flags» в свойствах ГП

Состояние объекта групповой политики указывается в значении атрибута `flags`. Данный атрибут может принимать следующие значения:

- значение «0» – объект ГП включен (все настройки политики применяются к целевым объектам домена);
- значение «1» – отключен раздел «Конфигурация пользователя» (не применяются настройки пользовательских политик);
- значение «2» – отключен раздел «Конфигурация компьютера» (не применяются настройки из параметров ГП компьютера);
- значение «3» – объект ГП полностью отключен (все настройки политики не применяются).

10.4.8.2. Наследование групповых политик

По умолчанию политики высокого уровня применяются ко всем вложенным объектам в иерархии домена.

Увидеть какие политики применяются к подразделению и местонахождение политики можно в ADMS при выборе подразделения на вкладке «Наследуемые политики» (рис. 455).

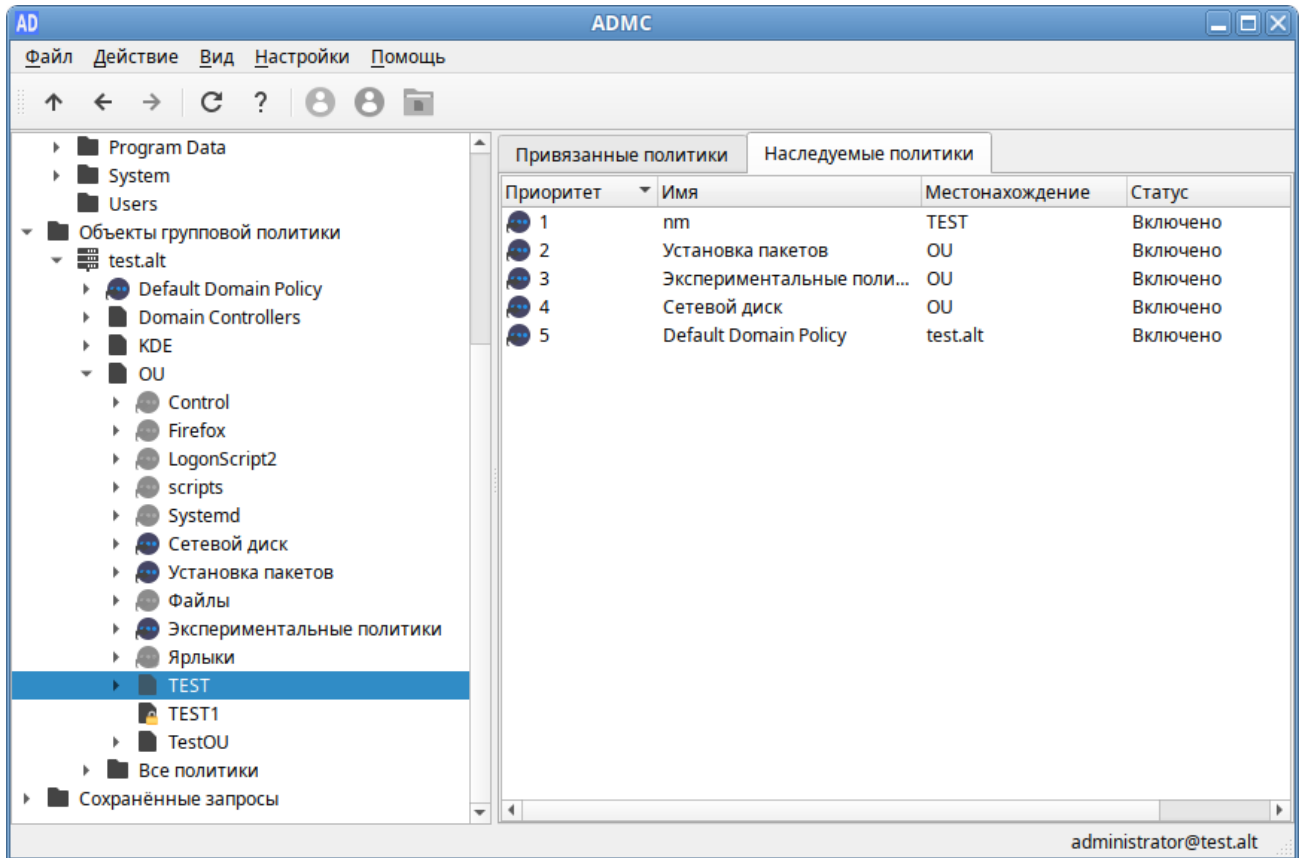


Рис. 455 – Политики подразделения без блокирования наследования

Также наследуемые политики можно увидеть на вкладке «Групповая политика» свойств подразделения (рис. 456).

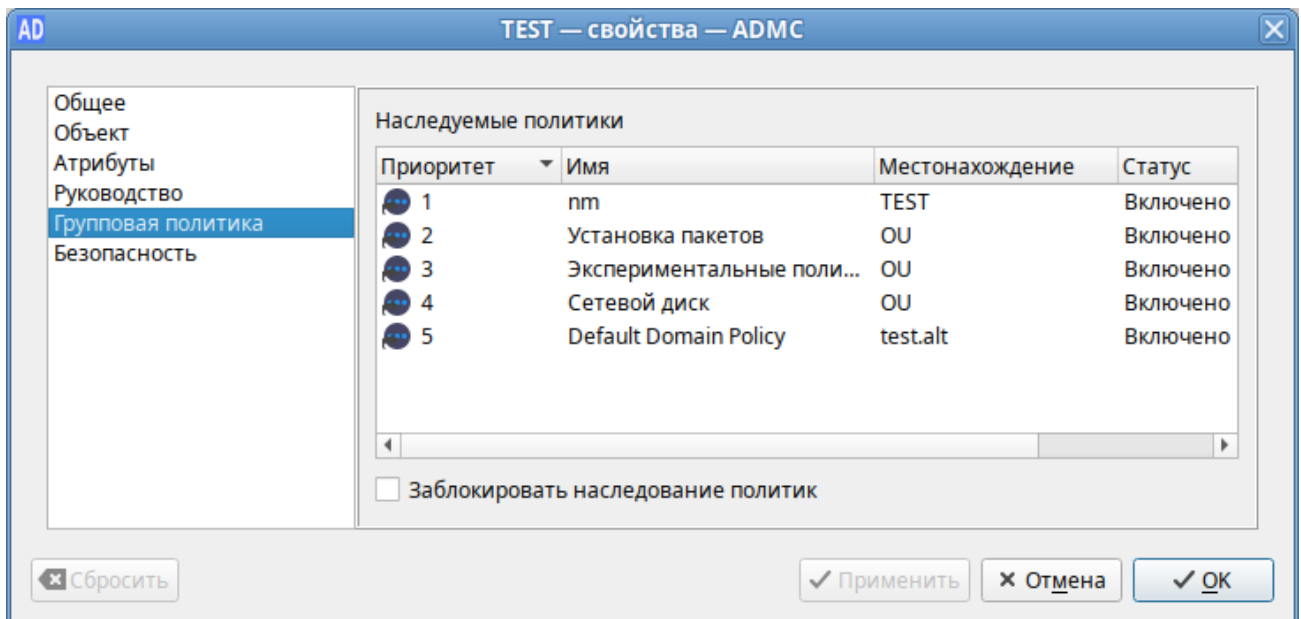


Рис. 456 – Вкладка «Групповая политика»

Каждый объект групповой политики можно настроить на блокирование наследования политик более высокого уровня (см. п. 10.4.5.12.3). Таким образом, политика подразделения может блокировать параметры политик домена и сайта. Блокирование наследования предохраняет объекты групповой политики, связанные с доменами или подразделениями родительского уровня, от автоматического наследования на дочернем уровне (рис. 457).

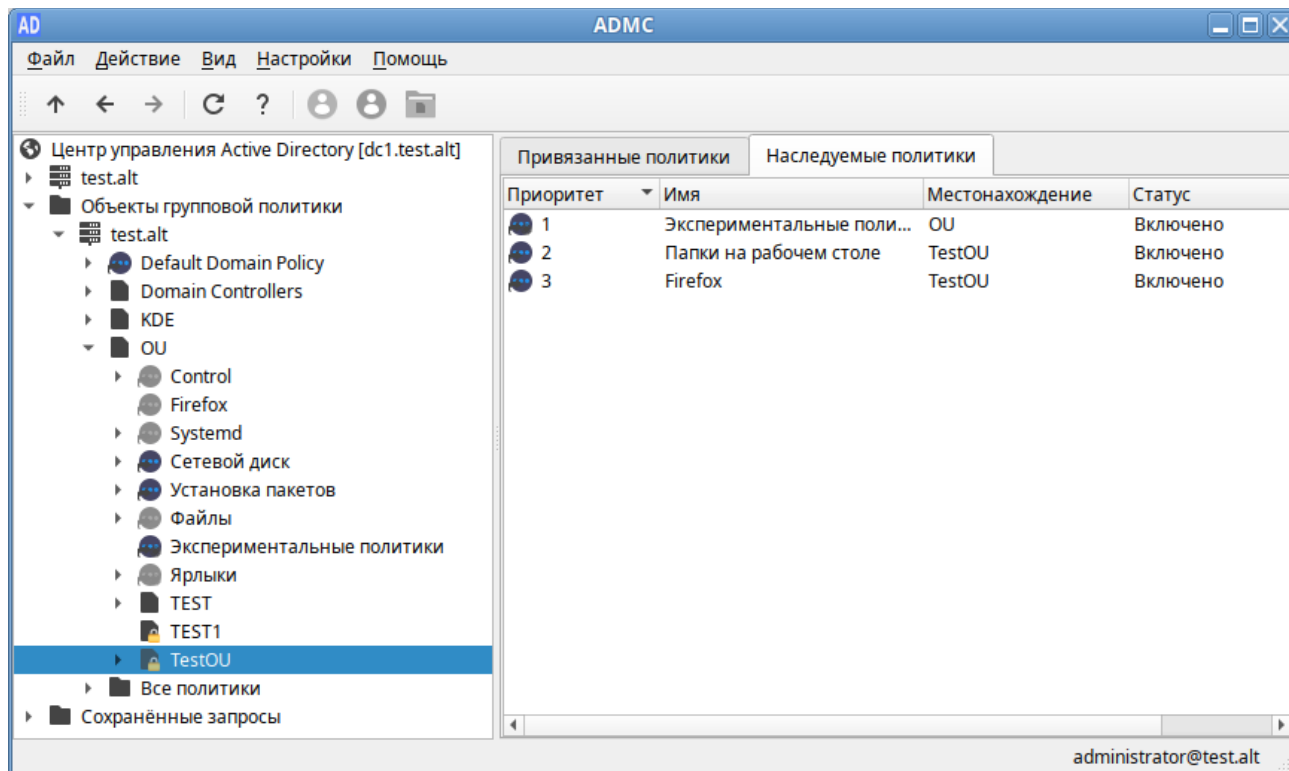


Рис. 457 – Политики подразделения с блокированием наследования

Так как администратор домена может не согласиться с тем, что администратор подразделения блокирует параметры политики домена, существует возможность запретить переопределение параметров с помощью отметки «Принудительно».

10.4.8.3. Порядок применения групповых политик

Групповые политики обрабатываются в следующем порядке:

- объект локальной групповой политики;
- объекты групповой политики, связанные с доменом (в рамках возможностей и ограничений поддержки леса доменов в Samba, как в наборе клиентских компонентов);

- объекты групповой политики, связанные с OU: сначала обрабатываются объекты групповой политики, связанные с OU, находящейся на самом высоком уровне в иерархии Active Directory, затем объекты групповой политики, связанные с дочерним подразделением и т. д. Последними обрабатываются объекты групповой политики, связанные с OU, в которой находится пользователь или компьютер.

Последние политики имеют наивысший приоритет. Т. е. если параметр включен на уровне политики домена, но на целевом OU данный параметр отключается другой политикой – это означает, что нужный параметр в результате будет отключен на клиенте (выиграет ближайшая политика к объекту в иерархии «Альт Домен»).

Если на OU назначено несколько групповых политик, то они обрабатываются в том порядке, в котором были назначены. Политики обрабатываются в обратном порядке (политика с номером 1 будет обработана последней) (рис. 458).

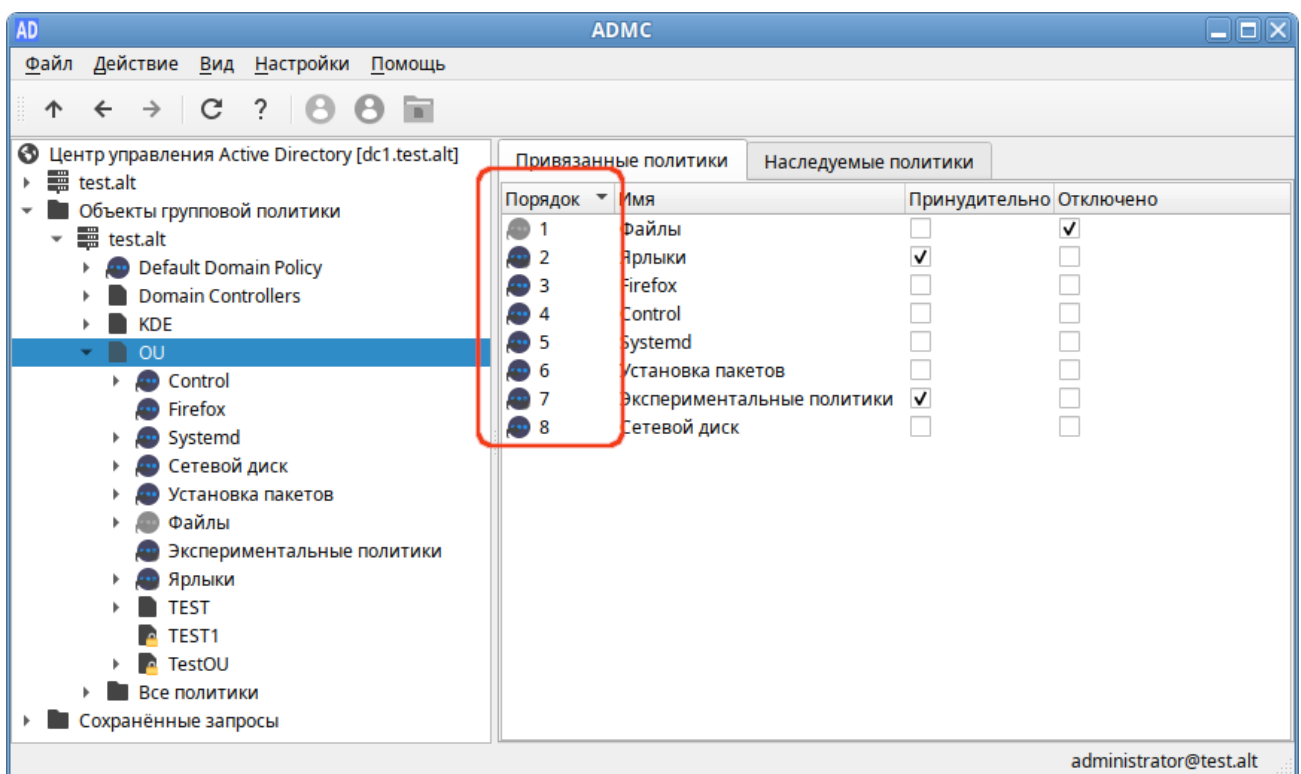


Рис. 458 – Порядок обработки групповых политик

При необходимости этот порядок можно изменить, выбрав в контекстном меню политики пункт «Переместить вверх» или «Переместить вниз» (рис. 459).

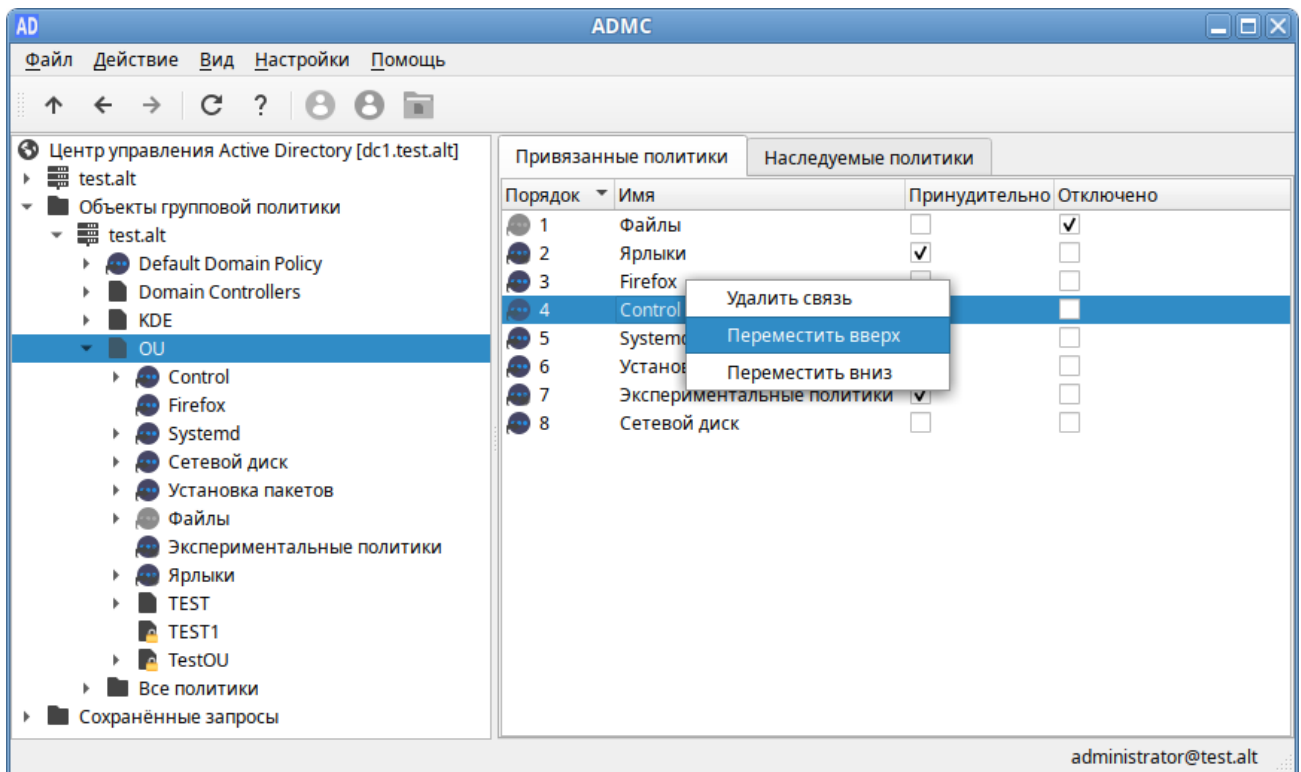


Рис. 459 – Изменение порядка обработки политики

При использовании параметра «Принудительно» у групповой политики выигрывает та политика, которая находится выше в иерархии домена, например, политика Default Domain Policy будет выигрывать у всех других групповых политик, если у нее активирован этот параметр.

У каждого объекта групповой политики, который привязан к организационному контейнеру домена можно включить или отключить связь (применение политики). Для этого нужно выбрать опцию «Удалить связь/Добавить связь» в меню политики. При отключении связи политика перестает применяться к клиентам, но ссылка на объект групповой политики не удаляется из иерархии. Активировать данную связь можно в любой момент.

10.4.8.4. Замыкание групповой политики

По умолчанию групповая политика применяется к пользователю или компьютеру способом, который зависит от того, где и пользователь, и объекты компьютера находятся в домене. В некоторых случаях может потребоваться применить к пользователям политику в зависимости от расположения объекта компьютера.

На компьютерах, расположенных в организационном подразделении (Organization Unit, OU), машинные объекты групповой политики применяются по порядку во время запуска компьютера. Пользовательские объекты групповой политики, пользователей из OU, применяются во время входа, независимо от того, на каком компьютере пользователь входит в систему.

Если пользовательская учетная запись находится в OU, на которое распространяется действие пользовательской политики, то применяться эти настройки будут при входе пользователя в систему независимо от того, в какое OU входит компьютер. Такое поведение может быть нежелательным, например, вполне разумно иметь одни пользовательские настройки для сервера, другие – для локального компьютера.

Политику замыкания можно использовать для применения пользовательских групповых политик в зависимости от того, на каком компьютере пользователь входит в систему.

Эта политика может принимать два значения:

- режим «Слияние» (Merge) – при входе пользователя в систему к компьютеру будут применяться политики, основанные на расположении пользователя, а затем политики, привязанные к компьютеру. При возникновении конфликтов между пользовательскими и машинными политиками, машинные политики будут иметь более высокий приоритет;
- режим «Замена» (Replace) – к пользователю будут применяться только политики, назначенные на OU, в котором содержится компьютер, на который пользователь выполнил вход.

В качестве примера рассмотрим домен с двумя организационными подразделениями – OU1 и OU2. В первом находятся объекты учетных записей пользователей и их локальные компьютеры, во втором – объекты серверов (рис. 460).

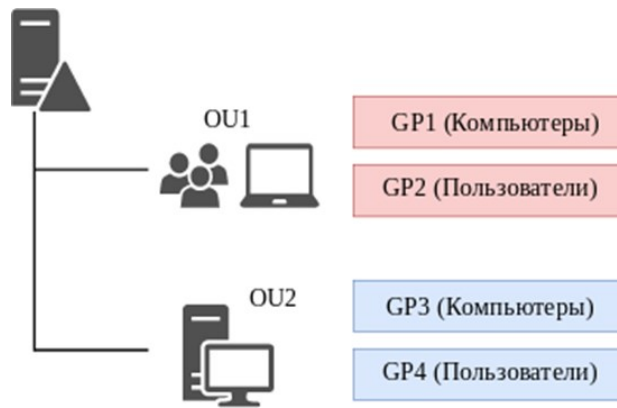


Рис. 460 – Схема деления домена

Если пользователь осуществляет вход в систему на локальном компьютере, то он оказывается под действием политики GP1 локального компьютера (которая была применена при его включении) и политики GP2 пользователя (примененной при входе в систему). Если пользователь осуществляет вход на сервер, то будут действовать политика сервера GP3 и политика пользователя GP2.

Если же включить политику замыкания (см. п. 10.4.8.4), то при входе на сервер будут действовать политика сервера GP3 и политика пользователя GP2+GP4 (в режиме «Слияние») или только GP4 (в режиме «Замена»). При возникновении любых конфликтов настроек между политиками OU пользователя и OU сервера в режиме «Слияние» политика в OU сервера будет иметь более высокий приоритет.

10.4.8.5. Диагностика применения ГП на стороне клиента

Для диагностики применения групповых политик на стороне клиента используются утилиты gpoa (на машинах Альт), gpresult (на машинах Windows).

Для диагностики механизмов применения групповых политик на клиенте можно выполнить команды:

1) получить и применить настройки для текущей машины:

```
# gpoa --loglevel 0
```

2) получить и применить настройки для пользователя:

```
# gpoa --loglevel 0 <имя_пользователя>
```

10.4.8.6. Коды ошибок

Сообщения, сопутствующие кодам ошибок, могут изменяться (переводиться, исправляться), но сам код уникален для определенной части программы, что позволяет однозначно идентифицировать проблему (таблица 67).

Т а б л и ц а 67 – Коды ошибок и их описание

Код	Описание	Решение
E00001	Недостаточно прав для запуска программы <code>grpupdate</code>	Необходимо повысить уровень привилегий. Может помочь запуск программы от имени администратора
E00002	Программа <code>grpupdate</code> не будет запущена из-за предыдущих ошибок	
E00003	Ошибка работы бэкэнда, которая привела к досрочному прекращению обработки групповых политик. Этот код характеризует серьезные ошибки, которые обрабатываются на самом высоком уровне	Возможно, это ошибка в коде и необходимо создать отчет об ошибке, чтобы разработчики узнали о ней
E00004	Ошибка во время работы фронтенда	Высокоуровневая ошибка при инициализации фронтенда или во время работы <code>appliers</code> . С большой вероятностью может оказаться ошибкой в коде
E00005	Не получилось запустить <code>appliers</code> политик для обновления групповых политик компьютера	Проверить, что машина все еще в домене, демон <code>oddjbd</code> доступен через D-Bus и у пользователя достаточно прав для запуска ПО
E00006	Показать список доступных бэкэндов	Проверить, что машина все еще в домене, демон <code>oddjbd</code> доступен через D-Bus и у пользователя достаточно прав для запуска ПО
E00007	Невозможно инициализировать бэкэнд Samba в силу неполадок компонентов, связанных с Samba	Необходимо проверить инсталляцию Samba на машине, убедиться, что машина введена в домен и домен доступен
E00008	Невозможно инициализировать бэкэнд <code>no-domain</code> для выполнения процедуры бутстрапа групповых политик	Возможно, было произведено вмешательство в локальную политику или произошел <code>misconfiguration</code> . Необходимо проверить целостность пакета <code>local-policy</code> и настройки домена в <code>Alterator</code> .
E00009	Произошла ошибка при попытке запуска <code>adp</code>	Необходимо обратиться к руководству по устранению неполадок проекта ADP
E00010	Произошел сбой при попытке получить имя домена Active Directory	Необходимо проверить работу доменной службы имен (DNS), а также доступность доменного LDAP. Для доступа к LDAP необходим работоспособный Kerberos, так что стоит проверить и его конфигурацию

Продолжение таблицы 67

Код	Описание	Решение
E00011	Во время работы <code>applier</code> с пониженным уровнем привилегий произошла неполадка	Возможно, что в используемой групповой политике заданы параметры, для установки которых требуются права администратора. Это необходимо проверить и исправить объект групповой политики соответственно
E00012	Высокоуровневая ошибка инициализации бэкэнда	Необходимо проверить наличие условий для запуска бэкэнда. В случае с Samba – удостовериться, что машина введена в домен
E00013	У пользователя, запустившего программу, недостаточно прав для обновления настроек машины	Запустить программу с правами администратора
E00014	Не прошла проверка наличия билета Kerberos. Билет Kerberos нужен для доступа к сервисам домена	Проверить конфигурацию Kerberos в файле <code>/etc/krb5.conf</code> . Попытаться получить билет Kerberos вручную
E00015	Запрос на получение имени домена Active Directory через LDAP не прошел	Проверить возможность получения Kerberos ticket для машины. Проверить работу DNS и возможность обратиться к доменному LDAP
E00016	Утилита <code>wbinfo</code> не отдает SID для пользователя, для которого выполняется обновление групповых политик	Проверить целостность программы <code>wbinfo</code> . Проверить, что машина введена в домен.
E00017	Невозможно получить список групповых политик для репликации на используемое имя пользователя	Следует удостовериться, что пользователь для которого происходит попытка получить список групповых политик, существует в домене. Также необходимо удостовериться, что проблема не вызвана <code>misconfiguration</code> домена
E00018	Не получилось прочесть содержимое настройки <code>XDG_DESKTOP_DIR</code>	Необходимо удостовериться, что <code>XDG</code> в системе сконфигурирован корректно и пользователь, для которого вычитывается настройка, существует
E00019	Произошла ошибка во время работы <code>applier</code> для пользователя	Необходимо удостовериться, что это не <code>misconfiguration</code> в используемой GPO. Возможно это ошибка. В таком случае необходимо создать отчет об ошибке, чтобы разработчики узнали о ней
E00020	Произошла ошибка во время работы <code>applier</code> для пользователя с пониженными привилегиями	Необходимо удостовериться, что это не <code>misconfiguration</code> в используемой GPO. Возможно это ошибка. В таком случае необходимо создать отчет об ошибке, чтобы разработчики узнали о ней
E00021	Не был получен ответ от D-Bus при попытке запустить <code>groa</code> для текущего пользователя	Следует удостовериться, что D-Bus работает корректно и демон <code>oddjobd</code> запущен.
E00022	Не был получен ответ от D-Bus при попытке запустить <code>groa</code> для машины	Необходимо удостовериться, что D-Bus работает корректно и демон <code>oddjobd</code> запущен

Продолжение таблицы 67

Код	Описание	Решение
E00023	Не был получен ответ от D-Bus при попытке запустить groa для пользователя	Следует удостовериться, что D-Bus работает корректно и демон oddjobd запущен. Необходимо удостовериться, что у текущего пользователя достаточно прав для обращения к D-Bus
E00024	Ошибка во время работы машинного applier	Необходимо проверить настройки applier вручную, чтобы убедиться, что соответствующая часть ОС не поломана
E00025	Ошибка во время инициализации пользовательского applier	Необходимо проверить, что машина является частью домена и контроллер домена доступен. Следует удостовериться, что пользователь существует и что соответствующая часть ОС не поломана
E00026	Ошибка слияния машинной групповой политики	Необходимо очистить кеш gpupdate
E00027	Ошибка слияния пользовательской групповой политики	Необходимо очистить кеш gpupdate
E00028	Ошибка слияния машинной части групповой политики	Необходимо очистить кеш gpupdate
E00029	Ошибка слияния пользовательской части групповой политики	Необходимо очистить кеш gpupdate
E00030	Ошибка при запуске процесса с пониженным уровнем привилегий в контексте пользователя	Необходимо проверить наличие домашнего каталога пользователя, для которого выполняется gpupdate
E00042	Не входит в возможные значения для control	Ошибка возникает в случае некорректного целочисленного типа данных, прописанного в шаблонах групповых политик (ADMX-файлах)
E00055	Ошибка при запуске pkcon_runner синхронно для компьютера	Необходимо проверить наличие в системе и корректность файла pkcon_runner
E00056	Ошибка запуска apt-get update	Необходимо проверить подключение к сети и корректность репозитория, отсутствие подключенных дополнительных репозиториях
E00057	Ошибка установки пакета	Необходимо проверить наличие пакета в репозиториях, правильность имени пакета, наличие подключения к сети и наличие в системе пакета PackageKit
E00058	Ошибка удаления пакета	Вероятно, пакет не установлен в систему или в системе отсутствует пакет PackageKit
E00059	Не входит в возможные значения для control	Ошибка возникает в случае некорректного строкового типа данных, прописанного в шаблонах групповых политик (ADMX-файлах)

Окончание таблицы 67

Код	Описание	Решение
E00060	Ошибка при запуске <code>pkcon_runner</code> синхронно для пользователя	Необходимо проверить наличие в системе и корректность файла <code>pkcon_runner</code>
E00061	Ошибка при запуске <code>pkcon_runner</code> асинхронно для компьютера	Необходимо проверить наличие в системе и корректность файла <code>pkcon_runner</code>
E00062	Ошибка при запуске <code>pkcon_runner</code> асинхронно для пользователя	Необходимо проверить наличие в системе и корректность файла <code>pkcon_runner</code>
E00067	Ошибка создания переменных среды	Необходимо убедиться в наличии переменных окружения: <code>XDG_DATA_DIRS</code> , <code>XDG_RUNTIME_DIR</code> , <code>DBUS_SESSION_BUS_ADDRESS</code> , <code>PATH</code>
E00068	Ошибка выполнения команды <code>kwriteconfig5</code>	Необходимо убедиться, что установлен пакет <code>kf5-kconfig</code>

10.4.8.7. Диагностика проблем при работе с политикой скриптов

На контроллере домена:

- 1) проверить работоспособность загружаемого скрипта в дистрибутиве ОС Альт СП;
- 2) убедиться, что кодировка файла со скриптом – UTF8, без BOM;
- 3) убедиться, что скрипт расположен в каталоге (GPT) применяемого объекта групповой политики (GPO);
- 4) убедиться, что включена групповая политика «Экспериментальные групповые политики» или политика «Управление logon-скриптами» (см. 10.4.6.6.3);
- 5) убедиться, что целевой компьютер, входит в подразделение (OU), к которому привязан объект групповой политики (GPO).

На компьютере пользователя:

- 6) проверить версию `gupdate` (политики скриптов выполняются с релиза 0.9.11-alt1);
- 7) убедиться, что механизм применения политик (`gupdate`) запущен:


```
# gupdate-setup status
```
- 8) убедиться, что служба скриптов запущена:


```
# systemctl status gupdate-scripts-run.service
```

9) проверить содержимое каталога и права для загруженных скриптов:

```
# ls -Rl /var/cache/gpupdate_scripts_cache/
```

10) проверить состояние службы запуска скриптов пользователя (от пользователя):

```
$ systemctl --user status gpupdate-scripts-run-user.service
```

11) вывести журнал применения политик:

```
# gpoa --loglevel 0
```

10.5. Доверительные отношения (Трасты)

Доверительные отношения (trusts) позволяют аутентифицироваться под пользователями не только текущего домена, но и доверенных.

10.5.1. Настройка доверия

10.5.1.1. Общие сведения

Доверительные отношения (рис. 461) реализуются в рамках механизма аутентификации. Суть доверительных отношений между двумя доменами сводится к тому, что доверяющий домен (trusting domain) доверяет процесс аутентификации доверенному домену (trusted domain). Пользователь, аутентифицированный доверенным доменом, может получить доступ к ресурсам в доверяющем домене.

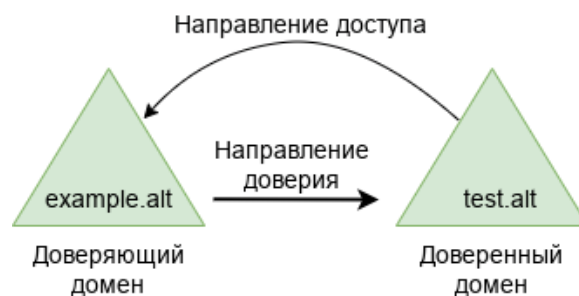


Рис. 461 – Схема доверительных отношений в рамках механизма аутентификации

Отношения доверия обеспечивают доступ к ресурсам в одном или двух направлениях:

- одностороннее доверие – позволяет пользователям и группам из домена А получать доступ к ресурсам в домене Б, но не наоборот. Домен А доверяет домену Б, но домен Б не доверяет домену А. При создании такого доверия нужно указать направление (входящее или исходящее);

- двустороннее доверие – позволяет пользователям и группам из домена А получать доступ к ресурсам в домене Б и наоборот. Запросы проверки подлинности могут передаваться между двумя доменами в обоих направлениях. Домен А доверяет домену Б, а домен Б доверяет домену А.

Транзитивность определяет, можно ли расширить доверие за пределы двух доменов, для которых оно сформировано:

- транзитивное доверие можно использовать для расширения отношений доверия на другие домены;
- нетранзитивное доверие можно использовать для запрета отношений доверия с другими доменами.

Типы доверия:

- доверие леса (Forest) – связывает леса и все их домены (это двусторонние или односторонние отношения доверия между разными лесами, всегда являющиеся транзитивными);
- внешнее доверие (External) – устанавливается между двумя доменами напрямую вне леса (для установки двустороннего доверия нужно использовать два разнонаправленных доверия, которыми надо связать все требуемые пары доменов).

10.5.1.2. Особенности доверительных отношений в Samba

Поддерживается:

- доверие леса (это доверие может быть установленным между двумя Samba-доменами или Samba-доменом и Windows-доменом);
- внешние доверительные отношения между доменом AD и доменом в стиле NT;
- добавление пользователей и групп доверенного домена в группы доверяющего домена (при этом необходимо использовать SID пользователей и групп, имя пользователя или имя группы использовать невозможно);
- в RSAT можно увидеть foreignSecurityPrincipal для всех добавленных пользователей и групп из доверенного домена.

Особенности и ограничения:

- не применяются правила фильтрации SID;
- нельзя добавить пользователей и группы доверенного домена в доменные группы доверяющего домена по имени;
- для входа в доверенный домен через SSSD надо использовать тип связи External, а не Forest;
- обе стороны траста должны полностью доверять друг другу (администратор из домена А может управлять всеми объектами в домене Б и наоборот);
- не поддерживается выборочная аутентификация;
- нельзя создать доверительные отношения между доменами в одном дереве с одним и тем же пространством имен верхнего уровня. NetBIOS имена доменов должны отличаться (домен MYDOMAIN.WIN и MYDOMAIN.NEW будут иметь одинаковое короткое имя – MYDOMAIN, это приведет к невозможности установки доверительных отношений).

Для управления доверием можно использовать инструмент командной строки `samba-tool` (таблица 68).

Т а б л и ц а 68 – Команды управления доверием

Команда	Описание	Примечание
<code>domain trust create <домен></code>	Создать доверие домена или леса	Можно использовать следующие опции: <code>--type=TYPE</code> – тип доверия (<code>external, forest</code>); <code>--direction=DIRECTION</code> – направление доверия (<code>incoming, outgoing, both</code>); <code>--create-location=LOCATION</code> – где создать объект доверенного домена (<code>local, both</code>); <code>--quarantined=yes no</code> – применять к доверию специальные правила фильтрации SID (если <code>--type=external</code> по умолчанию <code>yes</code> , если <code>--type=forest</code> по умолчанию <code>no</code>); <code>-U USERNAME</code> – имя пользователя
<code>domain trust modify <домен></code>	Изменить доверие домена или леса	
<code>domain trust delete <домен></code>	Удалить доверие домена или леса	Можно использовать следующие опции: <code>--delete-location=LOCATION</code> – где удалить объект доверенного домена (<code>local, both</code>); <code>-U USERNAME</code> – имя пользователя
<code>domain trust list</code>	Вывести список доверительных отношений домена	

Окончание таблицы 68

Команда	Описание	Примечание
domain trust show <домен>	Показать сведения о доверенном домене	
domain trust validate <домен>	Проверить доверие к домену	Можно использовать следующие опции: --validate-location=LOCATION – проверить объект доверенного домена (local, both); -U USERNAME – имя пользователя

10.5.2. Настройка DNS

Перед настройкой доверия необходимо убедиться, что серверы видят друг друга и правильно разрешают доменные имена.

10.5.2.1. Два домена Samba

Доменные имена, относящиеся к версии Samba, представлены в таблице 69.

Т а б л и ц а 69 – Исходные данные

Имя домена	Контроллер домена	IP-адрес	ОС контроллера домена	Версия Samba
TEST.ALT	dc1.test.alt	192.168.0.132	ALT Server SP	4.19.7
EXAMPLE.ALT	s1.example.alt	192.168.0.172	ALT Server SP	4.19.7

10.5.2.1.1. Настройка переадресации DNS на DC с BIND9_DLZ

Если используется dns_backend BIND9_DLZ, добавить информацию о зоне в конец файла /etc/bind/options.conf.

На контроллере домена dc1.test.alt добавить строки:

```
zone "example.alt" {
    type forward;
    forwarders { 192.168.0.172; };
};
```

На контроллере домена s1.example.alt:

```
zone "test.alt" {
    type forward;
    forwarders { 192.168.0.132; };
};
```

Перезапустить службу DNS:

```
# systemctl restart bind.service
```

Примечание. Если удаленный DNS-сервер не использует DNSSEC и включить проверку DNSSEC на удаленном DNS-сервере нельзя, можно отключить DNSSEC на сервере AD. Для этого необходимо в файл `/etc/bind/options.conf` в секцию `options` добавить параметр:

```
dnssec-validation no;
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

10.5.2.1.2. Настройка переадресации DNS на DC с SAMBA_INTERNAL

Если используется DC с `dns_backend SAMBA_INTERNAL`, самый простой способ заставить работать разрешение имен – настроить DNS-прокси между двумя доменами. DNS-прокси будет перенаправлять запрос между доменами и внешним DNS-серверами. В примере, в качестве DNS-прокси используется отдельный сервер (IP-адрес `192.168.0.150`) с настроенным `bind9`.

На каждом контроллере домена:

1) указать DNS-прокси, как сервер пересылки в

файле `/etc/samba/smb.conf` (в параметре `dns forwarder`). Например:

```
dns forwarder = 192.168.0.150 8.8.8.8
```

2) перезапустить службу `samba`:

```
# systemctl restart samba
```

На сервере `bind9` отредактировать файл `/etc/bind/options.conf`:

- отключить проверку DNSSEC, для этого в секцию `options` добавить параметр:

```
dnssec-validation no;
```

- в конец файла добавить информацию о зонах:

```
zone "example.alt" {
    type forward;
    forwarders { 192.168.0.172; };
};
```

```
zone "test.alt" {
    type forward;
    forwarders { 192.168.0.132; };
};
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

10.5.2.1.3. Проверка конфигурации DNS

Для проверки настройки следует убедиться, что на обоих контроллерах домена разрешаются SRV-записи:

- на контроллере домена dc1.test.alt:

```
# host -t srv _kerberos._tcp.example.alt
_kerberos._tcp.example.alt has SRV record 0 100 88
s1.example.alt.
# host -t srv _kerberos._tcp.test.alt
_kerberos._tcp.test.alt has SRV record 0 100 88 dc1.test.alt.
```

- на контроллере домена s1.example.alt:

```
# host -t srv _kerberos._tcp.example.alt
_kerberos._tcp.example.alt has SRV record 0 100 88
s1.example.alt.
# host -t srv _kerberos._tcp.test.alt
_kerberos._tcp.test.alt has SRV record 0 100 88 dc1.test.alt.
```

Проверить возможность получения билета Kerberos:

- на контроллере домена dc1.test.alt:

```
# kinit administrator@EXAMPLE.ALT
Password for administrator@EXAMPLE.ALT:
# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_eFyZ8Tr
Default principal: administrator@EXAMPLE.ALT

Valid starting          Expires                Service principal
25.04.2023             15:38:17              26.04.2023          01:38:17
krbtgt/EXAMPLE.ALT@EXAMPLE.ALT
renew until 26.04.2023 15:38:14
```

- на контроллере домена s1.example.alt:

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@TEST.ALT

Valid starting          Expires                Service principal
25.04.2023             15:17:50              26.04.2023          01:17:50
krbtgt/TEST.ALT@TEST.ALT
renew until 26.04.2023 15:17:46
```

ВАЖНО

realm должен быть записан заглавными буквами.

10.5.2.2. Samba DC и Windows Server с AD

Исходные данные Samba DC и Windows Server с AD представлены в таблице 70.

Т а б л и ц а 70 – Исходные данные

Имя домена	Контроллер домена	IP-адрес	ОС контроллера домена	Версия Samba
TEST.ALT	dc1.test.alt	192.168.0.132	ALT Server SP	4.19.7
WIN.ALT	DC1.win.alt	192.168.0.190	Windows Server 2012	

10.5.2.2.1. Windows Server с AD

На AD сервере создать сервер условной пересылки для зоны Samba домена.

В графическом интерфейсе:

- 1) открыть «Диспетчер DNS» (DNS Manager);
- 2) в разделе «Серверы условной пересылки» (Conditional Forwarders) добавить новый сервер пересылки, указав FQDN или IP-адрес сервера Samba (рис. 462);
- 3) сохранить настройки.

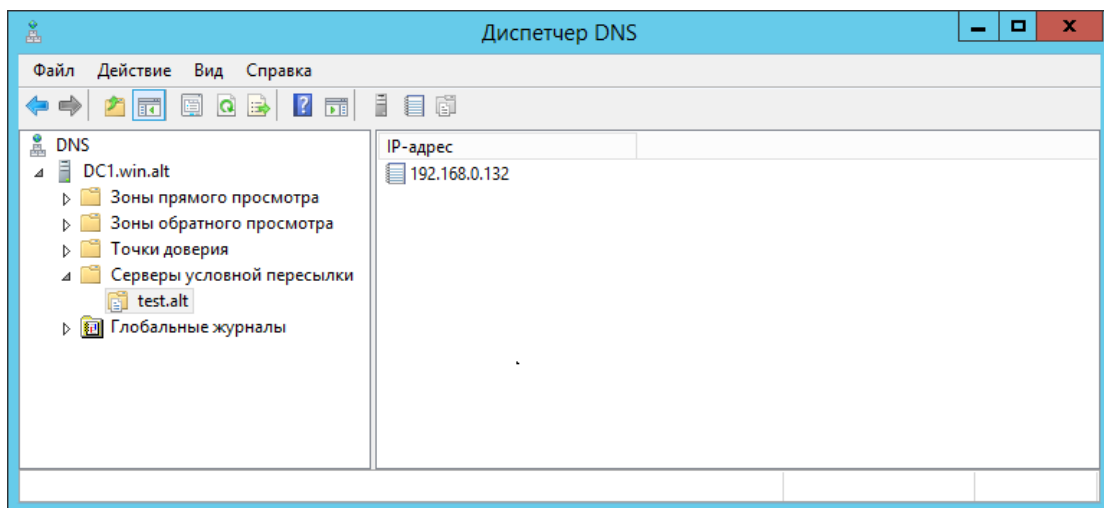


Рис. 462 – Окно «Диспетчер DNS»

В командной строке:

```
C:\> dnscmd 127.0.0.1 /ZoneAdd test.alt /Forwarder 192.168.0.132
DNS Server 127.0.0.1 created zone test.alt:
```

```
Command completed successfully
```

Или выполнить следующую команду в сеансе PowerShell, для настройки пересылки DNS:

```
PS C:\Windows\system32> Add-DnsServerConditionalForwarderZone -  
Name test.alt -MasterServers 192.168.0.132 -ReplicationScope Forest
```

10.5.2.2.2. Samba DC с BIND9_DLZ

Если используется `dns_backend BIND9_DLZ`, добавить в конец файла `/etc/bind/options.conf` (или `/etc/bind/ddns.conf`) строки:

```
zone "win.alt" {  
    type forward;  
    forwarders { 192.168.0.190; };  
};
```

и перезапустить службу DNS:

```
# systemctl restart bind.service
```

Примечание. Если удаленный DNS-сервер не использует DNSSEC и включить проверку DNSSEC на удаленном DNS-сервере нельзя, можно отключить DNSSEC на сервере AD. Для этого необходимо в файл `/etc/bind/options.conf` в секцию `options` добавить параметр:

```
dnssec-validation no;
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

10.5.2.2.3. Samba DC с SAMBA_INTERNAL

Если используется DC с `dns_backend SAMBA_INTERNAL`, самый простой способ заставить работать разрешение имен – настроить DNS-прокси между двумя доменами. DNS-прокси будет перенаправлять запрос между доменами и внешним DNS-серверами. В примере, в качестве DNS-прокси используется отдельный сервер (IP-адрес 192.168.0.150) с настроенным bind9.

На контроллере домена:

- указать DNS-прокси, как сервер пересылки в файле `/etc/samba/smb.conf` (в параметре `dns forwarder`). Например:

```
dns forwarder = 192.168.0.150 8.8.8.8
```

- перезапустить службу samba:

```
# systemctl restart samba
```

На сервере bind9 отредактировать файл /etc/bind/options.conf:

- отключить проверку DNSSEC, для этого в секцию options добавить параметр:

```
dnssec-validation no;
```

- в конец файла добавить информацию о зонах:

```
zone "win.alt" {
    type forward;
    forwarders { 192.168.0.190; };
};
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

10.5.2.2.4. Проверка конфигурации DNS

Перед настройкой доверия необходимо убедиться, что серверы могут разрешать себя и друг друга.

На Samba DC:

1) запись, отвечающая за работу сервисов Kerberos через UDP и LDAP через TCP:

```
# dig +short -t SRV _kerberos._udp.test.alt
0 100 88 dc1.test.alt.
# dig +short -t SRV _ldap._tcp.test.alt
0 100 389 dc1.test.alt.
```

В выводе команд должен быть отображен список всех серверов;

2) наличие записей для работы сервисов AD на DNS-сервере Samba:

```
# dig +short -t SRV _kerberos._tcp.dc._msdcs.win.alt
0 100 88 dc1.win.alt.
# dig +short -t SRV _ldap._tcp.dc._msdcs.win.alt
0 100 389 dc1.win.alt.
```

3) проверить возможность получения билета Kerberos:

```
# kinit administrator@WIN.ALT
Password for administrator@WIN.ALT:
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@WIN.ALT
```

```
Valid starting          Expires                Service principal
27.04.2023             17:42:28              28.04.2023           03:42:28
krbtgt/WIN.ALT@WIN.ALT
    renew until 28.04.2023 17:42:25
```

Проверить наличие записей DNS-сервере AD:

1) запустить утилиту nslookup.exe для поиска служебных записей:

```
C:\> nslookup.exe
> set type=SRV
```

2) ввести доменное имя для служебных записей Kerberos через UDP и LDAP через TCP:

```
> _kerberos._udp.test.alt
_kerberos._udp.test.alt      SRV service location:
    priority                  = 0
    weight                    = 100
    port                      = 88
    svr hostname              = dc1.test.alt
...
test.alt
    primary name server = dc1.test.alt
    responsible mail addr = hostmaster.test.alt
    serial = 7
    refresh = 900 (15 mins)
    retry = 600 (10 mins)
    expire = 86400 (1 days)
    default TTL = 3600 (1 hours)
> _ldap._tcp.test.alt
_ldap._tcp.test.alt          SRV service location:
    priority                  = 0
    weight                    = 100
    port                      = 389
    svr hostname              = dc1.test.alt
...
```

10.5.3. Создание двухстороннего транзитивного подключения

10.5.3.1. Два домена Samba

На контроллере домена dc1.test.alt:

```
# samba-tool domain trust create EXAMPLE.ALT --type=forest \
--direction=both --create-location=both -U administrator@EXAMPLE.ALT
LocalDomain  Netbios[TEST]      DNS[test.alt]      SID[S-1-5-21-1455776928-
3410124986-2843404052]
RemoteDC     Netbios[S1]            DNS[s1.example.alt]
ServerType[PDC, GC, LDAP, DS, KDC, TIMESERV, CLOSEST, WRITABLE, GOOD_TIMESERV,
FULL_SECRET_DOMAIN_6]
Password for [administrator@EXAMPLE.ALT]:
RemoteDomain Netbios[EXAMPLE]      DNS[example.alt]      SID[S-1-5-21-
3274802069-598906262-3677769431]
Creating remote TDO.
Remote TDO created.
Setting supported encryption types on remote TDO.
Creating local TDO.
```

ЛКНВ.11100-01 90 03

```

Local TDO created
Setting supported encryption types on local TDO.
Setup local forest trust information...
Namespaces[2] TDO[example.alt]:
TLN: Status[Enabled]                      DNS[*example.alt]
DOM: Status[Enabled]                      DNS[example.alt]
Netbios[EXAMPLE] SID[S-1-5-21-3274802069-598906262-3677769431]
Setup remote forest trust information...
Namespaces[2] TDO[test.alt]:
TLN: Status[Enabled]                      DNS[*test.alt]
DOM: Status[Enabled]                      DNS[test.alt] Netbios[TEST]
SID[S-1-5-21-1455776928-3410124986-2843404052]
Validating outgoing trust...
OK: LocalValidation: DC[\\s1.example.alt] CONNECTION[WERR_OK]
TRUST[WERR_OK] VERIFY_STATUS_RETURNED
Validating incoming trust...
OK: RemoteValidation: DC[\\dc1.test.alt] CONNECTION[WERR_OK]
TRUST[WERR_OK] VERIFY_STATUS_RETURNED
Success

```

ВАЖНО

Для входа в доверенный домен через SSSD надо использовать тип связи external, а не forest.

Проверка доверия:**- просмотр доверия с dc1.test.alt:**

```

[root@dc1 ~]# samba-tool domain trust show EXAMPLE.ALT

LocalDomain Netbios[TEST] DNS[test.alt] SID[S-1-5-21-1455776928-
3410124986-2843404052]
TrustedDomain:

NetbiosName: EXAMPLE
DnsName: example.alt
SID: S-1-5-21-3274802069-598906262-3677769431
Type: 0x2 (UPLEVEL)
Direction: 0x3 (BOTH)
Attributes: 0x8 (FOREST_TRANSITIVE)
PosixOffset: 0x00000000 (0)
kerb_EncTypes: 0x18
(AES128_CTS_HMAC_SHA1_96,AES256_CTS_HMAC_SHA1_96)
Namespaces[2] TDO[example.alt]:
TLN: Status[Enabled]                      DNS[*example.alt]
DOM: Status[Enabled]                      DNS[example.alt]
Netbios[EXAMPLE] SID[S-1-5-21-3274802069-598906262-3677769431]

```

- просмотр доверия с s1.example.alt:

```

[root@s1 ~]# samba-tool domain trust show TEST.ALT

LocalDomain Netbios[EXAMPLE] DNS[example.alt] SID[S-1-5-21-
3274802069-598906262-3677769431]

```


ЛКНВ.11100-01 90 03

TrustedDomain:

```

NetbiosName:      TEST
DnsName:          test.alt
SID:              S-1-5-21-1455776928-3410124986-2843404052
Type:             0x2 (UPLEVEL)
Direction:        0x3 (BOTH)
Attributes:        0x8 (FOREST_TRANSITIVE)
PosixOffset:      0x00000000 (0)
kerb_EncTypes:    0x18
                  (AES128_CTS_HMAC_SHA1_96,AES256_CTS_HMAC_SHA1_96)
Namespaces[2] TDO[test.alt]:
TLN: Status[Enabled]          DNS[*.test.alt]
DOM: Status[Enabled]          DNS[test.alt] Netbios[TEST]
SID[S-1-5-21-1455776928-3410124986-2843404052]

```

- список трастов:

```

[root@dc1 ~]# samba-tool domain trust list
Type[Forest]   Transitive[Yes] Direction[BOTH]   Name[example.alt]

```

В разных доменах могут быть разные результаты. Результат зависит от типа траста, который установлен с этим доменом.

Если после настройки доверия возникли проблемы с доступом пользователей из трастового домена в свой домен, тогда следует проверить, действительно ли установлен траст:

```

[root@dc1 ~]# samba-tool domain trust validate EXAMPLE.ALT -
Uadministrator@EXAMPLE.ALT
LocalDomain Netbios[TEST] DNS[test.alt] SID[S-1-5-21-1455776928-
3410124986-2843404052]
LocalTDO Netbios[EXAMPLE] DNS[example.alt] SID[S-1-5-21-
3274802069-598906262-3677769431]
OK: LocalValidation: DC[\\s1.example.alt] CONNECTION[WERR_OK]
TRUST[WERR_OK] VERIFY_STATUS_RETURNED
OK: LocalRediscover: DC[\\s1.example.alt] CONNECTION[WERR_OK]
RemoteDC Netbios[S1] DNS[s1.example.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIME
SERV,FULL_SECRET_DOMAIN_6]
Password for [administrator@EXAMPLE.ALT]:
OK: RemoteValidation: DC[\\dc1.test.alt] CONNECTION[WERR_OK]
TRUST[WERR_OK] VERIFY_STATUS_RETURNED
OK: RemoteRediscover: DC[\\dc1.test.alt] CONNECTION[WERR_OK]

```

10.5.3.2. Samba DC и Windows Server с AD

Настройка на стороне Windows:

- 1) открыть «Диспетчер серверов», выбрать «Средства» → «Active Directory – домены и доверие» (рис. 463);

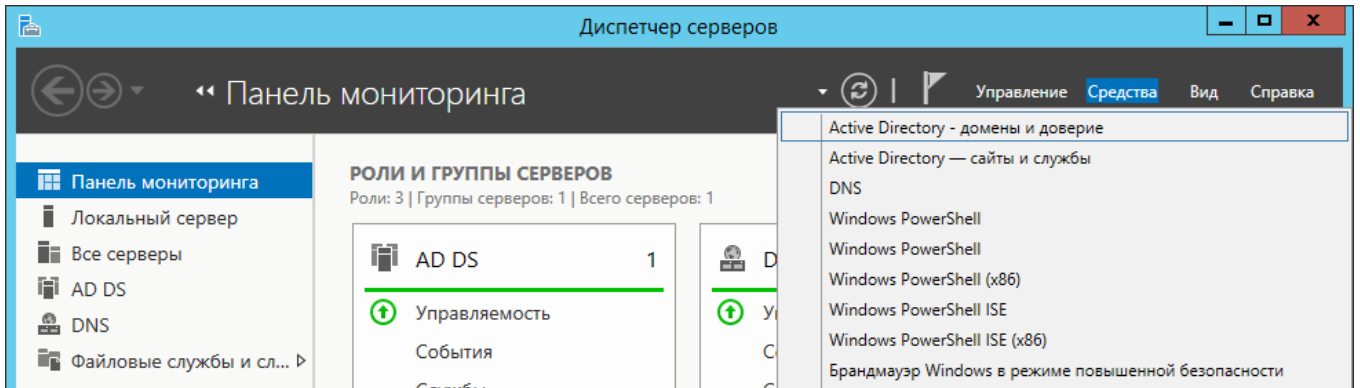


Рис. 463 – Окно «Диспетчер серверов»

- 2) в открывшемся окне в контекстном меню домена выбрать пункт «Свойства» (рис. 464);

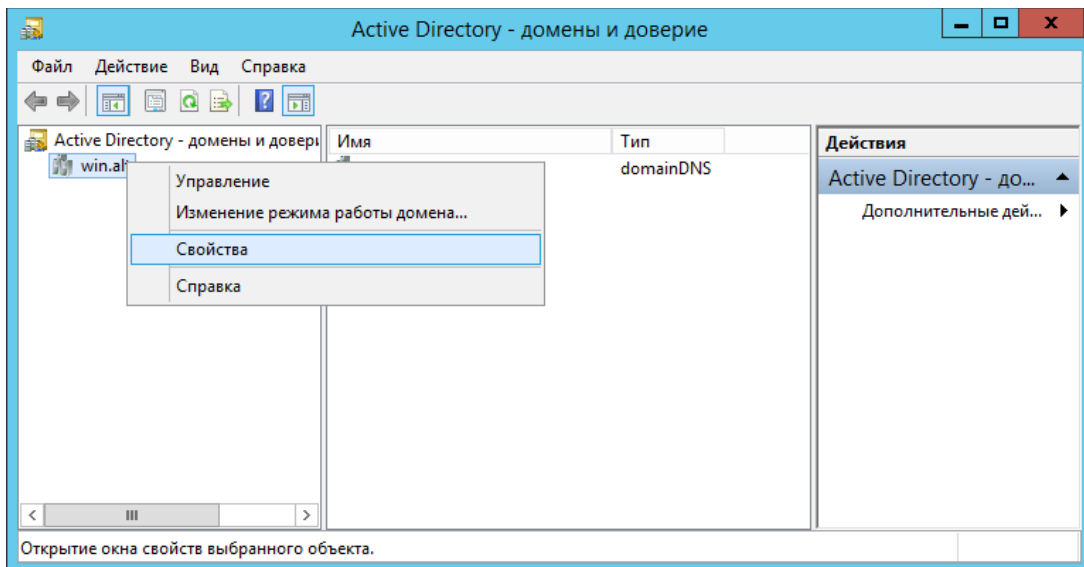


Рис. 464 – Окно «Active Directory – домены и доверие»

- 3) откроется окно свойств домена. Необходимо перейти во вкладку «Отношения доверия» и нажать кнопку «Создать отношение доверия...» (рис. 465);

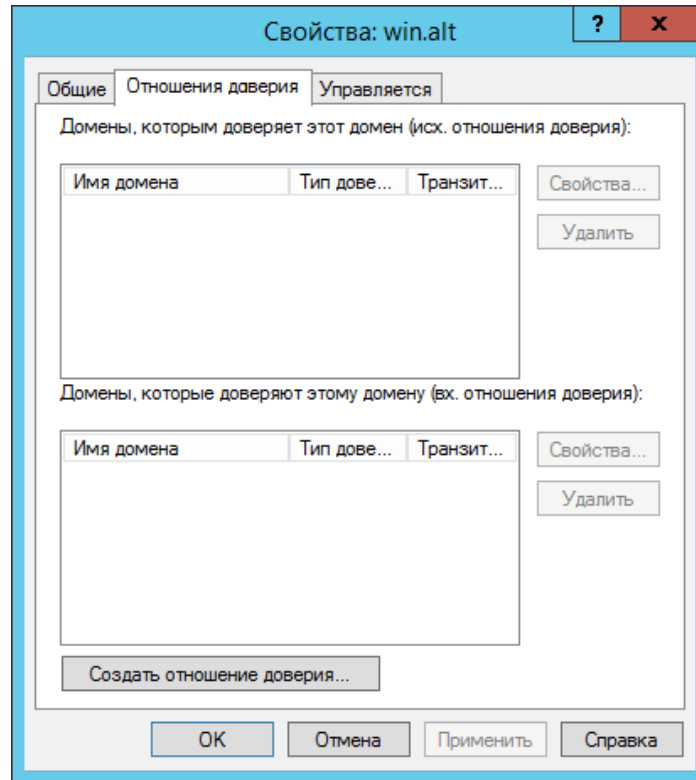


Рис. 465 – Окно свойств домена

4) будет запущен «Мастер создания отношения доверия» (рис. 466);

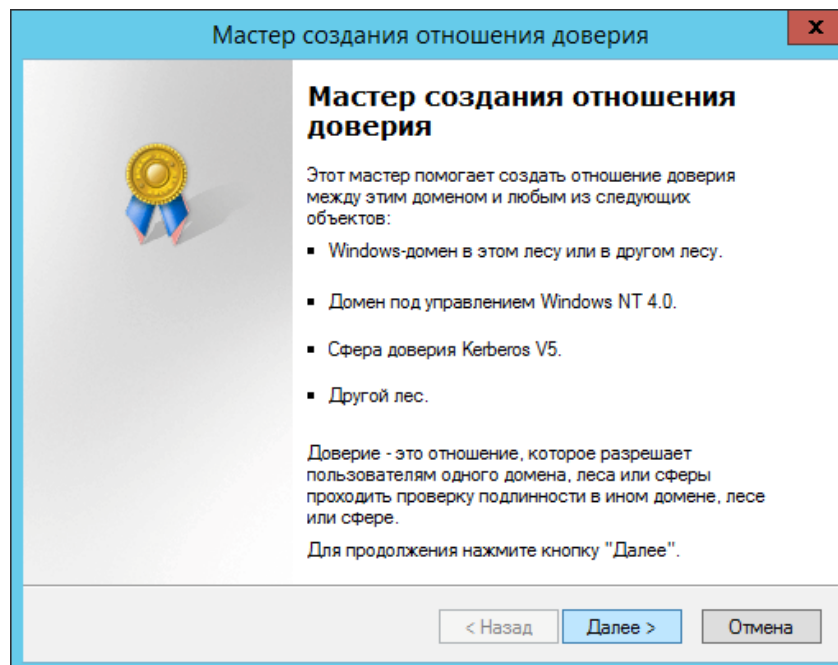


Рис. 466 – Окно «Мастер создания отношения доверия»

5) на втором шаге создания отношения доверия необходимо ввести имя домена Samba DC (в примере TEST.ALT) (рис. 467);

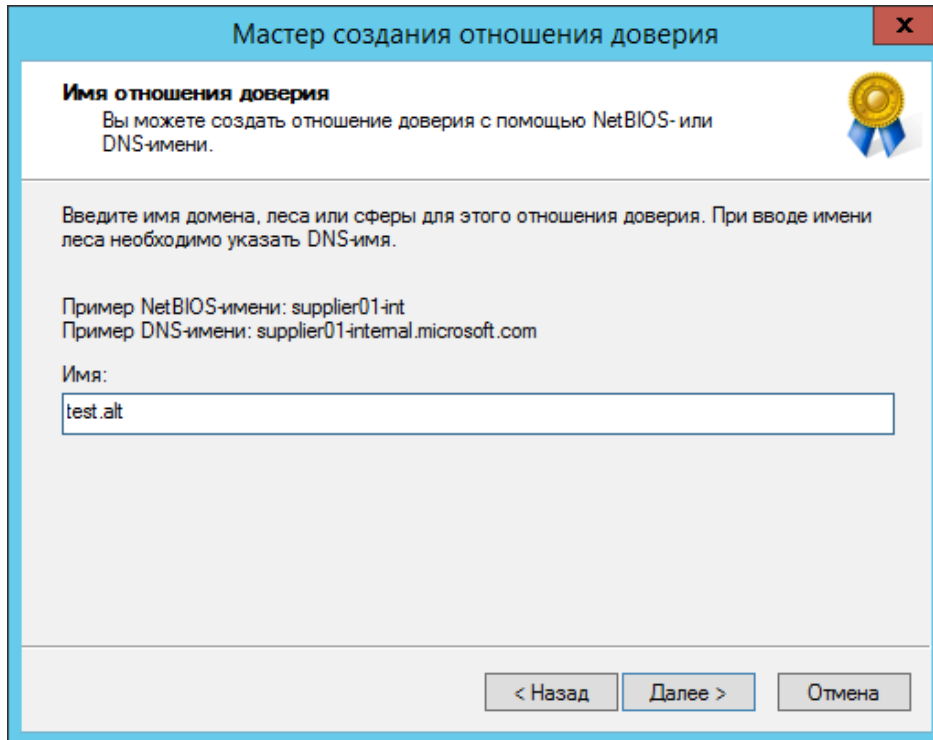


Рис. 467 – Окно ввода имени домена Samba DC

б) на следующем шаге следует выбрать тип доверия (рис. 468);

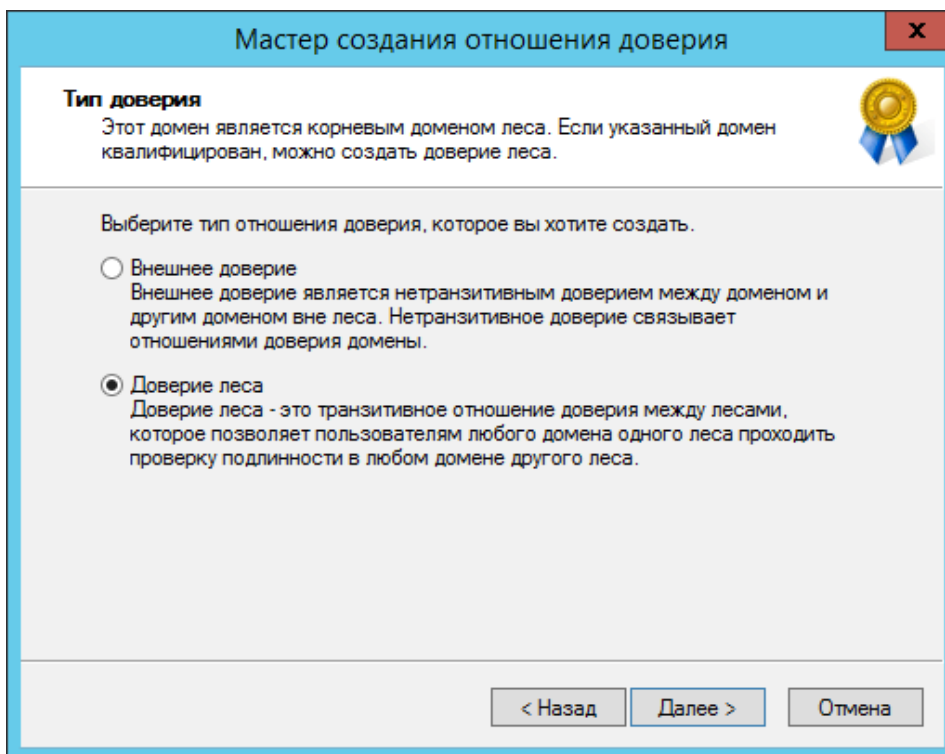


Рис. 468 – Окно выбора типа доверия

7) далее выбирается направление доверия (рис. 469);

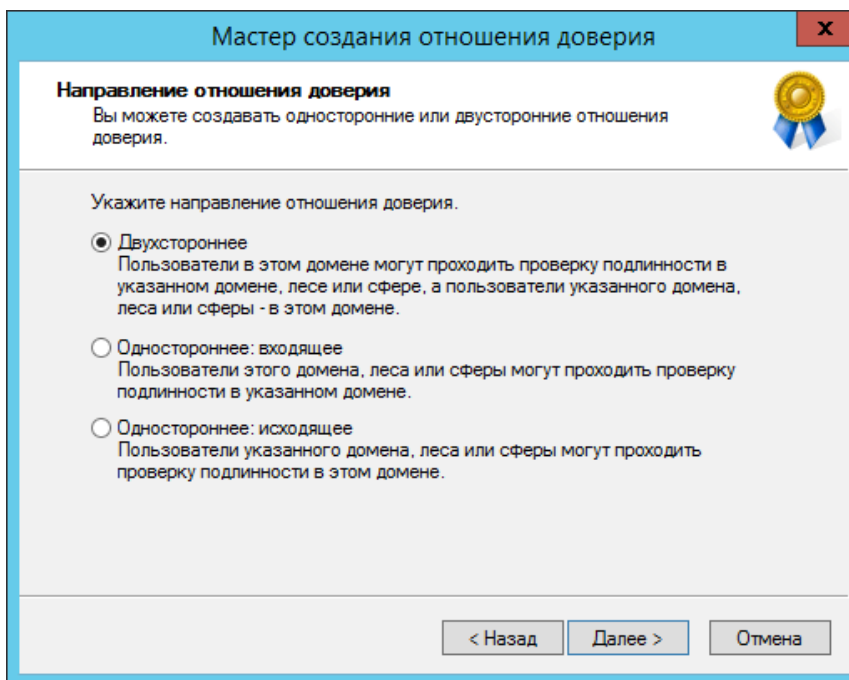


Рис. 469 – Окно выбора направления доверия

- 8) в открывшемся окне «Стороны отношения доверия» нужно выбрать, на каком из доменов применяется настройка. Если есть права администратора для обоих доменов, можно выбрать пункт «Для данного и указанного домена» (рис. 470);

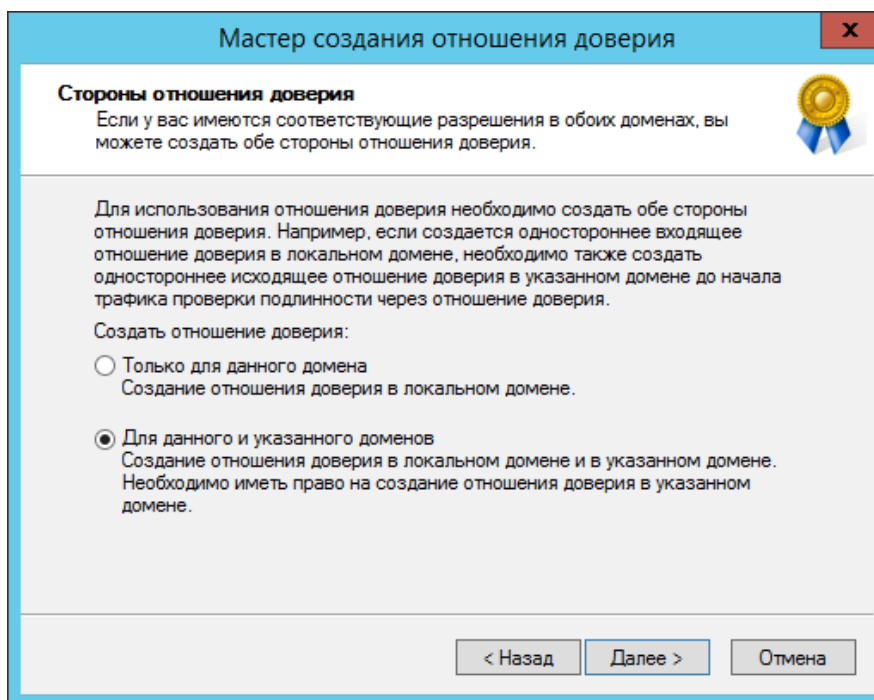


Рис. 470 – Стороны отношения доверия

Примечание. Если выбрать параметр «Только для данного домена» (рис. 471), необходимо задать «Пароль отношения доверия» (Trust Secret Key), который в дальнейшем будет использоваться при создании доверительного отношения на стороне Samba DC (рис. 472).

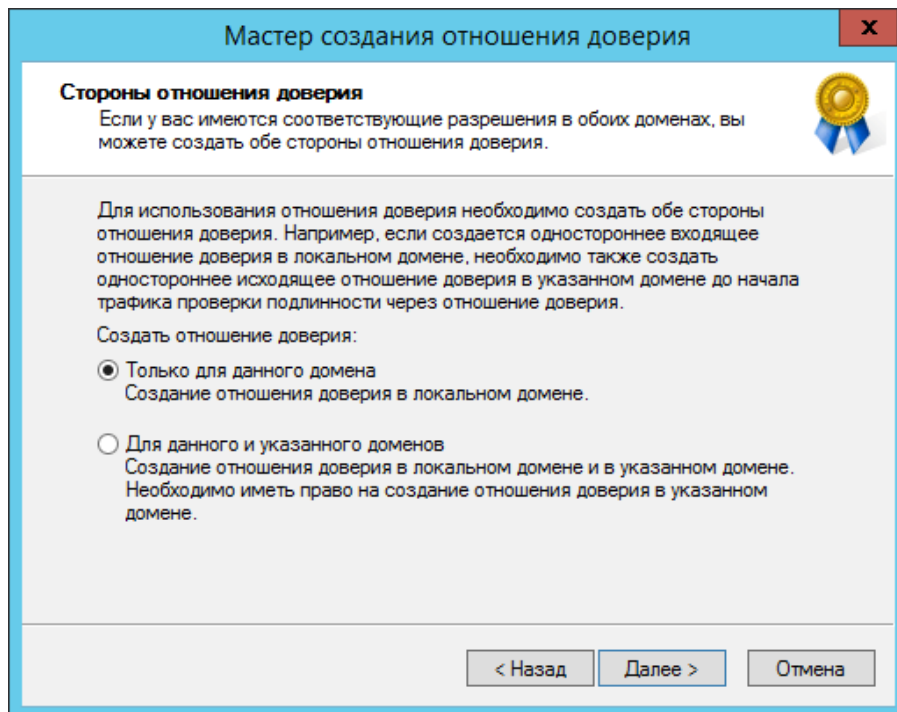


Рис. 471 – Стороны отношения доверия «Только для данного домена»

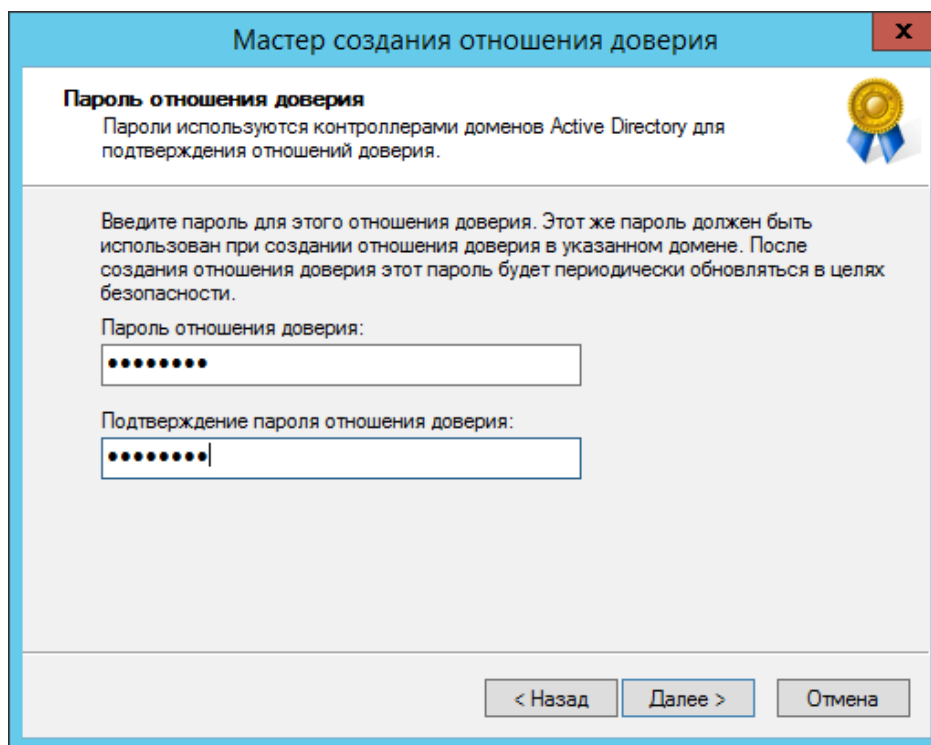


Рис. 472 – Окно «Пароль отношения доверия»

- 9) на следующем этапе мастер свяжется с удаленным доменом (если он доступен), и запросит имя и пароль пользователя с правами установки доверительных отношений в домене (рис. 473);

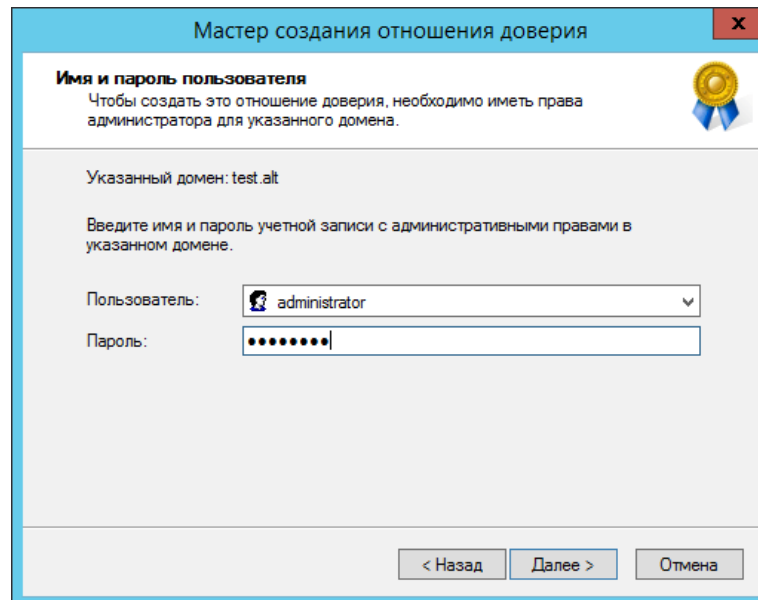


Рис. 473 – Окно ввода имени пользователя и пароля

- 10) далее на шаге «Уровень проверки подлинности исходящего доверия – Локальный лес» следует выбрать «Проверка подлинности в лесу» (рис. 474);

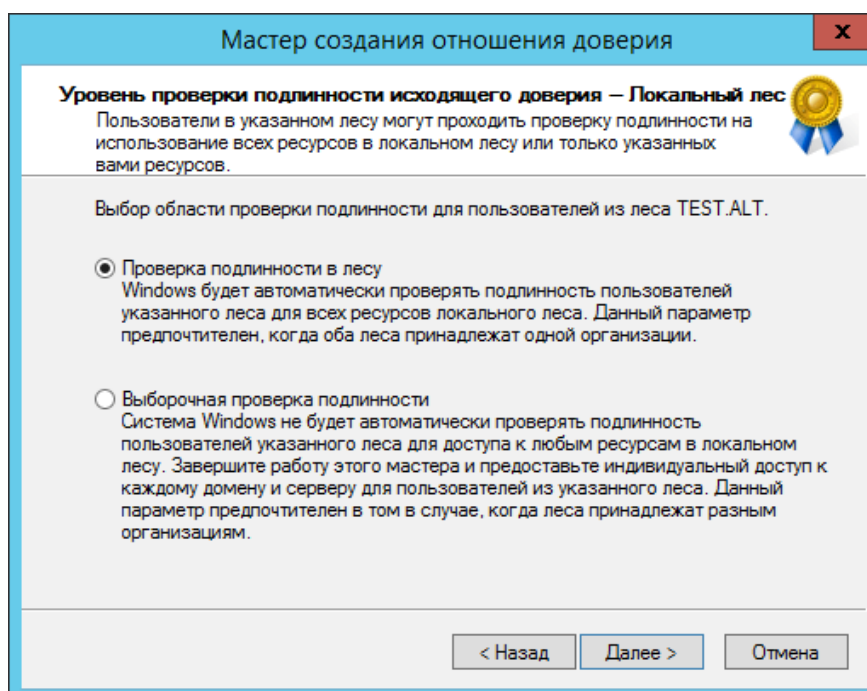


Рис. 474 – Окно выбора области проверки подлинности

- 11) на шаге «Уровень проверки подлинности исходящего доверия – Указанный лес» также следует выбрать пункт «Проверка подлинности в лесу»;
- 12) в окне «Выбор доверия завершено» мастер выдаст уведомление о том, что готов создать новое отношение доверия, и покажет краткую сводку с выбранными параметрами. Если согласиться с параметрами, то должно появиться уведомление о том, что создание доверия завершено (рис. 475);

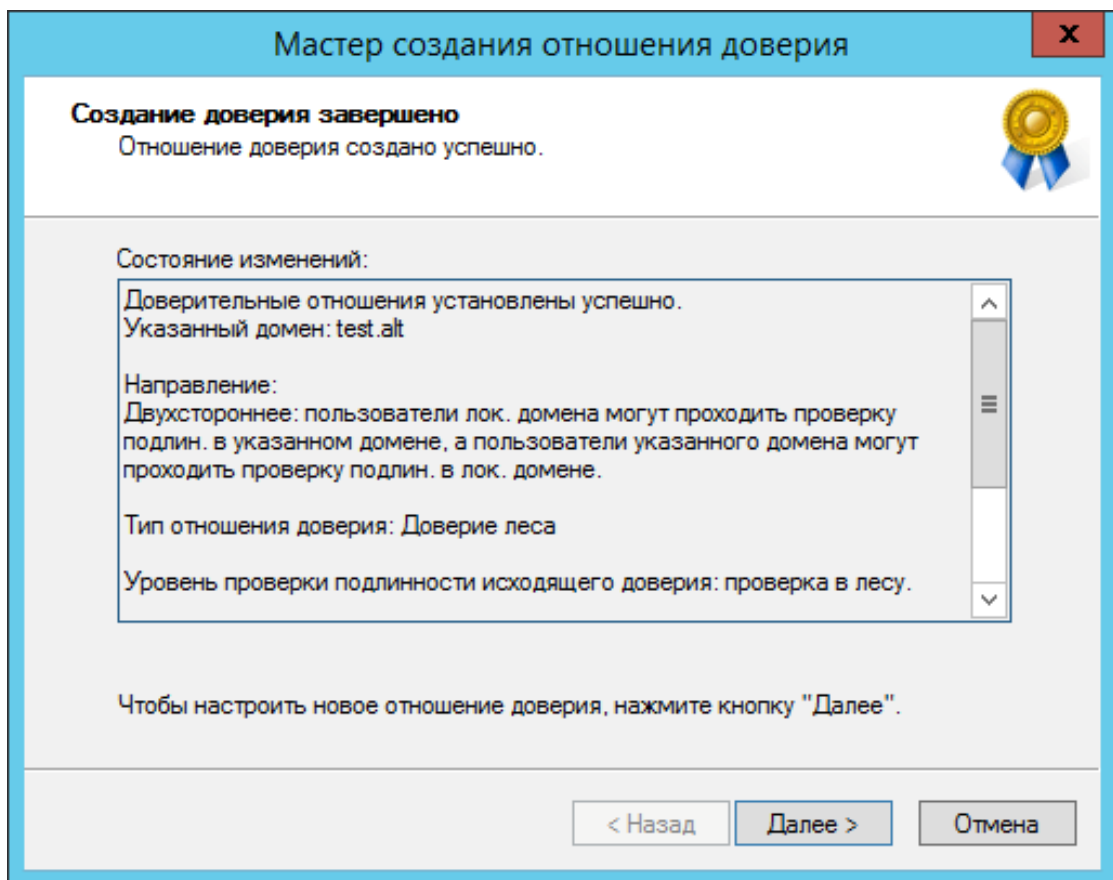


Рис. 475 – Окно «Создание доверия завершено»

- 13) после нажатия кнопки «Далее» появится окно «Подтверждение исходящего доверия», а после него «Подтверждение входящего доверия». Здесь можно оставить выбранным пункт «Нет, не подтверждаю это исходящее/входящее отношение доверия», так как на стороне Samba DC доверие еще не создавалось (рис. 476).

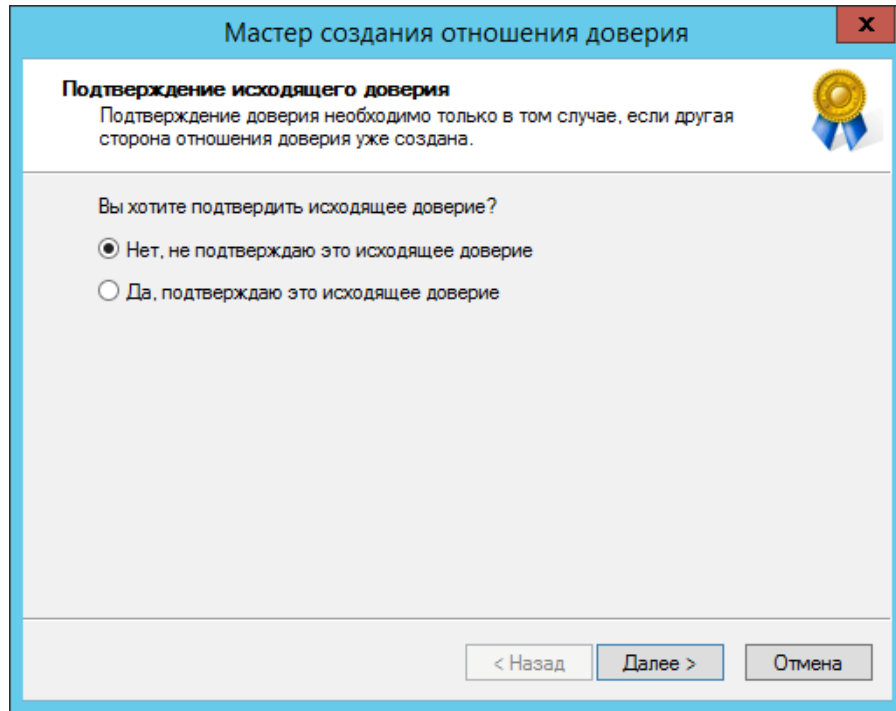


Рис. 476 – Окно подтверждения доверия

В результате будут получены двухсторонние доверительные отношения между доменами (рис. 477).

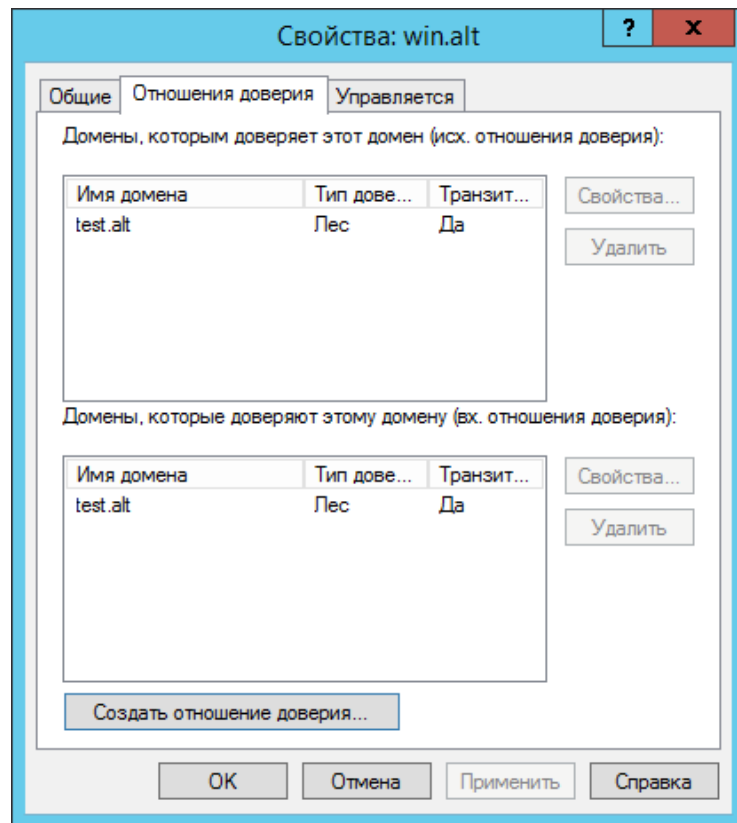


Рис. 477 – Окно установленных доверительных отношения между доменами

На стороне Samba DC для создания доверия необходимо выполнить команду:

```
# samba-tool domain trust create win.alt --type=forest \
--direction=both --create-location=both -Uadministrator@WIN
```

ВАЖНО

Для входа в доверенный домен через SSSD надо использовать тип связи external, а не forest.

При появлении запроса введите пароль администратора.

Если все настроено верно, будет установлено доверие к домену AD.

```
LocalDomain Netbios[TEST] DNS[test.alt] SID[S-1-5-21-3848605173-
1839566900-710408900]
RemoteDC Netbios[DC1] DNS[DC1.win.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIME
SERV,FULL_SECRET_DOMAIN_6,ADS_WEB_SERVICE,DS_8, __unknown_00008000
__]
Password for [administrator@WIN]:
RemoteDomain Netbios[WIN] DNS[win.alt] SID[S-1-5-21-212759798-
1661061060-862600140]
Creating local TDO.
Local TDO created
Setting supported encryption types on local TDO.
Setup local forest trust information...
Namespaces[2] TDO[win.alt]:
TLN: Status[Enabled] DNS[*win.alt]
DOM: Status[Enabled] DNS[win.alt] Netbios[WIN]
SID[S-1-5-21-212759798-1661061060-862600140]
Validating outgoing trust...
OK: LocalValidation: DC[\\DC1.win.alt] CONNECTION[WERR_OK]
TRUST[WERR_OK] VERIFY_STATUS_RETURNED
Validating incoming trust...
OK: RemoteValidation: DC[\\dc1.test.alt] CONNECTION[WERR_OK]
TRUST[WERR_OK] VERIFY_STATUS_RETURNED
Success.
```

В случае использования Trust Secret Key в параметре --create-location нужно заменить опцию both на local, Samba DC прежде чем создать доверительные отношения сначала запросит Trust Key, созданный ранее при настройке в Windows.

```
# samba-tool domain trust create win.alt --type=forest --
direction=both --create-location=local -Uadministrator@WIN

New Incoming Trust Password:
Retype Incoming Trust Password:
New Outgoing Trust Password:
Retype Outgoing Trust Password:
```

ЛКНВ.11100-01 90 03

```
LocalDomain Netbios[TEST] DNS[test.alt] SID[S-1-5-21-3848605173-1839566900-710408900]
RemoteDC Netbios[DC1] DNS[DC1.win.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,...]
Password for [administrator@WIN]:
...
```

Проверка доверия с dc1.test.alt:**- просмотр доверия:**

```
# samba-tool domain trust show WIN.ALT

LocalDomain Netbios[TEST] DNS[test.alt] SID[S-1-5-21-3848605173-1839566900-710408900]
TrustedDomain:

NetbiosName: WIN
DnsName: win.alt
SID: S-1-5-21-212759798-1661061060-862600140
Type: 0x2 (UPLEVEL)
Direction: 0x3 (BOTH)
Attributes: 0x8 (FOREST_TRANSITIVE)
PosixOffset: 0x00000000 (0)
kerb_EncTypes: 0x18
(AES128_CTS_HMAC_SHA1_96,AES256_CTS_HMAC_SHA1_96)
Namespaces[2] TDO[win.alt]:
TLN: Status[Enabled] DNS[*win.alt]
DOM: Status[Enabled] DNS[win.alt] Netbios[WIN]
SID[S-1-5-21-212759798-1661061060-862600140]
```

- список трастов:

```
# samba-tool domain trust list
Type[Forest] Transitive[Yes] Direction[BOTH] Name[win.alt]
```

В разных доменах могут быть разные результаты. Результат зависит от типа траста, который установлен с этим доменом.

Если после настройки доверия возникли проблемы с доступом пользователей из трастового домена в свой домен, тогда следует проверить, действительно ли установлен траст:

```
# samba-tool domain trust validate win.alt -Uadministrator@WIN
LocalDomain Netbios[TEST] DNS[test.alt] SID[S-1-5-21-3848605173-1839566900-710408900]
LocalTDO Netbios[WIN] DNS[win.alt] SID[S-1-5-21-212759798-1661061060-862600140]
OK: LocalValidation: DC[\\DC1.win.alt] CONNECTION[WERR_OK]
TRUST[WERR_OK] VERIFY_STATUS_RETURNED
OK: LocalRediscover: DC[\\DC1.win.alt] CONNECTION[WERR_OK]
RemoteDC Netbios[DC1] DNS[DC1.win.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIME]
```

```
SERV,FULL_SECRET_DOMAIN_6,ADS_WEB_SERVICE,DS_8, __unknown_00008000
__]
Password for [administrator@WIN]:
OK: RemoteValidation: DC[\\dc2.test.alt] CONNECTION[WERR_OK]
TRUST[WERR_OK] VERIFY_STATUS_RETURNED
OK: RemoteRediscover: DC[\\dc2.test.alt] CONNECTION[WERR_OK]
```

10.5.4. Управление пользователями и группами

После настройки доверия можно назначать пользователей и группы из доверяющего домена в группу доверенного домена. Так как настроено двустороннее доверие, можно назначать пользователей и группы в обоих направлениях.

Примечание. Предварительно необходимо создать несколько пользователей и групп в обоих доменах.

10.5.4.1. Список пользователей и групп

С помощью команды `wbinfo` нельзя получить список пользователей и групп из доверяющего домена, можно получить список пользователей и групп только из своего домена. Пример:

- команды выполняются на контроллере домена `dc1.test.alt`:

```
# wbinfo -u --domain=EXAMPLE.ALT
# wbinfo -u --domain=TEST.ALT
TEST\administrator
TEST\guest
TEST\krbtgt
TEST\dns-dc1
TEST\ivanov
```

- команды выполняются на контроллере домена `s1.example.alt`:

```
# wbinfo -u --domain=EXAMPLE.ALT
EXAMPLE\administrator
EXAMPLE\guest
EXAMPLE\krbtgt
EXAMPLE\dns-s1
EXAMPLE\kim
# wbinfo -u --domain=TEST.ALT
```

Для получения списка всех пользователей можно выполнить LDAP-запрос с помощью команды `samba-tool`. Пример получения списка пользователей из обоих доменов на контроллере домена `dc1.test.alt`:

```
# samba-tool user list -H ldap://s1 -Uadministrator@EXAMPLE.ALT
Password for [administrator@EXAMPLE.ALT]:
```

```

dns-s1
krbtgt
Administrator
Guest
kim
# samba-tool user list -H ldap://dc1 -Uadministrator@TEST.ALT
Password for [administrator@TEST.ALT]:
dns-dc1
krbtgt
Guest
Administrator
ivanov

```

Получение дополнительной информации о доменах (в примере команды выполняются на контроллере домена dc1.test.alt):

```

# wbinfo --all-domains
BUILTIN
TEST
EXAMPLE

# wbinfo --own-domain
TEST

# wbinfo --trusted-domains
BUILTIN
TEST
EXAMPLE

# wbinfo --online-status
BUILTIN : active connection
TEST : active connection
EXAMPLE : active connection

```

Получение SID пользователей и групп (в примере команды выполняются на контроллере домена dc1.test.alt):

```

# wbinfo -n TEST\\ivanov
S-1-5-21-1455776928-3410124986-2843404052-1105 SID_USER (1)

# wbinfo -n EXAMPLE\\kim
S-1-5-21-3274802069-598906262-3677769431-1104 SID_USER (1)

# wbinfo -n TEST\\office
S-1-5-21-1455776928-3410124986-2843404052-1107 SID_DOM_GROUP (2)

# wbinfo -n EXAMPLE\\office2
S-1-5-21-3274802069-598906262-3677769431-1107 SID_DOM_GROUP (2)

# wbinfo -i TEST\\ivanov
TEST.ALT\ivanov:*:3000022:100::/home/TEST.ALT/ivanov:/bin/false

# wbinfo -i EXAMPLE\\kim
EXAMPLE\kim:*:3000020:3000021::/home/EXAMPLE/kim:/bin/false

```

10.5.4.2. Тестирование аутентификации

С помощью команды `wbinfo` можно протестировать процесс аутентификации разных пользователей из обоих доменов.

`wbinfo` попытается авторизовать пользователя. Первой проверкой будет аутентификация по паролю с открытым текстом. Этот тип аутентификации применяется, когда пользователь входит в систему локально (`plaintext` не означает, что пароль будет отправлен без шифрования, это просто название процесса входа в систему). Вторая проверка – аутентификация по паролю запрос/ответ. Этот тип аутентификации использует NTLM или Kerberos.

Проверка методов аутентификации (в примере команды выполняются на контроллере домена `dc1.test.alt`):

```
# wbinfo -a TEST\\ivanov
Enter TEST\ivanov's password:
plaintext password authentication succeeded
Enter TEST\ivanov's password:
challenge/response password authentication succeeded

# wbinfo -a EXAMPLE\\kim
Enter EXAMPLE\kim's password:
plaintext password authentication succeeded
Enter EXAMPLE\kim's password:
challenge/response password authentication succeeded
```

Посмотреть какие контроллеры домена отвечают за аутентификацию:

```
# wbinfo --ping-dc
checking the NETLOGON for domain[TEST] dc connection to
"dc1.test.alt" succeeded

# wbinfo --ping-dc --domain=EXAMPLE.ALT
checking the NETLOGON for domain[EXAMPLE.ALT] dc connection to
"s1.example.alt" succeeded
```

Назначение пользователей и групп из доверенных доменов в группу доверяющего домена:

```
# wbinfo -n EXAMPLE\\kim
S-1-5-21-3274802069-598906262-3677769431-1104 SID_USER (1)

# samba-tool group addmembers office S-1-5-21-3274802069-
598906262-3677769431-1104
Added members to group office
```

```
# wbinfo -n EXAMPLE\\office2
S-1-5-21-3274802069-598906262-3677769431-1107 SID_DOM_GROUP (2)
```

```
# samba-tool group addmembers office S-1-5-21-3274802069-
598906262-3677769431-1107
Added members to group office
```

```
# samba-tool group listmembers office
S-1-5-21-3274802069-598906262-3677769431-1104
ivanov
S-1-5-21-3274802069-598906262-3677769431-1107
```

10.5.4.3. Просмотр доверия в Windows

Модуль RSAT (см. п. 10.4.2.3) «Active Directory – домены и доверие» (Active Directory – Domain and Trusts) позволяет проверить состояние отношений доверия между доменами (рис. 478).

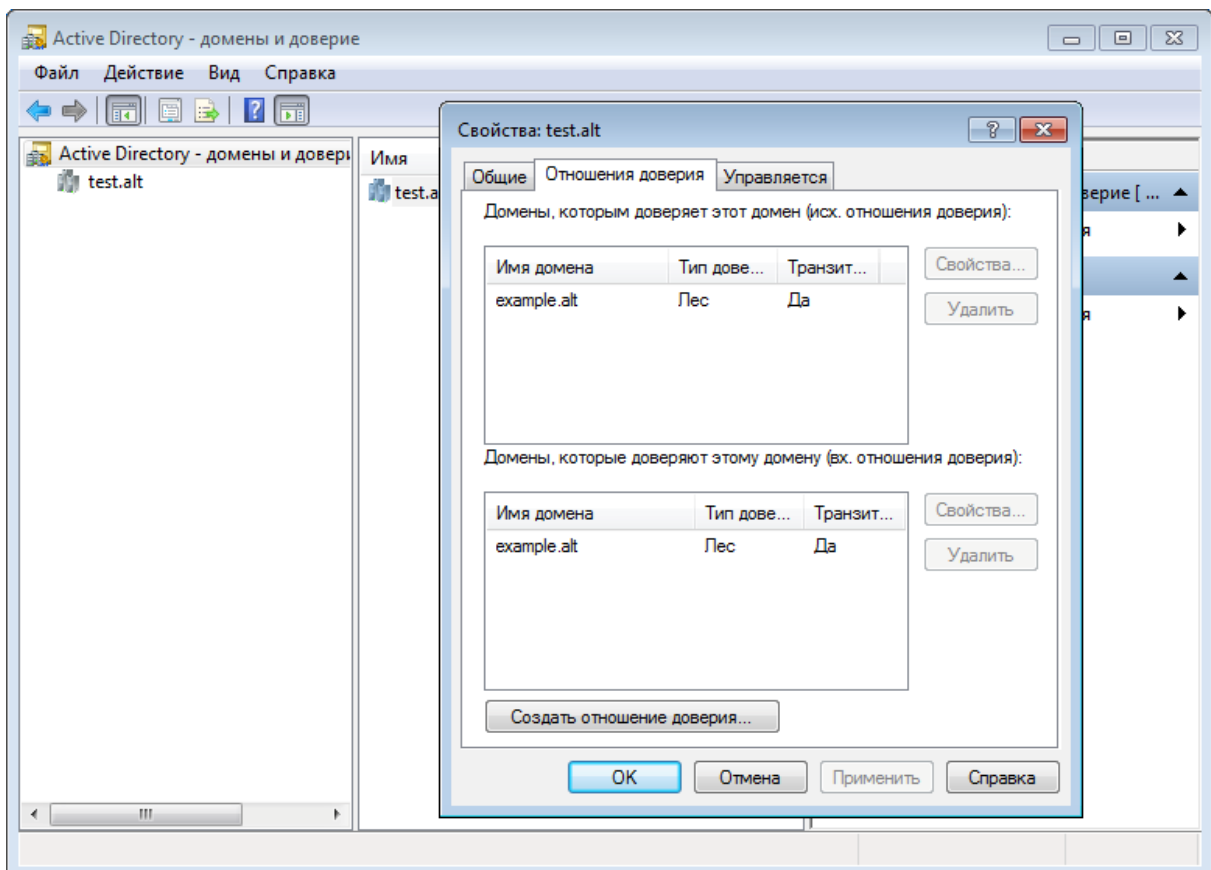


Рис. 478 – Модуль RSAT «Active Directory – домены и доверие»

В модуле RSAT «Active Directory – пользователи и компьютеры» (Active Directory – Users and Computers) можно просмотреть список пользователей группы (рис. 479).

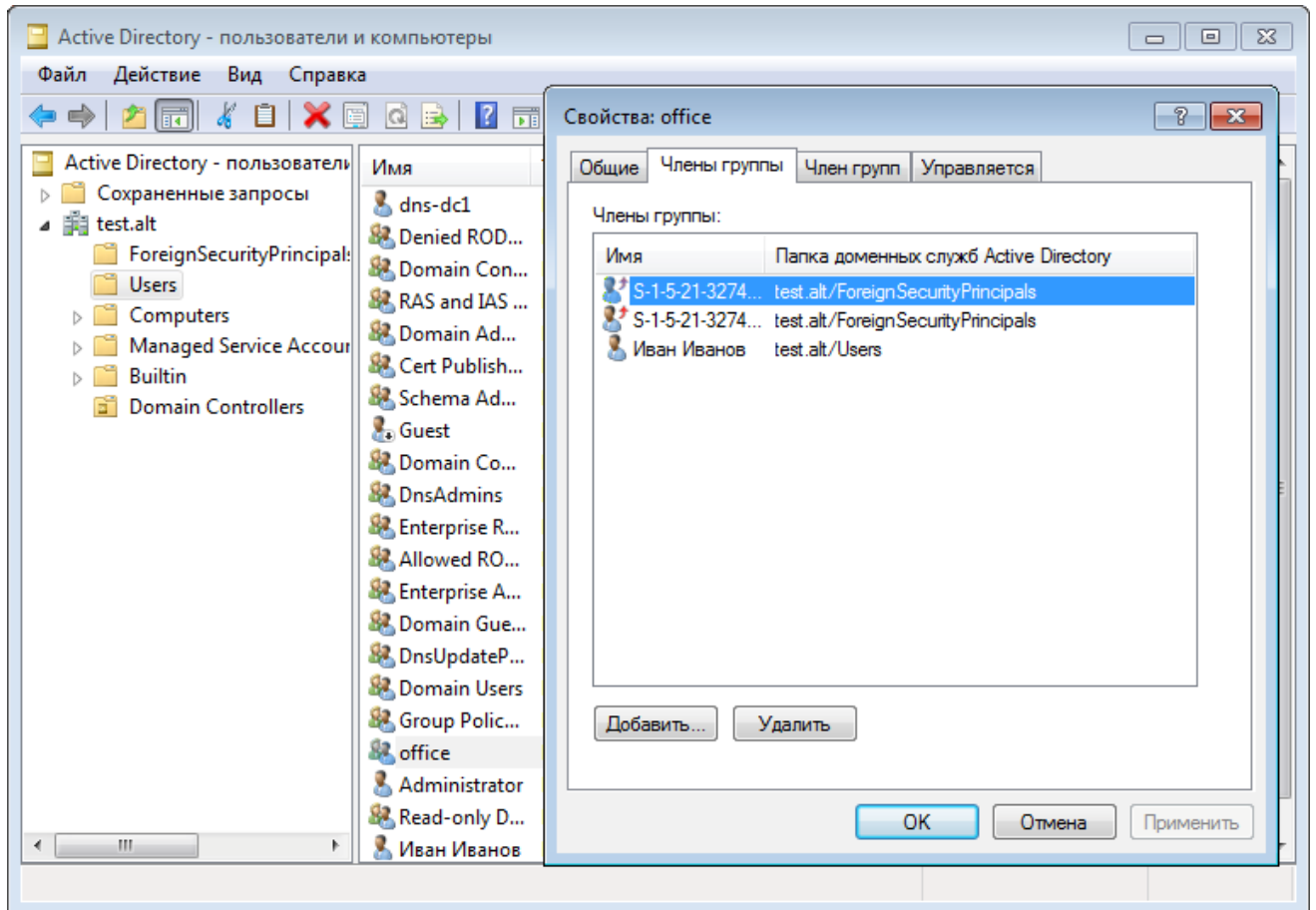


Рис. 479 – Модуль RSAT «Active Directory – пользователи и компьютеры»

10.5.5. Использование трстов на LINUX-клиентах

Если необходимо использовать пользователей из обоих доменов (установлены двухсторонние доверительные отношения с типом связи лес), то рабочую станцию с ОС Альт СП следует вводить в домен через winbind (см. п. 10.3.3.3).

10.5.5.1. Настройка winbind

На машине, введенной в домен, необходимо в файле `smb.conf` установить ID-маппинг для обоих доменов (`backend = rid/tdb`).

Пример файла `smb.conf` на машине, введенной в домен `example.alt`:

```
[global]
security = ads
realm = EXAMPLE.ALT
workgroup = EXAMPLE
netbios name = WORK1
template shell = /bin/bash
kerberos method = system keytab
wins support = no
winbind use default domain = yes
```


ЛКНВ.11100-01 90 03

```

winbind enum users = no
winbind enum groups = no
template homedir = /home/EXAMPLE.ALT/%U
winbind refresh tickets = yes
winbind offline logon = yes
idmap config * : range = 10000-20000000
idmap config * : backend = tdb

idmap config EXAMPLE : backend = rid
idmap config EXAMPLE : range = 10000-20000000
idmap config TEST : backend = rid
idmap config TEST : range = 10000-20000000

```

После перезапуска `smbd`, `nmbd`, `winbind` можно проверить, есть ли возможность просматривать пользователей из обоих доменов:

```

# net rpc trustdom list -Uadministrator
Password for [EXAMPLE\administrator]:
Trusted domains list:

TEST                S-1-5-21-1455776928-3410124986-2843404052

```

```

Trusting domains list:

TEST                S-1-5-21-1455776928-3410124986-2843404052

```

```

# wbinfo -n TEST\\ivanov
S-1-5-21-1455776928-3410124986-2843404052-1105 SID_USER (1)

```

```

# wbinfo -n EXAMPLE\\kim
S-1-5-21-3274802069-598906262-3677769431-1104 SID_USER (1)

```

Проверка с помощью getent:

```

# getent group TEST\\office
TEST\office*:11107:

```

```

# getent group EXAMPLE\\office2
office2*:11107:

```

```

# getent passwd TEST\\ivanov
TEST\ivanov*:11105:10513::/home/EXAMPLE.ALT/ivanov:/bin/bash

```

```

# getent passwd EXAMPLE\\kim
kim*:10000:10001:Олег Ким:/home/EXAMPLE.ALT/kim:/bin/bash

```

Проверка входа по SSH пользователями из обоих доменов:

```
$ ssh TEST\\ivanov@192.168.0.126
TEST\ivanov@192.168.0.126's password:
[TEST\ivanov@work1 ~]$ exit
ВЫХОД
Connection to 192.168.0.126 closed.
```

```
$ ssh EXAMPLE\\kim@192.168.0.126
EXAMPLE\kim@192.168.0.126's password:
[kim@work1 ~]$ exit
ВЫХОД
Connection to 192.168.0.126 closed.
```

Для авторизации в доверенном домене следует вводить учетные данные пользователя в формате DOMAIN\user.

10.5.5.2. Настройка SSSD

На машине, введенной в домен, необходимо в файл /etc/sss/sss.conf добавить доверенный домен:

```
[domain/EXAMPLE.ALT/TEST.ALT]
use_fully_qualified_names = false
```

После перезапуска sssd можно проверить, есть ли возможность просматривать пользователей из обоих доменов:

```
# getent passwd ivanov
ivanov:*:1855401105:1855400513:Иван
Иванов:/home/TEST.ALT/ivanov:/bin/bash
# getent passwd kim
```

10.5.6. Удаление доверия

10.5.6.1. На стороне Samba

Пример удаления доверия на контроллере домена dc1.test.alt:

```
# samba-tool domain trust delete EXAMPLE.ALT -U
administrator@EXAMPLE.ALT
LocalDomain Netbios[TEST] DNS[test.alt] SID[S-1-5-21-1455776928-
3410124986-2843404052]
RemoteDC Netbios[S1] DNS[s1.example.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,
FULL_SECRET_DOMAIN_6]
Password for [administrator@EXAMPLE.ALT]:
RemoteDomain Netbios[EXAMPLE] DNS[example.alt] SID[S-1-5-21-
3274802069-598906262-3677769431]
RemoteTDO deleted.
```

Проверка:

```
# samba-tool domain trust list
```

10.5.6.2. На стороне Windows Server с AD

Удаление доверия:

- 1) открыть «Диспетчер серверов», выбрать «Средства» → «Active Directory – домены и доверие» (рис. 480);

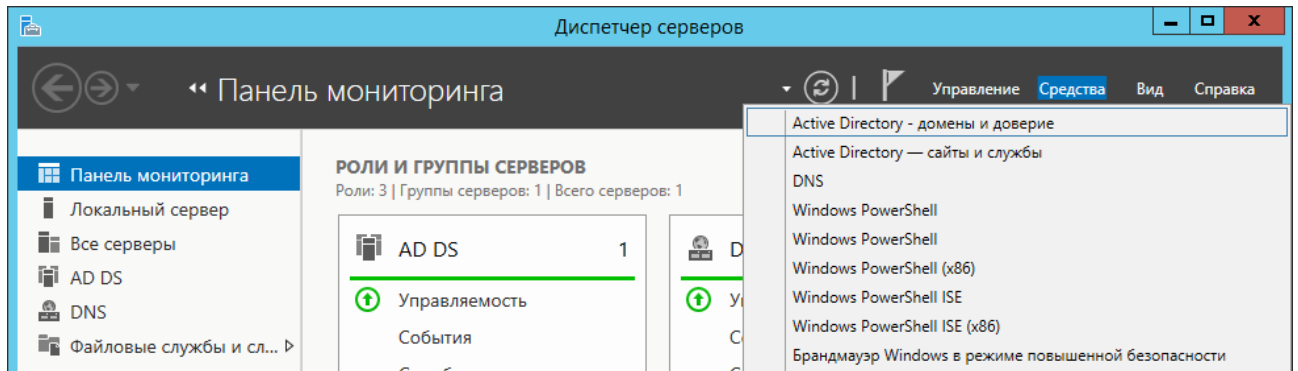


Рис. 480 – Окно «Диспетчер серверов»

- 2) в открывшемся окне в контекстном меню домена выбрать пункт «Свойства» (рис. 481);

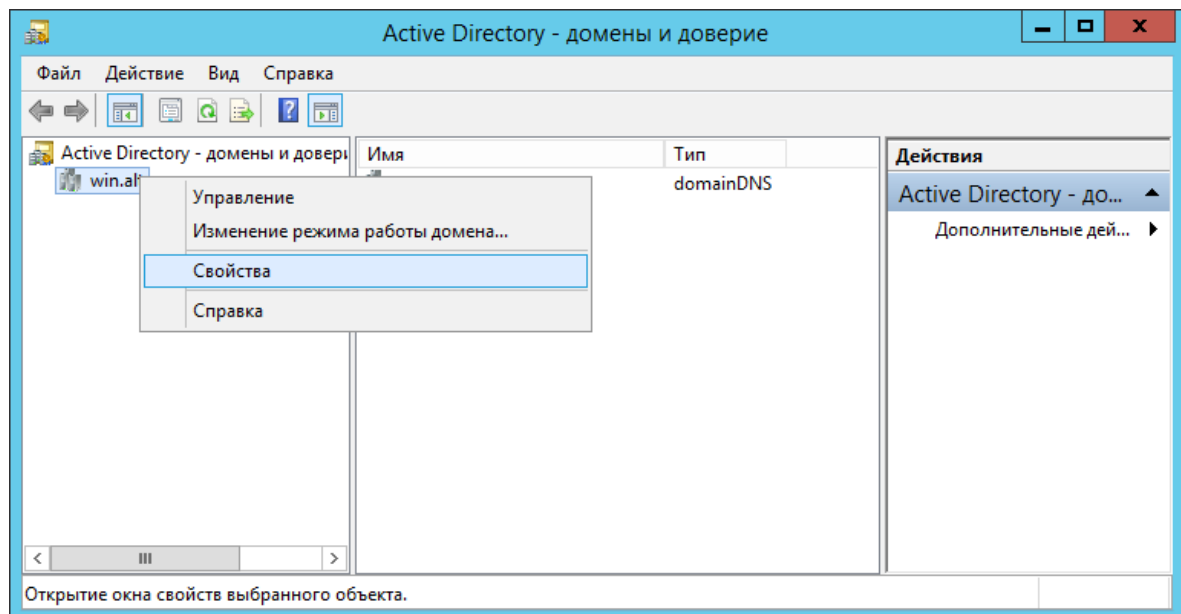


Рис. 481 – Окно «Active Directory – домены и доверие»

- 3) откроется окно свойств домена. Необходимо перейти во вкладку «Отношения доверия» и нажать кнопку «Создать отношение доверия...» (рис. 482);

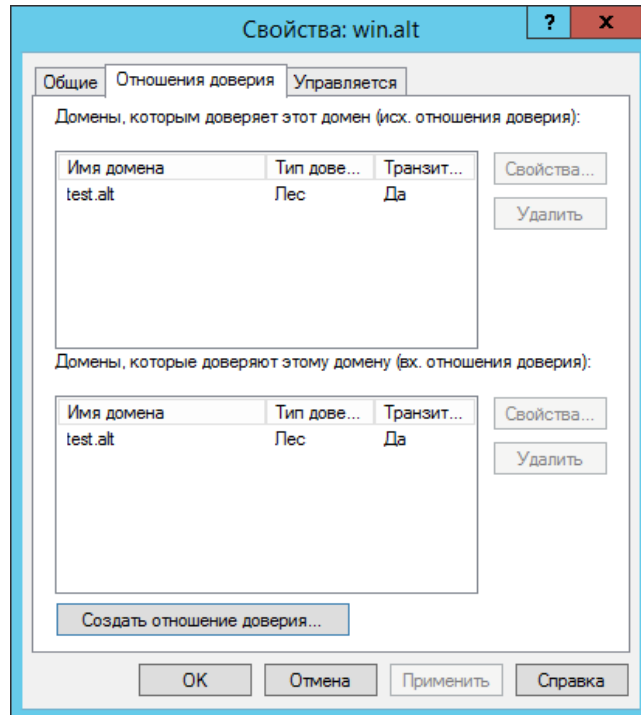


Рис. 482 – Вкладка «Отношения доверия»

- 4) в группе «Домены, которым доверяет этот домен (исх. отношения доверия)» или группе «Домены, которые доверяют этому домену (вх. отношения доверия)» выбрать доверие, которое требуется удалить, а затем нажать кнопку «Удалить»;
- 5) в открывшемся окне выбрать пункт, где нужно удалить доверие, и нажать кнопку «ОК» (рис. 483).

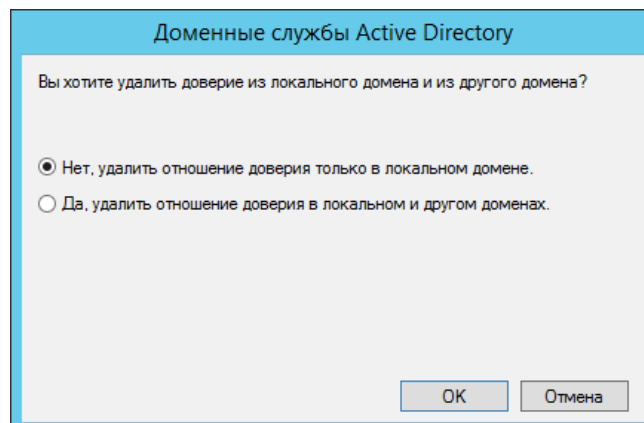


Рис. 483 – Окно выбора пункта удаления доверия

Если выбран параметр «Нет, удалить отношение доверия только в локальном домене», рекомендуется повторить эту процедуру для домена второй стороны.

Если выбран параметр «Да, удалить отношение доверия в локальном и другом доменах», необходимо ввести учетную запись и пароль администратора для домена второй стороны.

10.6. Администрирование домена

10.6.1. Управление пользователями и группами

10.6.1.1. В ADMS

Для управления пользователями и группами в «Альт Домен» можно использовать модуль удаленного управления базой данных конфигурации (ADMS). Подробнее см. п. 10.4.5.

10.6.1.2. Подкоманда user и group утилиты samba-tool

Для управления пользователями и группами в «Альт Домен» можно использовать инструмент командной строки samba-tool.

Примечание. Для выполнения команд на удаленном компьютере можно использовать опцию `-H` или `--URL=` с указанием URI LDAP-сервера. Например:

```
# samba-tool user add domainuser Qwerty1 -H ldap://<DC> -Uadministrator
```

По умолчанию в качестве значения опции `-H` передается текущий узел в формате `ldap://<имя узла>`.

Команды управления пользователями представлены в таблице 71.

Т а б л и ц а 71 – Команды управления пользователями инструмента samba-tool

Команда	Описание	Примечание
user add <имя пользователя> [<пароль>] [опции]	Создать нового пользователя	<p>Переданное в команде значение <имя пользователя> интерпретируется как имя учетной записи SAM (значение атрибута sAMaccountName). Оно должно быть уникальным.</p> <p>Некоторые опции:</p> <ul style="list-style-type: none"> - --surname – фамилия пользователя; - --given-name – имя пользователя; - --initials – инициалы; - --must-change-at-next-login – пользователь должен изменить пароль при первом входе в домен; - --random-password – сформировать пароль случайным образом; - --smartcard-required – требовать наличие смарт-карты при входе в интерактивном режиме; - --use-username-as-cn – включить принудительное использование имени пользователя в качестве общего имени (CN); - --userou – имя (DN) альтернативного расположения (без domainDN), в котором будет создан пользователь (вместо используемого по умолчанию CN=Users); - --company – компания пользователя; - --department – подразделение, к которому относится пользователь; - --description – информация о пользователе; - --mail-address – адрес электронной почты пользователя; - --rfc2307-from-nss – включить копирования атрибутов пользователя Unix из диспетчера службы имен (NSS); значение параметра переопределяется в случае явного задания числового идентификатора пользователя (UID), числового идентификатора основной группы пользователя (GID), информации о пользователе (GECOS) или интерпретатора команд, который должен запускаться при входе пользователя в систему (shell); - --nis-domain – домен службы сетевой информации (NIS) для пользователя (Unix/RFC 2307);

Продолжение таблицы 71

Команда	Описание	Примечание
		<ul style="list-style-type: none"> - <code>--unix-home</code> – домашний каталог пользователя (Unix/RFC 2307); - <code>--uid</code> – имя пользователя (Unix/RFC 2307); - <code>--uid-number</code> – уникальный числовой идентификатор пользователя (Unix/RFC 2307); - <code>--gid-number</code> – числовой идентификатор основной группы пользователя (Unix/RFC 2307); - <code>--gecos</code> – информация о пользователе в поле GECOS (Unix/RFC 2307); - <code>--login-shell</code> – оболочка (shell), которая должна запускаться при входе в систему пользователя (Unix/RFC 2307)
<code>user create</code> <имя пользователя> [<пароль>] [опции]	Создать нового пользователя	Команда доступна только в целях совместимости. Рекомендуется вместо этой команды использовать команду: <code>samba-tool user add</code>
<code>user delete</code> <имя пользователя> [опции]	Удалить существующего пользователя	При удалении учетной записи также удаляются все связанные с ней разрешения, права и членства в группах
<code>user disable</code> <имя пользователя> <code>--filter</code> <фильтр> [опции]	Отключить пользовательский аккаунт	Параметры вызова: <ul style="list-style-type: none"> - <code>--filter</code> – LDAP-фильтр для поиска объектов в домене
<code>user edit</code> <имя пользователя> [опции]	Редактировать объект пользовательского аккаунта	В опции <code>-editor = <редактор></code> можно указать редактор (по умолчанию <code>vi</code>)
<code>user enable</code> <имя пользователя> > <code>--filter</code> <фильтр> [опции]	Включить пользовательский аккаунт	Параметры вызова: <ul style="list-style-type: none"> - <code>--filter</code> – LDAP-фильтр для поиска объектов в домене
<code>user list</code> [опции]	Вывести список пользователей	По умолчанию выводятся <code>sAMAccountNames</code> пользователей. Можно использовать следующие опции: <ul style="list-style-type: none"> - <code>--full-dn</code> – показать различающиеся имена пользователей (CN) вместо <code>sAMAccountNames</code>; - <code>-b BASE_DN --base-dn=BASE_DN</code> – вывести пользователей с указанным базовым DN; - <code>--hide-expired</code> – не выводить просроченные учетные записи пользователей; - <code>--hide-disabled</code> – не выводить отключенные учетные записи пользователей

Продолжение таблицы 71

Команда	Описание	Примечание
user setprimarygroup <имя пользователя> <имя группы> [опции]	Установить основную группу для учетной записи пользователя	
user getgroups <имя пользователя> [опции]	Вывести список групп, в которые входит учетная запись пользователя напрямую	Можно использовать следующие опции: - --full-dn – показать в списке вместо имен групп SAM (sAMAccountName) их полные уникальные имена (DN)
user show <имя пользователя> [опции]	Вывести пользовательский объект	В опции --attributes=USER_ATTRS можно указать, разделенный запятыми, список атрибутов, значения которых требуется отобразить. Для вывода скрытых атрибутов, их необходимо явно указать в параметре --attributes
user move <имя пользователя> <контейнер> [опции]	Переместить учетную запись пользователя в указанную организационную единицу или контейнер	Имя пользователя указывается в команде в формате sAMAccountName. Имя организационной единицы или контейнера можно указать как полное DN или без компонента domainDN.
user password [опции]	Изменить пароль, текущей учетной записи (пользователя, прошедшего аутентификацию)	Если пароль не передается в открытом виде в значении параметра --newpassword, пользователь получит запрос на ввод пароля в командной строке
user rename <имя пользователя> [опции]	Переименовать пользователя и изменить его атрибуты	По умолчанию выводятся sAMAccountNames пользователей. Для удаления атрибута следует использовать пустое значение атрибута. Имя пользователя указывается в команде в формате sAMAccountName. Можно использовать следующие опции: - --surname=SURNAME – новая фамилия; - --given-name=GIVEN_NAME – новое имя; - --initials=INITIALS – новые инициалы; - --force-new-cn=NEW_CN – новый CN (вместо использования комбинации имени, инициалов и фамилии); - --reset-cn – установить CN на комбинацию имени, инициалов и фамилии по умолчанию; - --display-name=DISPLAY_NAME – новое отображаемое имя; - --mail-address=MAIL_ADDRESS – новая электронная почта; - --samaccountname = SAMACCOUNTNAME – новое имя для входа (sAMAccountName); - --upn=UPN – новое основное имя

Окончание таблицы 71

Команда	Описание	Примечание
<pre>user setexpiry <имя пользователя> --filter <фильтр>) [опции]</pre>	Установить срок действия для учетной записи пользователя	<p>По истечении заданного периода учетная запись отключается; пользователь не может получать доступ к ресурсам домена. При этом сохраняются связанные с учетной записью разрешения, права и членства.</p> <p>Параметры вызова:</p> <ul style="list-style-type: none"> - <code>--filter</code> – LDAP-фильтр для поиска объектов в домене; - <code>--days=DAY</code>S – продолжительность периода в днях; - <code>--noexpiry</code> – период действия неограничен
<pre>user setpassword <имя пользователя> --filter <фильтр>) [опции]</pre>	Установить или сбросить пароль учетной записи пользователя	<p>Если пароль не передается в открытом виде в значении параметра <code>--newpassword</code>, пользователь получит запрос на ввод пароля в командной строке.</p> <p>Параметры вызова:</p> <ul style="list-style-type: none"> - <code>--filter</code> – LDAP-фильтр для поиска объектов в домене; - <code>--newpassword</code> – новый пароль; - <code>--must-change-at-next-login</code> – пользователь должен изменить пароль при первом входе в домен; - <code>--random-password</code> – сформировать пароль случайным образом; - <code>--smartcard-required</code> – требовать наличие смарт-карты при входе в интерактивном режиме
<pre>user unlock <имя пользователя> -- filter <фильтр>) [опции]</pre>	Разблокировать учетную запись пользователя в домене	<p>Параметры вызова:</p> <ul style="list-style-type: none"> - <code>--filter</code> – LDAP-фильтр для поиска объектов в домене
<pre>user getpassword <имя пользователя> -- filter <фильтр>) [опции]</pre>	Получить атрибуты пароля учетной записи пользователя	<p>Параметры вызова:</p> <ul style="list-style-type: none"> - <code>--filter</code> – LDAP-фильтр для поиска объектов в домене; - <code>--attributes</code> – атрибуты (через запятую), которые требуется вывести или передать скрипту, заданному в параметре <code>--script</code>. В параметре могут передаваться любые атрибуты, заданные в схеме каталога, а также следующие виртуальные атрибуты: <code>virtualClearTextUTF16</code>, <code>virtualClearTextUTF8</code>, <code>virtualCryptSHA256</code>, <code>virtualCryptSHA512</code>, <code>virtualKerberosSalt</code>, <code>virtualSSHA</code>, <code>virtualSambaGPG</code>, <code>virtualDigest01..29</code>; - <code>--decrypt-samba-gpg</code> – дешифровать пароль SambaGPG (должен быть установлен пакет <code>python3-module-gpg</code>)

Окончание таблицы 71

Команда	Описание	Примечание
user syncpasswords [--cache-ldb- initialize] [опции]	Синхронизировать пароли всех учетных записей пользователей с помощью дополнительного сценария	Эта команда должна выполняться только на одном контроллере домена (обычно на PDC). В первый раз команда должна выполняться с параметром, обеспечивающим инициализацию кеша: --cache-ldb-initialize Для корректной инициализации кеша требуется передать список атрибутов в параметре --attributes

Полный список параметров каждой команды можно увидеть в справке, например:

```
# samba-tool user add --help
```

Примеры:

- создать пользователя `ivanov` в подразделении `KDE`, пользователь должен изменить пароль при следующем входе в систему:

```
# samba-tool user add ivanov --given-name='Иван' \
--surname='Иванов' --mail-address='ivanov@test.alt' \
--userou='OU=KDE' --must-change-at-next-login
```

```
New Password:
```

```
Retype Password:
```

```
User 'ivanov' added successfully
```

- создать пользователя `kim` со случайным паролем, с указанием удаленного LDAP-сервера, пользователь должен изменить пароль при следующем входе в систему:

```
# samba-tool user add kim --given-name='Виталий' \
--surname='Ким' --mail-address='kim@test.alt' \
--must-change-at-next-login --random-password \
```

```
-H ldap://dc2.test.alt -U administrator
```

```
Password for [TEST\administrator]:
```

```
User 'kim' added successfully
```

- установить, что срок действия пароля пользователя `ivanov` никогда не истекает:

```
# samba-tool user setexpiry ivanov --noexpiry
```

```
Expiry for user 'ivanov' disabled.
```

- задать 20-дневный период действия (начиная с текущей даты) для учетной записи kim:

```
# samba-tool user setexpiry kim --days=20
Expiry for user 'kim' set to 20 days.
```

- просмотреть список учетных записей пользователей:

```
# samba-tool user list
Guest
ivanov
Administrator
krbtgt
kim
```

- отключить пользователя ivanov:

```
# samba-tool user disable ivanov
```

- включить всех пользователей, почтовый ящик которых начинается на k:

```
# samba-tool user disable --filter=mail=k*
Enabled user 'mail=k*'
```

- изменить пароль пользователя ivanov:

```
# samba-tool user setpassword ivanov
```

- переместить пользователя kim в подразделение KDE:

```
# samba-tool user move kim 'OU=KDE'
Moved user "kim" into "OU=KDE,DC=test,DC=alt"
```

- получить информацию о пароле пользователя ivanov:

```
# samba-tool user getpassword ivanov \
--attributes=pwdLastSet,virtualClearTextUTF8
dn: CN=Иван Иванов,OU=TEST,DC=test,DC=alt
pwdLastSet: 133628348830281440
Got password OK
```

- удалить пользователя ivanov:

```
# samba-tool user delete ivanov
Deleted user ivanov
```



Не следует допускать одинаковых имен для пользователя и компьютера, это может привести к коллизиям (например, такого пользователя нельзя добавить в группу). Если компьютер с таким именем заведен, удалить его можно командой:

```
pdbedit -x -m имя
```

Примечание. При удалении учетной записи также удаляются все связанные с ней разрешения, права и членства в группах. Если в последствии в домен будет добавлена учетная запись с тем же именем, она не получит разрешения,

права или членства удаленной записи, так как ей будет присвоен новый идентификатор безопасности (SID).

Учетная запись может быть отключена, например, по следующим причинам:

- достигнуто максимальное количество попыток входа, установленное для учетной записи политикой;
- учетная запись отключена администратором;
- истек период действия учетной записи.

Команда включения учетной записи может использоваться администратором как для восстановления доступа отключенной ранее учетной записи к ресурсам домена, так и для включения группы учетных записей, созданных с разрешениями по умолчанию.

Команды инструмента командной строки `samba-tool` для управления группами в «Альт Домен» приведены в таблице 72.

В группу могут входить учетные записи пользователей и компьютеров, а также другие группы. Такое объединение объектов в рамках одной сущности упрощает работу с ними, включая выполнение задач по управлению безопасностью и системному администрированию.

Группы также могут использоваться для создания списков рассылки (группы рассылки). Для этого при вызове команды должна быть передана опция `--group-type=Distribution`.

Группы располагаются в подразделениях (OU). Область действия (scope) группы определяет место группы в дереве доменов.

Т а б л и ц а 72 – Команды управления группами инструмента samba-tool

Команда	Описание	Примечание
<pre>group add <имя группы> [опции]</pre>	Создать новую группу	<p>Переданное в команде значение <имя группы> интерпретируется как имя учетной записи SAM (значение атрибута sAMAccountName). Оно должно быть уникальным.</p> <p>Некоторые опции:</p> <ul style="list-style-type: none"> - --groupou – имя (DN) альтернативного расположения (без domainDN), в котором будет создана группа (вместо используемого по умолчанию CN=Users); - --group-scope – область действия, возможные значения: Domain, Global, Universal; - --group-type – тип группы, возможные значения: Security, Distribution; - --description – описание группы; - --mail-address – адрес электронной почты группы; - --notes – дополнительная информация; - --gid-number – числовой идентификатор группы Unix/RFC 2307; - --nis-domain – домен NIS; - --special – используется для создания группы безопасности с именем Protected Users
<pre>group create <имя группы> [опции]</pre>	Создать новую группу	<p>Доступна только в целях совместимости. Рекомендуется вместо этой команды использовать команду <code>samba-tool group add</code></p>
<pre>group addmembers (<список участников> -- member- dn=<member-dn>) [опции]</pre>	Добавить участников в группу	<p>Команда позволяет добавить в группу одного или нескольких участников (указанных через запятую). В качестве участника группы может выступать учетная запись пользователя, учетная запись компьютера или другая группа, существующая в домене.</p> <p>Некоторые опции:</p> <ul style="list-style-type: none"> - --member-dn – уникальное составное имя (DN) добавляемого в группу нового участника (значение опции --object-types игнорируется); - --object-types – список типов объектов (через запятую); указанные типы используются в качестве фильтра при выполнении поиска для указанных в команде участников; возможные значения: user, group, computer, serviceaccount, contact, all; значение по умолчанию – user,group,computer;

Продолжение таблицы 72

Команда	Описание	Примечание
		- <code>--member-base</code> – базовое уникальное имя (DN) для поиска участников группы; значение по умолчанию – уникальное имя (DN) домена
<code>group delete</code> <имя группы> [опции]	Удалить группу	Операция удаления является необратимой. При удалении группы также удаляются все связанные с ней разрешения и права, а также унаследованные от нее разрешения и права участников
<code>group addunixattrs</code> <имя группы> <gidnumber> [опции]	Добавить атрибуты Unix/RFC 2307 для группы	Для использования этих атрибутов для сопоставления UID/GID в конфигурации (<code>smb.conf</code>) должен быть задан параметр <code>idmap_ldp:use rfc2307 = Yes</code>
<code>group edit</code> <имя группы> [опции]	Редактировать объект группы	В опции <code>--editor=<редактор></code> можно указать редактор (по умолчанию <code>vi</code>)
<code>group list</code> [опции]	Вывести список групп	По умолчанию выводится список имен учетных записей SAM (<code>sAMAccountName</code>). Можно использовать следующие опции: - <code>--full-dn</code> – выводить уникальные имена (DN) вместо <code>sAMAccountNames</code> ; - <code>-b BASE_DN --base-dn=BASE_DN</code> – выводить в списке только группы с указанным базовым уникальным именем (DN)
<code>group listmembers</code> <имя группы> [опции]	Вывести список участников данной группы	По умолчанию выводятся <code>sAMAccountNames</code> участников. Если <code>sAMAccountName</code> недоступен, будет использоваться CN. Можно использовать следующие опции: - <code>--full-dn</code> – показать различающиеся имена участников (CN) вместо <code>sAMAccountNames</code> ; - <code>--hide-expired</code> – не выводить членов группы с истекшим сроком действия; - <code>--hide-disabled</code> – не выводить отключенных членов группы
<code>group move</code> <имя группы> <контейнер> [опции]	Переместить группу в указанную организационную единицу или контейнер	Имя организационной единицы или контейнера можно указать как полное DN или без компонента <code>domainDN</code>
<code>group stats</code> [опции]	Показать статистику для общих групп и членства в группах	В результате выполнения команды выводятся следующие сведения: - общее количество групп; - общее количество участников (без учета вложенности); - среднее количество участников в группе; - максимальное количество участников в группе; - медианное количество участников в группе; - распределение участников по группам с точки зрения количественного состава

Окончание таблицы 72

Команда	Описание	Примечание
group show <имя группы> [опции]	Вывести группу и ее атрибуты	В опции --attributes=USER_ATTRS можно указать, разделенный запятыми, список атрибутов
group removemembers <имя группы> (<список участников> --member-dn=<member-dn>) [опции]	Удалить участника из группы	Команда позволяет удалить из группы одного или нескольких участников (указанных через запятую). При удалении из группы участник теряет все унаследованные от нее разрешения и права. Некоторые опции: <ul style="list-style-type: none"> - --member-dn – уникальное составное имя (DN) удаляемого из группы участника (значение опции --object-types игнорируется); - --object-types – список типов объектов (через запятую); указанные типы используются в качестве фильтра при выполнении поиска для указанных в команде участников; возможные значения: user, group, computer, serviceaccount, contact, all; значение по умолчанию – user,group,computer; - --member-base – базовое уникальное имя (DN) для поиска участников группы; значение по умолчанию – уникальное имя (DN) домена
group rename <имя группы> [опции]	Переименовать группу и изменить ее атрибуты	Для удаления атрибута следует использовать пустое значение атрибута. Имя группы указывается в команде в формате sAMAccountName. Можно использовать следующие опции: <ul style="list-style-type: none"> - --force-new-cn=NEW_CN – новый CN (вместо использования sAMAccountName); - --reset-cn – установить CN равным sAMAccountName; - --mail-address=MAIL_ADDRESS – новая электронная почта; - --samaccountname=SAMACCOUNTNAME – новое имя для входа (sAMAccountName)

Полный список параметров каждой команды можно увидеть в справке, например:

```
# samba-tool group add --help
```

Примеры:

- добавить группу:

```
# samba-tool group add office --description='Simple group'
Added group office
```

- добавить новую группу рассылки с указанием удаленного LDAP-сервера:
samba-tool group add manager --group-type=Distribution \
-H ldap://dc2.test.alt -U administrator
Added group manager
- добавить новую группу в соответствии с RFC 2307 в домен NIS samdom с
GID 12345:
samba-tool group add mygroup --nis-domain=samdom \
--gid-number=12345
Added group mygroup
- удалить группу:
samba-tool group delete office
Deleted group office
- добавить пользователя ivanov в группу Domain Users:
samba-tool group addmembers "Domain Users" ivanov
- добавить в группу mygroup пользователей kim, ivanov и группу manager:
samba-tool group addmembers mygroup manager,kim,ivanov
- удалить пользователя ivanov из группы Domain Users:
samba-tool group removemembers "Domain Users" ivanov
- переместить группу manager в подразделение OU:
samba-tool group move manager 'OU=OU'
Moved group "manager" into "OU=OU,DC=test,DC=alt"
- вывести список пользователей группы Domain Users:
samba-tool group listmembers "Domain Users"
- получить определенные атрибуты группы manager:
samba-tool group show manager --attributes=member,objectGUID
dn: CN=test2,CN=Users,DC=test,DC=alt
objectGUID: 2f708ea2-f42c-4344-af22-bc243301c777
member: CN=Иван Иванов,OU=KDE,DC=test,DC=alt
- получить общую информацию о группах и их участниках:
samba-tool group stats
Group membership statistics*

Total groups: 48
Total memberships: 32
Average members per group: 0.67

ЛКНВ.11100-01 90 03

Max members: 8 (Denied RODC Password Replication Group)

Median members per group: 0.0

Members Number of Groups

```
-----
0-1 42
2-4 5
5-9 1
```

* Note this does not include nested group membership

В «Альт Домен» поддерживается работа с группой безопасности «Protected Users» («Защищенные пользователи»). В данную группу должны включаться только учетные записи пользователей. После добавления в группу в отношении учетной записи начинают действовать следующие ограничения:

- недоступна аутентификация по протоколу NTLM;
- пользователю не выдаются и от пользователя не принимаются билеты Kerberos с использованием алгоритма шифрования RC4 (используется алгоритм AES);
- максимальный период действия билета – 4 часа;
- недоступно неограниченное и ограниченное делегирование Kerberos.

Примечание. Группа «Защищенные пользователи» доступна только при функциональном уровне домена Windows Server 2012 R2.

Для создания группы безопасности «Защищенные пользователи» следует создать группу «Protected Users» с указанием опции `--special`:

```
# samba-tool group add 'Protected Users' --special
```

10.6.2. Администрирование DNS

Для связывания доменных имен с IP-адресами используются А-записи (для IPv4) и AAAA-записи (для IPv6), которые создаются при настройке DNS и содержат соответствующий IP-адрес узла. PTR-записи применяются для обратного разрешения, связывая IP-адреса с доменными именами в обеих версиях протокола и создаются в зоне обратного DNS.

В процессе эксплуатации IP-адреса узла могут меняться (из-за перезагрузки устройства, изменений в конфигурации сети или обновления через DHCP).

В таких случаях необходимо обновить соответствующие DNS-записи, чтобы сохранить корректное разрешение имен и обеспечить работу служб аутентификации, таких как Kerberos или LDAP, для успешной проверки подлинности пользователей. Это обновление может выполняться автоматически как со стороны DHCP-сервера, так и со стороны клиента домена. DHCP-сервер может обновлять записи в DNS при изменении IP-адресов, в то время как клиент домена может обновлять записи через такие службы, как Winbind и SSSD, а также через встроенные функции операционных систем (на Windows-клиенте). Возможно также ручное обновление записей администраторами.

10.6.2.1. DNS-записи при вводе машины в домен

При вводе машины в домен, в DNS-записи на DNS-сервере прописывается текущий IP-адрес машины.

Например, если машина с именем `work.test.alt` вводится в домен и имеет IP-адрес `192.168.0.55` (независимо от того, получен ли он статически или через DHCP), то на DNS-сервере будет создана (или обновлена) запись:

```
work.test.alt. IN A 192.168.0.55
```

Эта запись будет храниться в DNS-зоне прямого просмотра домена и использоваться для разрешения имени `work.test.alt` в IP-адрес `192.168.0.55`.

PTR DNS-запись автоматически не создается, даже если существует обратная зона в базе данных домена. Для ее создания необходимо на клиенте включить необходимые настройки для обновления PTR DNS-записей (то есть в дальнейшем вместо обновления запись будет зарегистрирована). В противном случае запись нужно будет создать вручную:

```
$ samba-tool dns add dc1.test.alt 0.168.192.in-addr.arpa \
55 PTR work.test.alt -U administrator
Password for [TEST\administrator]:
Record added successfully
```

При этом будет создана DNS-запись:

```
55.0.168.192.in-addr.arpa. 3600 IN PTR work.test.alt.
```

Проверить наличие записи можно, выполнив команду:

```
$ host -t PTR 192.168.0.55 dc1.test.alt
Using domain server:
```

```
Name: dc1.test.alt
Address: 192.168.0.132#53
Aliases:
```

```
55.0.168.192.in-addr.arpa domain name pointer work.test.alt.
```

Примечание. Обратная зона создается так:

```
$ samba-tool dns zonecreate dc1.test.alt 0.168.192.in-addr.arpa -Uadministrator
Password for [TEST\administrator]:
Zone 0.168.192.in-addr.arpa created successfully
```

10.6.2.2. Подкоманда dns утилиты samba-tool

Для администрирования службы доменных имен (DNS) в «Альт Домен» можно использовать подкоманду dns утилиты samba-tool.

Примечание. Для выполнения команд на удаленном компьютере можно использовать опцию `-H` или `--URL=` с указанием URI LDAP-сервера. Например:

```
$ samba-tool dns add 192.168.0.132 test.alt \
DC2 А 192.168.0.133 -H ldap://<DC> -Uadministrator
```

По умолчанию в качестве значения опции `-H` передается текущий узел в формате `ldap://<имя узла>`.

10.6.2.2.1. Работа с DNS-записями

Команды инструмента командной строки samba-tool для управления DNS-записями приведены в таблице 73.

Т а б л и ц а 73 – Команды управления DNS-записями инструмента samba-tool

Команда	Описание	Примечание
<pre>dns add <сервер> <зона> <имя> <A AAAA PTR CNAME NS MX SRV TXT> <данные></pre>	Добавить новую запись	Параметры вызова: <ul style="list-style-type: none"> - сервер – IP-адрес или доменное имя DNS-сервера; - зона – зона DNS; - имя – имя DNS-записи; - тип добавляемой записи с данными (см. ниже)
<pre>dns delete <сервер> <зона> <имя> <A AAAA PTR CNAME NS MX SRV TXT> <данные></pre>	Удалить DNS-запись	
<pre>dns edit <сервер> <зона> <имя> <A AAAA PTR CNAME NS MX SOA SRV TXT> <текущие-данные> <новые-данные></pre>	Изменить DNS-запись	Дополнительно для изменения доступен тип записи SOA (Start of Authority), являющейся начальной записью зоны, со следующими данными (порядок пунктов в списке ниже соответствует порядку следования параметров в строке): <ul style="list-style-type: none"> - nameserver – доменное имя DNS-сервера, на котором хранятся другие DNS-записи; - email – адрес электронной почты администратора зоны (вместо @ указывается точка, например для адреса user@test.alt указывается значение user.test.alt); - serial – серийный номер файла зоны, представляющий собой номер версии записи SOA; увеличивается при каждом изменении значения записи и служит сигналом другим DNS-серверам о том, что требуется обновить данные; - refresh – интервал для запроса изменений; - retry – интервал для повторных попыток запроса данных в случае неудачи; - expire – время, в течение которого обновленные данные могут быть применены на других DNS-серверах; - minimum-ttl – время хранения в кеше информации о зоне

Окончание таблицы 73

Команда	Описание	Примечание
<code>dns cleanup <сервер> <имя узла> [опции]</code>	Очистить DNS-записи указанного DNS-узла	Во многих случаях данная подкоманда только устанавливает значение true в атрибуте <code>dNSTombstoned</code> DNS-записей. После этого при запросе таких записей информация о них возвращаться не будет, но в базе данных могут оставаться соответствующие им записи-заполнители
<code>dns query <сервер> <зона> <имя> <A AAAA PTR CNAME NS MX SOA SRV TXT ALL> [опции]</code>	Вывести информацию о DNS-записях	Можно использовать следующие опции: <ul style="list-style-type: none"> - <code>--authority</code> – поиск по записям полномочного DNS-сервера (значение по умолчанию); - <code>--cache</code> – поиск по записям в кеше; - <code>--glue</code> – поиск по связующим (<code>glue</code>) записям; - <code>--root</code> – поиск по корневым ссылкам DNS-сервера; - <code>--additional</code> – вывод списка дополнительных записей; - <code>--no-children</code> – исключение вывода дочерних записей; - <code>--only-children</code> – вывод только дочерних записей

Возможные типы записей:

- A <IPv4-адрес> – IPv4-адрес для связи с именем домена;
- AAAA <IPv6-адрес> – IPv6-адрес для связи с именем домена;
- PTR <FQDN> – полное доменное имя (FQDN) для связи с IP-адресом домена;
- CNAME <FQDN> – полное доменное имя (FQDN) для создания псевдонима;
- NS <FQDN> – полное доменное имя (FQDN) сервера, выполняющего роль сервера имен;
- MX <FQDN> <preference> – полное доменное имя (FQDN) и приоритет почтового сервера;

- SRV <FQDN> <port> <priority> <weight> – полное доменное имя (FQDN) сервера, на котором доступна определенная служба, порт для доступа к службе (port), приоритет (priority) и относительный вес (weight) на случай, если существует несколько записей с одинаковым приоритетом;
- TXT "'string1' 'string2' ..." – информация о домене в текстовом формате (string).

Примечание. Полный список параметров каждой команды можно увидеть в справке, например:

```
$ samba-tool dns add --help
```

⚠ При использовании команды `samba-tool dns` указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

Примеры:

- добавить запись типа A:

```
$ samba-tool dns add 192.168.0.132 test.alt \
DC2 A 192.168.0.133 -U administrator
Password for [TEST\administrator]:
Record added successfully
```

- добавить запись типа PTR для обратной зоны 192.168.0.0/24:

```
$ samba-tool dns add dc1.test.alt 0.168.192.in-addr.arpa \
55 PTR demo.test.alt -U administrator
Password for [TEST\administrator]:
Record added successfully
```

- удалить запись типа A:

```
$ samba-tool dns delete dc1.test.alt test.alt \
DC2 A 192.168.0.133 -U administrator
Password for [TEST\administrator]:
Record deleted successfully
```

- изменить запись типа A:

```
$ samba-tool dns update dc1.test.alt test.alt DC2 \
A 192.168.0.133 192.168.0.149 -U administrator
Password for [TEST\administrator]:
Record updated successfully
```

- изменить адрес электронной почты администратора в записи типа SOA:

```
$ samba-tool dns update dc1.test.alt test.alt @ SOA \
"dc1.test.alt admin.test.alt 63 900 600 86400 3600" \
"dc1.test.alt new.test.alt 64 900 600 86400 3600" \
-U administrator
Password for [TEST\administrator]:
Record updated successfully
```

- вывести все DNS-записи для указанной зоны:

```
$ samba-tool dns query dc1.test.alt 0.168.192.in-addr.arpa \
@ ALL -U administrator
```

10.6.2.2.2. Работа с DNS-зонами

Команды инструмента командной строки `samba-tool` для управления DNS-зонами приведены в таблице 74.

Т а б л и ц а 74 – Команды управления DNS-зонами инструмента `samba-tool`

Команда	Описание	Примечание
<code>dns zonecreate <сервер> <зона> [опции]</code>	Создать зону DNS	Дополнительно с помощью параметра <code>--client-version</code> можно указать версию DNS-клиента. Возможные значения: <code>w2k</code> , <code>dotnet</code> , <code>longhorn</code> (по умолчанию)
<code>dns zonedelate <сервер> <зона> [опции]</code>	Удалить зону DNS	
<code>dns zoneinfo <сервер> <зона> [опции]</code>	Вывести информацию о зоне DNS	
<code>dns zonelist <сервер> [опции]</code>	Вывести список зон DNS	Можно использовать следующие опции: <ul style="list-style-type: none"> - <code>--client-version</code> – версия DNS-клиента. Возможные значения: <code>w2k</code>, <code>dotnet</code>, <code>longhorn</code> (по умолчанию); - <code>--primary</code> – получение списка первичных зон DNS (по умолчанию); - <code>--secondary</code> – получение списка вторичных зон DNS; - <code>--cache</code> – получение списка зон DNS из кеша; - <code>--auto</code> – получение списка автоматически созданных зон DNS; - <code>--forward</code> – получение списка прямых зон DNS; - <code>--reverse</code> – получение списка обратных зон DNS; - <code>--ds</code> – получение списка зон DNS, интегрированных с доменом; - <code>--non-ds</code> – получение списка зон DNS без интеграции с доменом

Окончание таблицы 74

Команда	Описание	Примечание
<pre>dns zoneoptions <сервер> <зона> [опции]</pre>	<p>Изменить настройки очистки от устаревших записей для зоны DNS</p>	<p>Можно использовать следующие опции:</p> <ul style="list-style-type: none"> - <code>--client-version</code> – версия DNS-клиента. Возможные значения: <code>w2k</code>, <code>dotnet</code>, <code>longhorn</code> (по умолчанию); - <code>--mark-old-records-static=YYYY-MM-DD</code> – записи старше указанной даты становятся статическими (их временные метки становятся нулевыми); - <code>--mark-records-static-regex=REGEXP</code> – записи, соответствующие заданному регулярному выражению, становятся статическими; - <code>-n --dry-run</code> – запуск в тестовом режиме для проверки корректности заданных параметров; фактически изменения не вносятся; - <code>--aging</code> – признак необходимости очистки от устаревших записей: 0 – очистка отключена (по умолчанию), 1 – очистка включена; - <code>--norefreshinterval=[0-87600]</code> – интервал блокировки для зоны с включенной очисткой в часах; если параметр равен нулю, используется значение по умолчанию (168 часов, одна неделя); - <code>--refreshinterval=[0-87600]</code> – интервал обновления для зоны с включенной очисткой в часах; если параметр равен нулю, используется значение по умолчанию (168 часов, одна неделя)

Примеры:

- создать обратную зону /24:

```
$ samba-tool dns zonecreate 192.168.0.132 \
0.168.192.in-addr.arpa -U administrator
Password for [TEST\administrator]:
Record added successfully
```

- вывести информацию об обратной зоне DNS:

```
$ samba-tool dns zoneinfo dc1.test.alt \
0.168.192.in-addr.arpa -U administrator
```

- включить очистку с большим интервалом обновления:

```
$ samba-tool dns zoneoptions dc1.test.alt \
test.alt --aging=1 --refreshinterval=306600
```


Примечание. Чтобы очистка работала, в файле `smb.conf` хотя бы на одном контроллере домена должен быть задан параметр `dns zone scavenging = yes`.

10.6.2.2.3. Получение информации о DNS-серверах

Команды инструмента командной строки `samba-tool` для получения информации о DNS-серверах приведены в таблице 75.

Т а б л и ц а 75 – Команды `samba-tool` для получения информации о DNS-серверах

Команда	Описание	Примечание
<code>dns serverinfo</code> <сервер> [опции]	Вывести информацию о DNS-сервере	Дополнительно с помощью параметра <code>--client-version</code> можно указать версию DNS-клиента. Возможные значения: <code>w2k</code> , <code>dotnet</code> , <code>longhorn</code> (по умолчанию)
<code>dns roothints</code> <сервер> [<имя>] [опции]	Вывести информацию о корневых серверах DNS	

Примеры:

- вывести информацию о DNS-сервере:

```
$ samba-tool dns serverinfo dcl.test.alt -U administrator
```

Команда возвращает структуру `DNS_RPC_SERVER_INFO`, содержащую информацию о состоянии и конфигурации DNS-сервера, в формате, соответствующем версии DNS-клиента;

- вывести информацию о корневых серверах DNS:

```
$ samba-tool dns roothints dcl.test.alt -U administrator
```

10.6.2.3. Утилита `nsupdate`

Утилита `nsupdate` используется для отправки запросов на обновление динамического DNS серверу имен в соответствии со стандартом RFC 2136. С ее помощью можно добавлять или удалять записи ресурсов из зоны без необходимости правки зонного файла вручную. Один запрос на обновление может содержать запросы на добавление или удаление нескольких записей ресурсов.

Синтаксис команды `nsupdate`:

```
nsupdate [-dDi] [-L level] [-l][-g | -o | -y keyname:secret | -k keyfile] [-v] [-V] [-P] [-T] [-4 | -6] [filename]
```

Опции команды `nsupdate` приведены в таблице 76.

Т а б л и ц а 76 – Опции команды nsupdate

Ключ	Описание
-4	Использовать только IPv4
-6	Использовать только IPv6
-d	Включить режим отладки
-D	Включить дополнительный режим отладки
-i	Принудительно включить интерактивный режим, даже если стандартный ввод не является терминалом
-k keyfile	Позволяет указать файл, содержащий ключ аутентификации TSIG. Файлы могут быть в двух форматах: один файл, содержащий оператор ключа named.conf-format, который может быть автоматически сгенерирован ddns-confgen; или пара файлов, имена которых имеют формат K{name}+.157.+.random}.key и K{name}+.157.+.random}.private, которые могут быть сгенерированы dnssec-keygen. Параметр -k также может использоваться для указания ключа SIG(0), используемого для аутентификации запросов на обновление Dynamic DNS. В этом случае указанный ключ не является ключом HMAC-MD5
-l	Установить режим локального хоста. Адрес сервера будет установлен на localhost (отключая сервер, чтобы адрес сервера не мог быть переопределен). Подключения к локальному серверу используют ключ TSIG, найденный в /var/run/named/session.key, который автоматически генерируется named, если какая-либо локальная первичная зона установила update-policy на local. Расположение этого файла ключа можно переопределить с помощью опции -k
-L level	Установить уровень отладки ведения журнала. Если 0, ведение журнала отключено
-p port	Установить порт для подключения к серверу имен. Значение по умолчанию – 53
-P	Вывести список частных типов записей ресурсов BIND, формат которых понимает nsupdate
-r udpretries	Установить количество повторных попыток UDP. Значение по умолчанию – 3. Если 0, выполняется только один запрос на обновление
-t timeout	Установить максимальное время, которое может занять запрос на обновление, прежде чем он будет прерван. Значение по умолчанию – 300 секунд. Если 0, тайм-аут отключен
-T	Вывести список стандартных типов записей ресурсов IANA, формат которых понимает nsupdate. nsupdate завершает работу после вывода списков. Параметр -T можно комбинировать с параметром -P. Другие типы можно ввести с помощью TYPEXXXXX, где XXXXX – это десятичное значение типа без начальных нулей. Rdata, если они присутствуют, анализируются с использованием формата UNKNOWN rdata (<обратная косая черта> <хеш> <пробел> <длина> <пробел> <шестнадцатеричная строка>)
-u udptimeout	Задать интервал повтора UDP. Значение по умолчанию – 3 секунды. Если равно 0, интервал вычисляется из интервала тайм-аута и количества повторов UDP
-v	Указывает, что TCP следует использовать даже для небольших запросов на обновление. По умолчанию nsupdate использует UDP для отправки запросов на обновление на сервер имен, если только они не слишком велики для того, чтобы поместиться в запрос UDP, в этом случае используется TCP. TCP может быть предпочтительнее, когда выполняется пакет запросов на обновление

Окончание таблицы 76

Ключ	Описание
-v	Вывести номер версии
-y [hmac:]keyname:secret	<p>Задаёт буквальный ключ аутентификации TSIG. keyname – имя ключа, а secret – общий секрет в кодировке base64. hmac – имя алгоритма ключа; допустимые варианты: hmac-md5, hmac-sha1, hmac-sha224, hmac-sha256, hmac-sha384 или hmac-sha512. Если hmac не указан, по умолчанию используется hmac-md5 или, если MD5 отключен, hmac-sha256.</p> <p>Использование опции -y не рекомендуется, поскольку общий секрет предоставляется как аргумент командной строки в виде открытого текста.</p>

nsupdate считывает входные данные из filename или стандартного ввода. Каждая команда (таблица 77) предоставляется ровно в одной строке ввода. Некоторые команды предназначены для административных целей; другие – это либо инструкции по обновлению, либо проверки предварительных условий содержимого зоны. Эти проверки устанавливают условия, что некоторое имя или набор записей ресурсов (RRset) либо существует, либо отсутствует в зоне. Эти условия должны быть выполнены, чтобы весь запрос на обновление был успешным. Обновления отклоняются, если тесты на предварительные условия не пройдены.

Каждый запрос на обновление состоит из нуля или более предварительных условий и нуля или более обновлений. Это позволяет соответствующим образом аутентифицированному запросу на обновление продолжить работу, если некоторые указанные записи ресурсов либо присутствуют, либо отсутствуют в зоне. Пустая строка ввода (или команда send) приводит к отправке накопленных команд как одного запроса на обновление Dynamic DNS на сервер имен.

Т а б л и ц а 77 – Форматы команд и их значения

Команда	Описание
server servername port	Отправить все динамические запросы на обновление на сервер имен servername. Если не указано ни одного оператора сервера, nsupdate отправляет обновления на основной сервер правильной зоны. Поле MNAME записи SOA этой зоны определяет основной сервер для этой зоны. port – это номер порта на servername, куда отправляются динамические запросы на обновление. Если номер порта не указан, используется номер порта DNS по умолчанию 53. Примечание. Эта команда не действует, если используется GSS-TSIG
local address port	Отправить все динамические запросы на обновление, используя локальный адрес. Если локальный оператор не указан, nsupdate отправляет обновления, используя адрес и порт, выбранные системой. port также может использоваться для принудительного поступления запросов с определенного порта. Если номер порта не указан, система назначает его
zone zonename	Указывает, что все обновления должны быть сделаны в зоне zonename. Если оператор zone не указан, nsupdate пытается определить правильную зону для обновления на основе остальной части ввода
class classname	Указывает класс по умолчанию. Если класс не указан, класс по умолчанию – IN
ttl seconds	Указывает время жизни по умолчанию в секундах для добавляемых записей. Значение none очищает TTL по умолчанию
key hmac:keyname secret	Указывает, что все обновления должны быть подписаны TSIG с использованием пары keyname-secret. Если указан hmac, он устанавливает используемый алгоритм подписи. Значение по умолчанию – hmac-md5; если MD5 отключен, то по умолчанию используется hmac-sha256. Команда key переопределяет любой ключ, указанный в командной строке с помощью -u или -k
gsstsig	Эта команда использует GSS-TSIG для подписи обновлений. Это эквивалентно указанию -g в командной строке
oldgsstsig	Эта команда использует версию GSS-TSIG для Windows 2000 для подписи обновлений. Это эквивалентно указанию -o в командной строке
realm [realm_name]	При использовании GSS-TSIG эта команда указывает использование realm_name вместо realm по умолчанию в krb5.conf. Если realm не указан, сохраненная realm очищается
check-names [yes_or_no]	Включить или выключить обработку check-names для добавляемых записей. Check-names не влияет на предварительные условия или удаляемые записи. По умолчанию обработка check-names включена. Если обработка check-names завершается неудачей, запись не добавляется в сообщение UPDATE
prereq nxdomain domain-name	Эта команда требует, чтобы не существовало ни одной записи ресурса любого типа с именем domain-name
prereq yxdomain domain-name	Эта команда требует, чтобы существовал domain-name (как минимум одна запись ресурса любого типа)
prereq nxrrset domain-name class type	Эта команда требует, чтобы не существовало ни одной записи ресурса указанного типа, класса и domain-name. Если class не указан, предполагается IN (Интернет)
prereq yxrrset domain-name class type	Для этой команды требуется, чтобы существовала запись ресурса указанного типа, класса и доменного имени. Если class не указан, предполагается IN (Интернет)

Окончание таблицы 77

Команда	Описание
prereq yxrrset domain-name class type data	С помощью этой команды данные из каждого набора предварительных условий этой формы, имеющих общий тип, класс и доменное имя, объединяются для формирования набора RR. Этот набор RR должен точно соответствовать набору RR, существующих в зоне с указанным типом, классом и доменным именем. Данные записываются в стандартном текстовом представлении RDATA записи ресурса
update delete domain-name ttl class type data	Удалить все записи ресурсов с именем domain-name. Если указаны type и data, удаляются только соответствующие записи ресурсов. Если class не указан, предполагается класс Internet. TTL игнорируется и допускается только для совместимости
update add domain-name ttl class type data	Добавить новую запись ресурса с указанным ttl, class и data
show	Отобразить текущее сообщение, содержащее все предварительные условия и обновления, указанные с момента последней отправки
send	Отправить текущее сообщение (эквивалентно вводу пустой строки)
answer	Отобразить ответ
debug	Включить отладку
version	Вывести номер версии
help	Вывести список команд

Примечание. Строки, начинающиеся с точки с запятой (;), являются комментариями и игнорируются.

При использовании утилиты `nsupdate` для динамического обновления DNS-записей в доменных средах AD, необходимо использовать механизм аутентификации GSS-TSIG, который использует Kerberos-билет для аутентификации машины в домене. Kerberos-билет используется при обновлении DNS-записей с помощью `nsupdate` с флагом `-g`.

Перед выполнением команды `nsupdate -g` необходимо получить Kerberos-билет для машинного аккаунта с помощью команды:

```
# kinit -k 'MACHINENAME$'
```

Примечание. Имя машинного аккаунта можно узнать, используя команду `hostname -s`. В команде `kinit` имя машинного аккаунта нужно указывать в верхнем регистре со знаком \$, например:

```
# hostname -s  
comp01  
# kinit -k 'COMP01$'
```

В следующих примерах показано использование команды `nsupdate` для добавления и удаления записей ресурсов из зоны `test.alt`:

- удалить записи А для `oldhost.test.alt` и добавить запись А для `newhost.test.alt` с IP-адресом `192.168.0.195`:

```
# nsupdate -g
> update delete oldhost.test.alt A
> update add newhost.test.alt 86400 A 192.168.0.195
> send
```

Новая запись будет имеет TTL 1 день (86400 секунд);

- указать предварительное условие перед обновлением DNS-сервера

```
# nsupdate -g
> prereq nxdomain nickname.test.alt
> update add nickname.test.alt 86400 CNAME somehost.test.alt
> send
```

Предварительное условие позволяет серверу имен проверить, нет ли записей о ресурсах любого типа для `nickname.test.alt`. Если в зоне есть записи ресурсов, запрос на обновление не выполняется. Если этого имени не существует, добавляется CNAME.

10.6.2.4. Оснастка DNS в RSAT

Оснастка DNS в RSAT позволяет администраторам Windows удаленно управлять DNS-записями через графический интерфейс. С его помощью можно добавлять, удалять и изменять DNS-записи.

Примечание. Для возможности администрирования DNS с клиента Windows должна быть установлена оснастка DNS MMC (см. п. 10.4.2.3).

Существуют следующие известные проблемы если используется внутренний сервер DNS:

- очистка еще не реализована. Возвращается сообщение об ошибке «This function is not supported on this system»;
- условные пересылки еще не реализованы. Возвращается то же сообщение об ошибке, что и выше;
- пересылку DNS можно изменить только в `smb.conf`, а не через оснастку MMC;

- создание статических записей. Когда создается статическая запись, она имеет временную метку и опцию «Delete this record when it becomes stale». В Windows AD статические записи имеют «статическую» временную метку и не могут быть случайно удалены.

Для подключения к своему DNS-серверу в оснастке DNS необходимо в контекстном меню «DNS» выбрать пункт «Connect to DNS Server...» (рис. 484). В открывшемся окне следует выбрать пункт «The following computer», ввести в поле имя домена (также можно использовать IP-адрес или FQDN), установить отметку «Connect to the special computer now» (рис. 485) и нажать кнопку «OK».

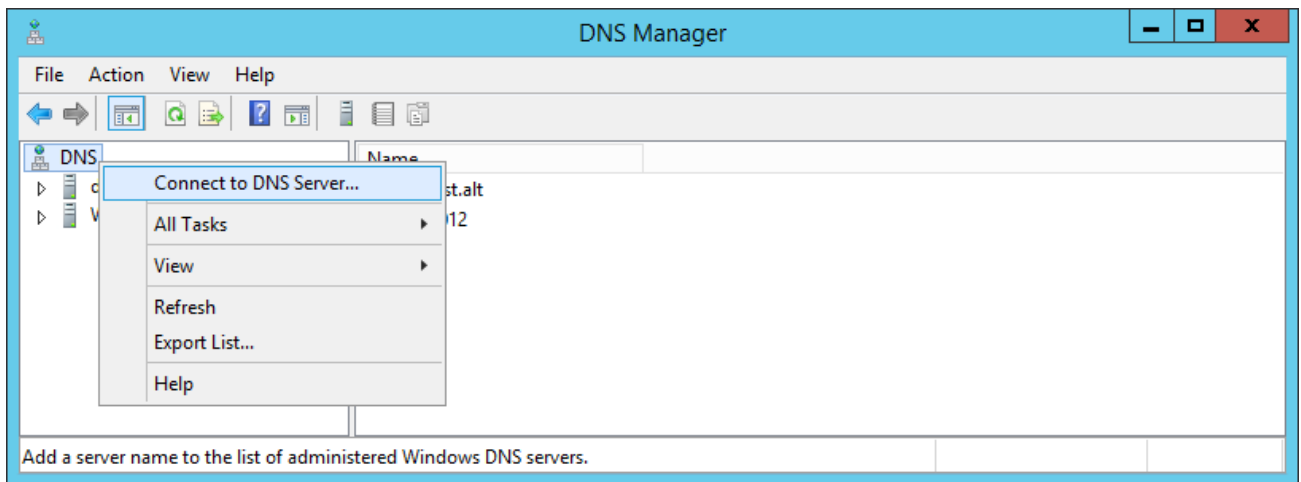


Рис. 484 – Подключение к DNS-серверу



Рис. 485 – Адрес DNS-сервера

10.6.2.4.1. Работа с DNS-записями

Чтобы добавить новую запись необходимо:

- 1) перейти в зону, в которую нужно добавить новую запись;
- 2) в контекстном меню зоны выбрать тип записи (рис. 486);
- 3) заполнить поля и сохранить запись, нажав кнопку «Add Host» (рис. 487).

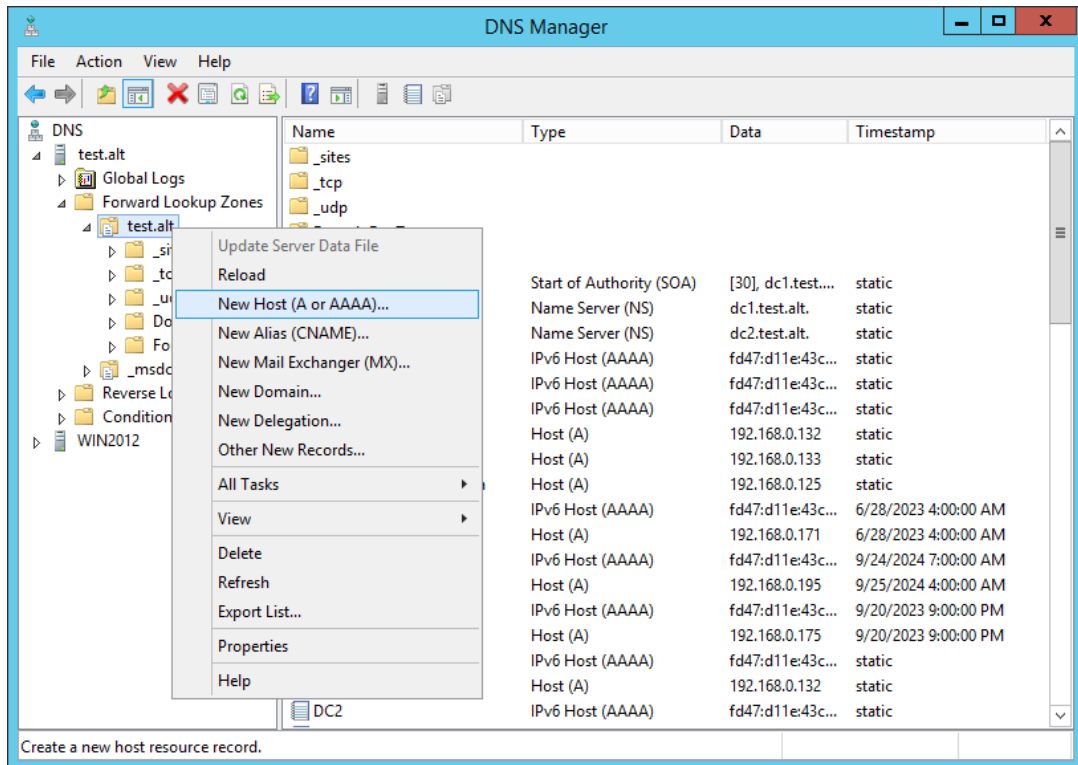


Рис. 486 – Добавление DNS-записи

New Host

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

IP address:

Create associated pointer (PTR) record

Allow any authenticated user to update DNS records with the same owner name

Рис. 487 – Новая A-запись

Для обновления существующей записи необходимо:

- 1) перейти в зону, содержащую запись, которую нужно изменить;
- 2) в контекстном меню записи выбрать пункт «Properties» (рис. 488);
- 3) отредактировать запись и сохранить изменения, нажав кнопку «Apply» (рис. 489).

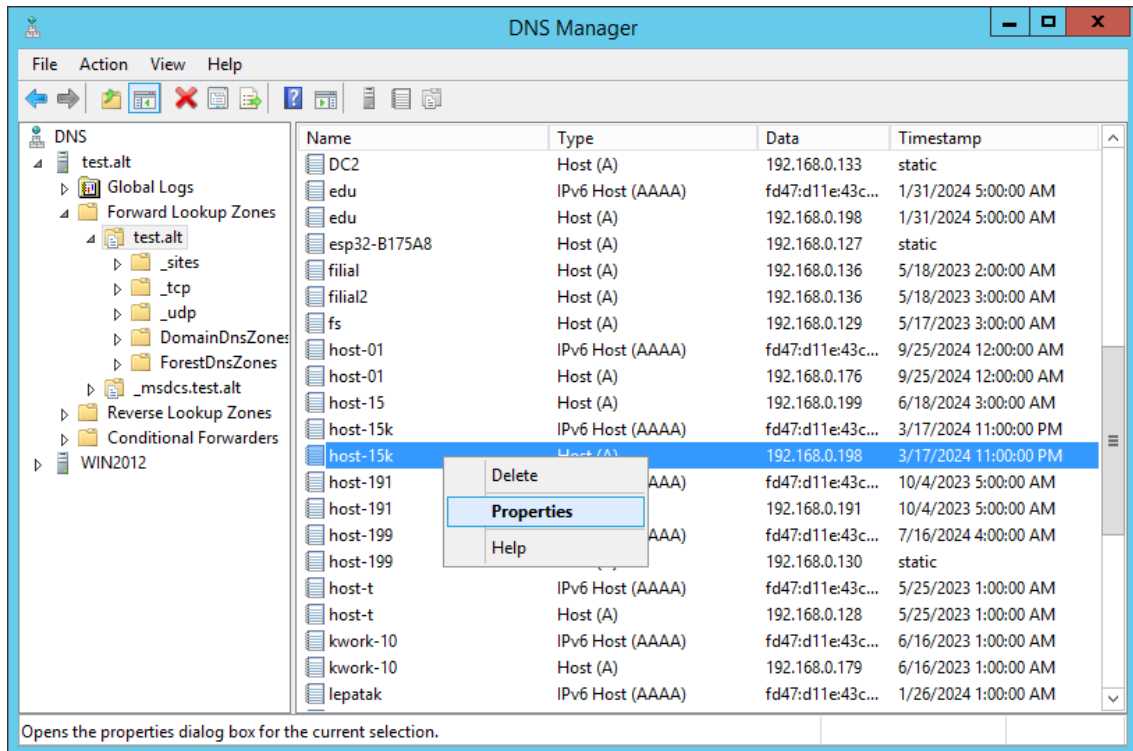


Рис. 488 – Изменение DNS-записи

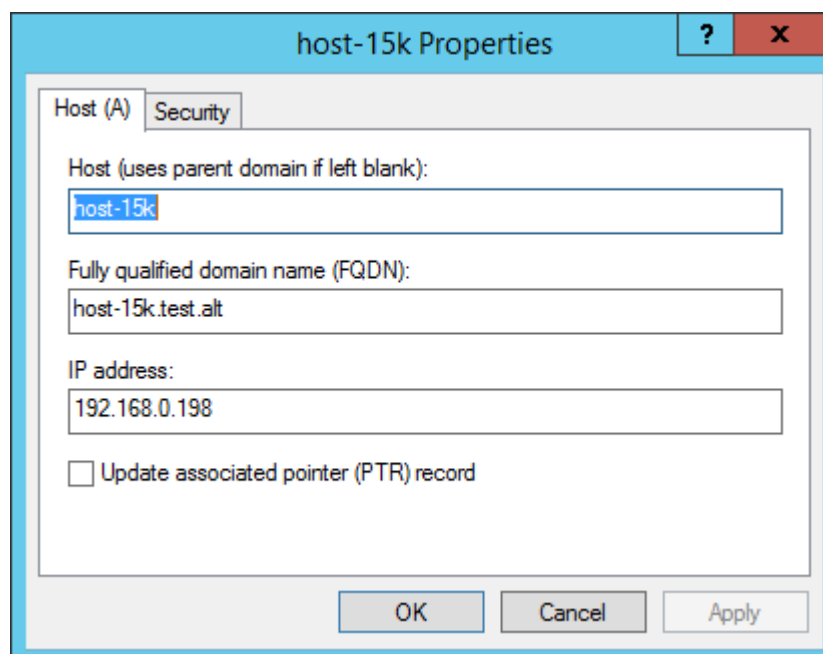


Рис. 489 – Параметры DNS-записи

Для удаления записи необходимо:

- 1) перейти в зону, содержащую запись, которую нужно удалить;
- 2) в контекстном меню записи выбрать пункт «Delete» (рис. 490).

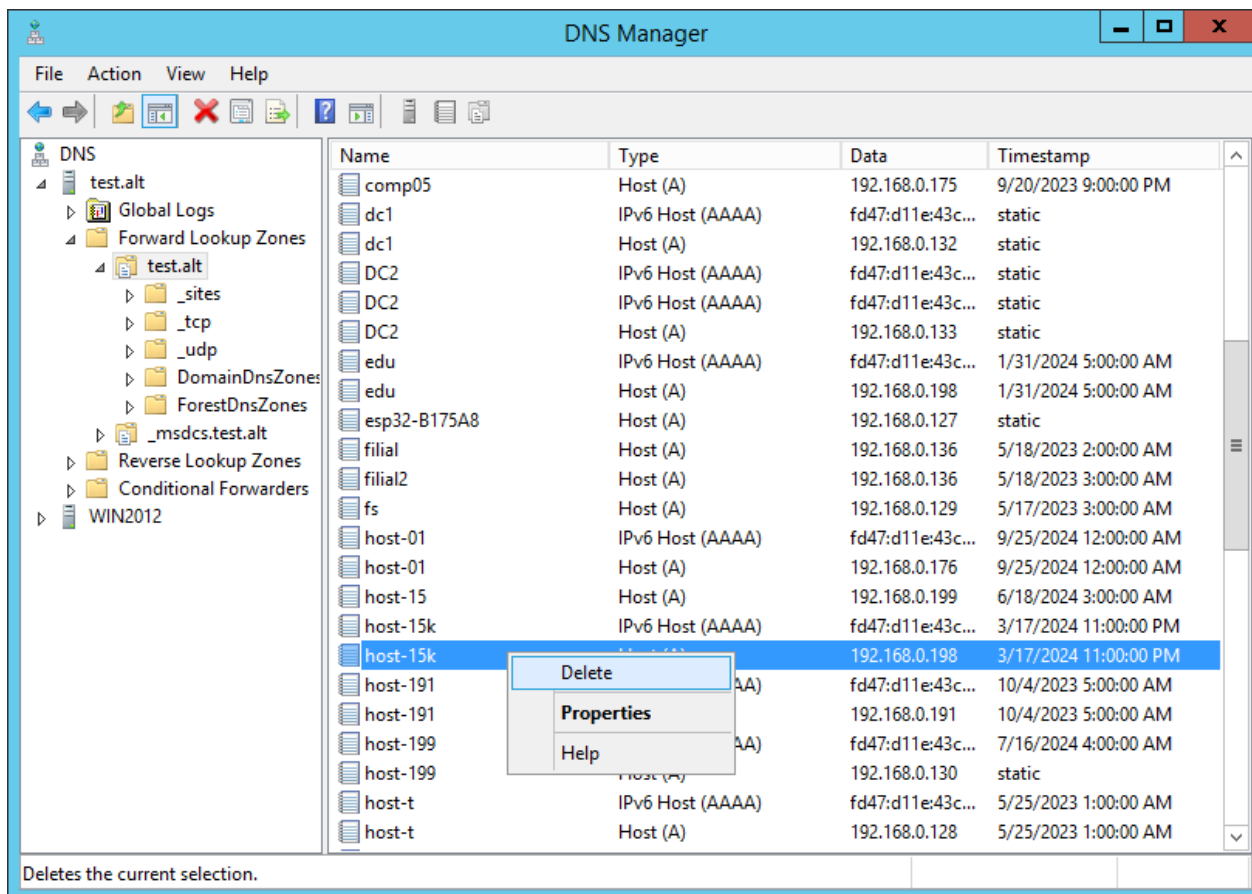


Рис. 490 – Удаление DNS-записи

10.6.2.4.2. Работа с DNS-зонами

В качестве примера рассмотрено добавление зоны обратного просмотра:

- 1) в контекстном меню зоны обратного просмотра (Reverse Lookup Zones) выбрать пункт «New Zone...» (рис. 491);
- 2) на втором шаге мастера создания новой зоны выбрать «Primary zone» и установить отметку в пункте «Store the zone in Active Directory» (рис 492);
- 3) на следующем шаге мастера указать область репликации зоны (рис. 493);
- 4) указать имя зоны обратного просмотра (рис. 494);
- 5) включить динамическое обновление (рис. 495);
- 6) завершить работу мастера.

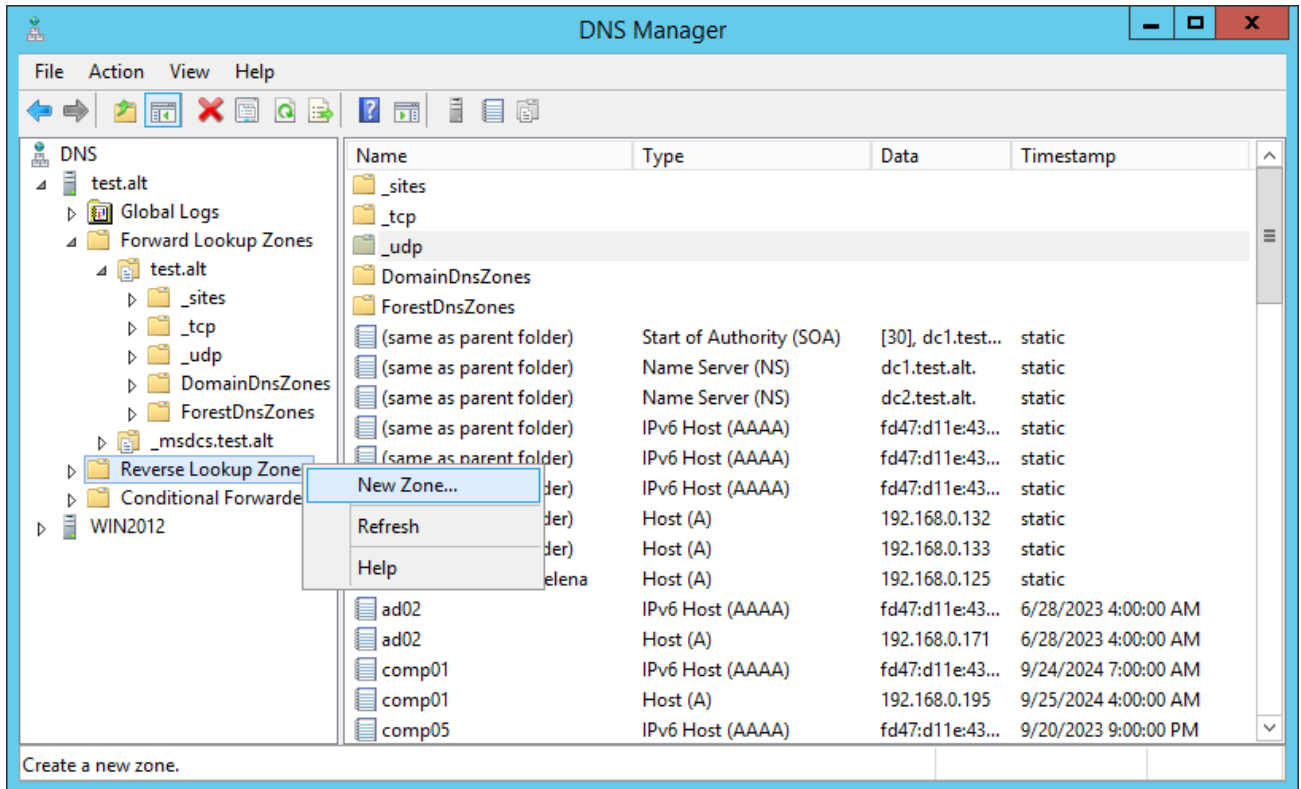


Рис. 491 – Добавление зоны обратного просмотра

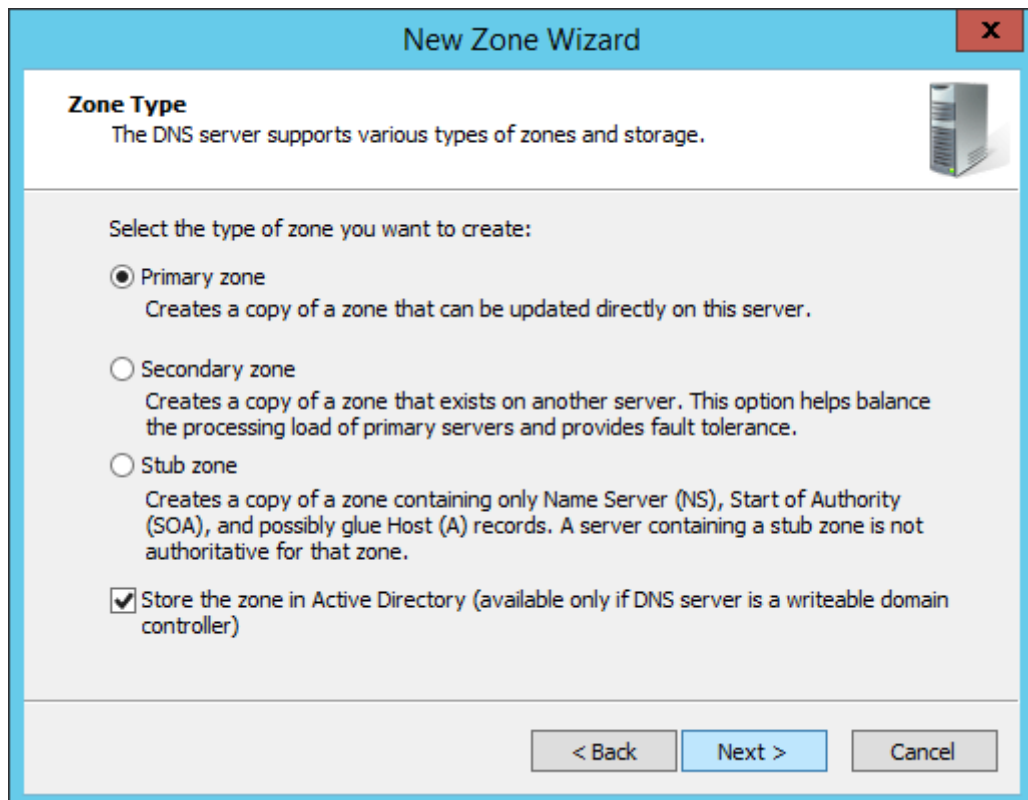


Рис. 492 – Выбор типа зоны

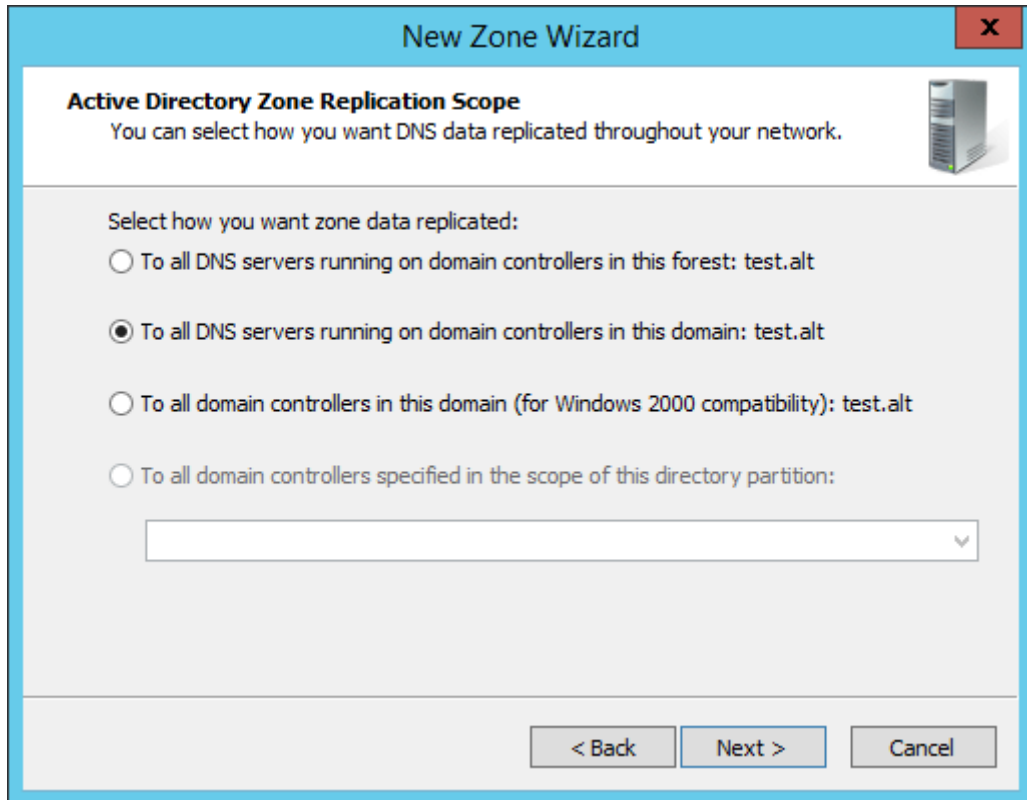


Рис. 493 – Область репликации зоны

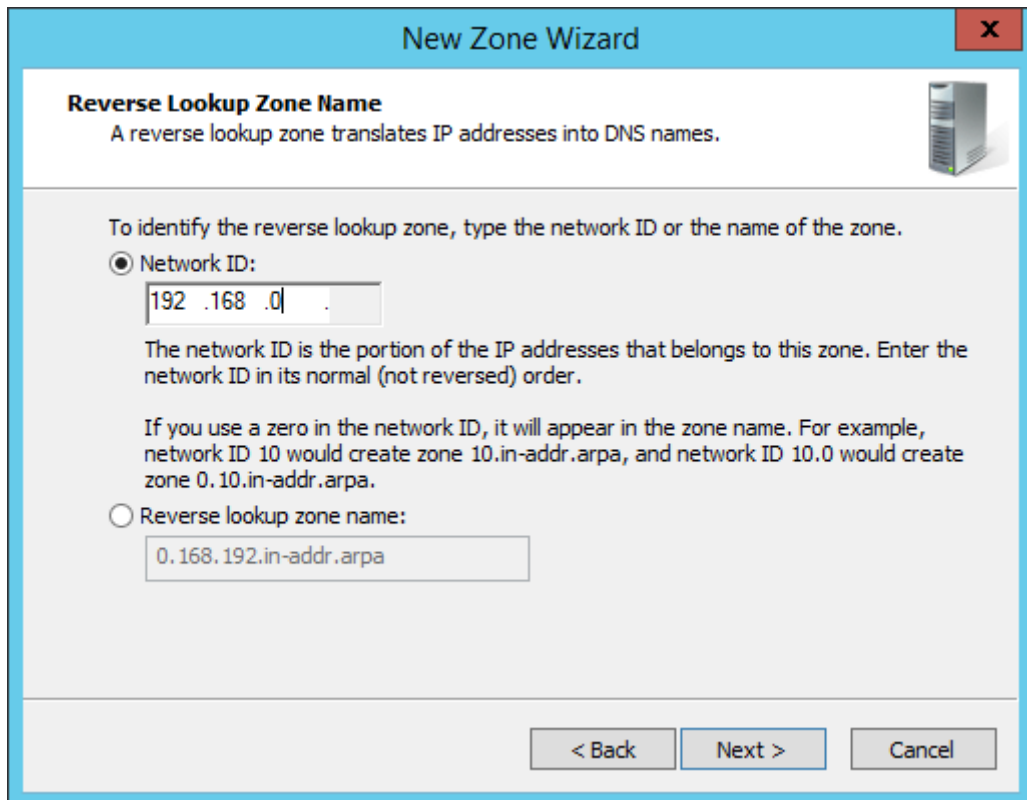


Рис. 494 – Имя зоны обратного просмотра

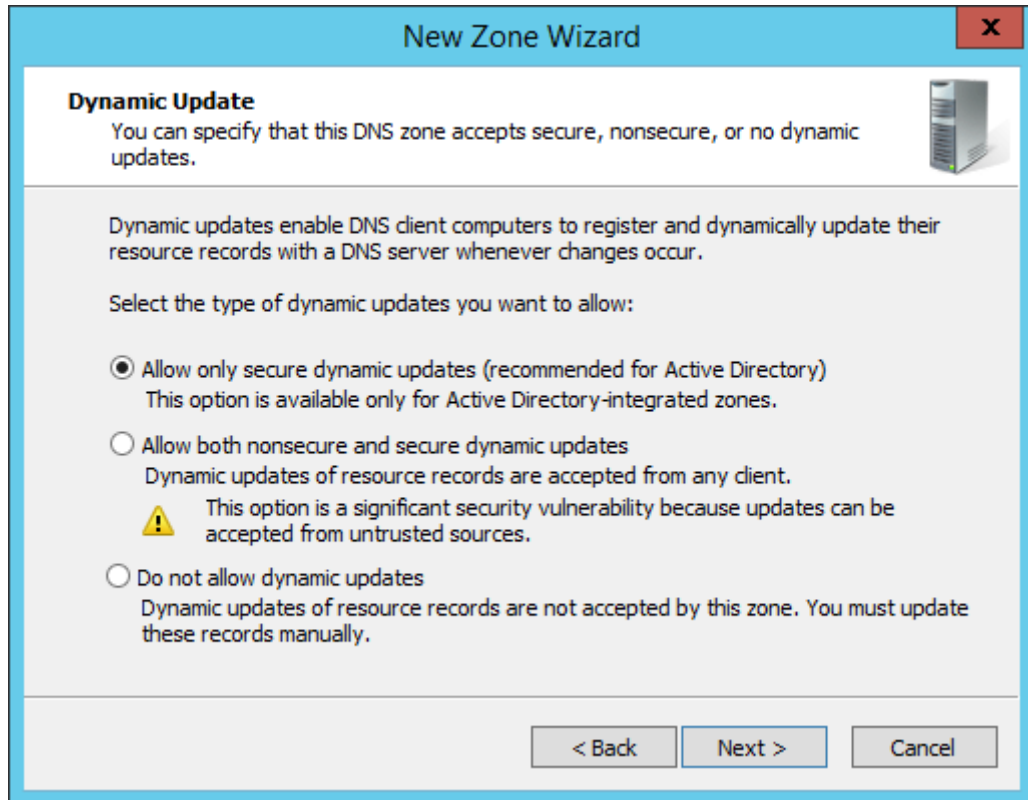


Рис. 495 – Динамическое обновление

Новая зона будет активна сразу, без перезапуска Samba или BIND.

Для удаления зоны следует в контекстном меню зоны выбрать пункт «Delete» (рис. 496).

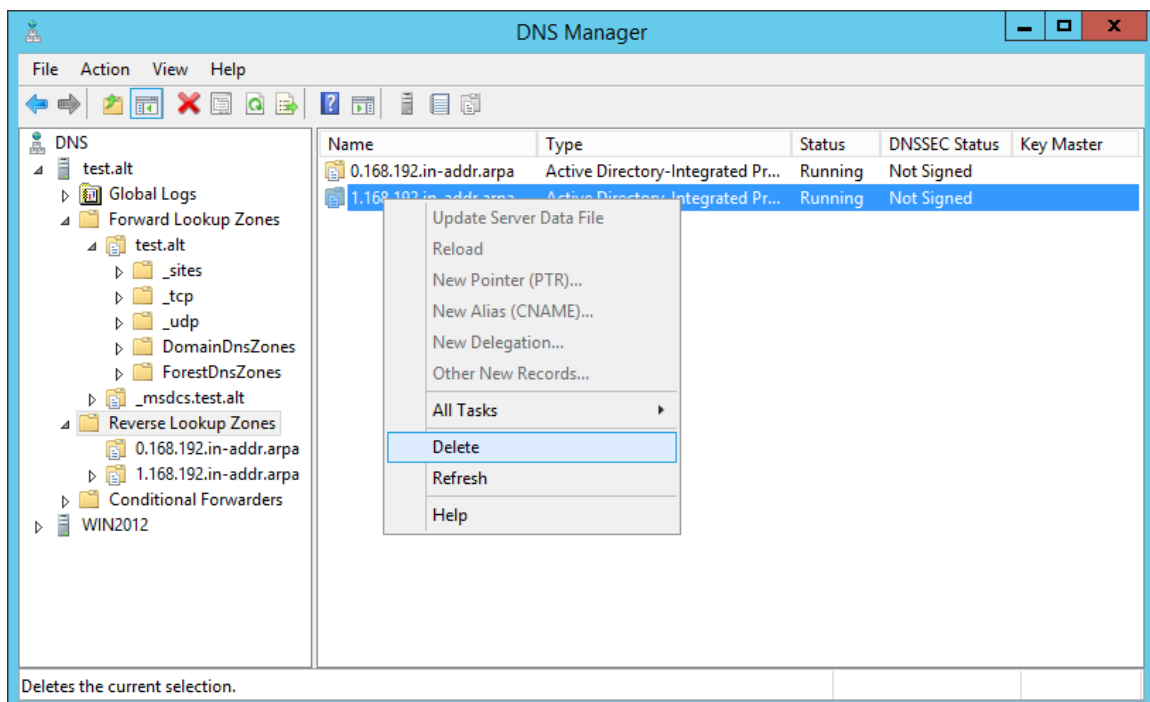


Рис. 496 – Удаление зоны

10.6.2.5. Динамическое обновление DNS-записей

Используются следующие механизмы обновления DNS-записей:

- на стороне DHCP: динамическое обновление DNS-записей часто осуществляется с помощью DHCP-серверов. В частности, такие системы как ISC DHCP и Kea DHCP могут автоматически обновлять записи на DNS-сервере при выдаче нового IP-адреса клиенту;
- на стороне клиента: в доменных средах с использованием Linux-клиентов для взаимодействия с доменом могут использоваться службы Winbind и SSSD для обновления DNS-записей. На Windows-клиентах обновление происходит через встроенные функции операционных систем. Кроме того, обновление записей может быть выполнено вручную администраторами.

10.6.2.5.1. На стороне клиента

10.6.2.5.1.1. SSSD

Включить обновление IP-адресов службой sssd можно несколькими способами:

- отредактировав файл `/etc/sss/sss.conf`;
- в модуле ЦУС «Аутентификация» (пакет `alterator-auth`);
- применением `control`;
- групповыми политиками.

10.6.2.5.1.1.1. Настройка через файл `/etc/sss/sss.conf`

В файл конфигурации службы SSSD (`/etc/sss/sss.conf`) в секцию с параметрами домена можно добавить опции, приведенные в таблице 78.

Т а б л и ц а 78 – Параметры настройки автоматического обновления DNS

Параметр	Описание	Значение по умолчанию
dyndns_update	Позволяет включить или отключить автоматическое обновление DNS-записей (защищенных с помощью GSS-TSIG) IP-адресом клиента через SSSD. Соответственно, администратору домена требуется только разрешить защищенные обновления для зоны DNS. Для обновления будет использован IP-адрес LDAP-соединения AD, если с помощью параметра dyndns_iface не указано иное	true
dyndns_ttl	Значение TTL, которое применяется при обновлении DNS-записи клиента. Если dyndns_update имеет значение false, этот параметр не имеет никакого эффекта. Если администратором установлено значение TTL на стороне сервера, оно будет переопределено этим параметром	3600 (секунд)
dyndns_iface	Позволяет указать интерфейс или список интерфейсов, IP-адреса которых должны использоваться для динамических обновлений DNS. Специальное значение «*» подразумевает, что следует использовать IP-адреса всех интерфейсов. Если dyndns_update имеет значение false, этот параметр не имеет никакого эффекта.	IP-адреса интерфейса, который используется для подключения LDAP AD
dyndns_refresh_interval	Определяет как часто внутреннему серверу следует выполнять периодическое обновление DNS в дополнение к автоматическому обновлению, выполняемому при переходе внутреннего сервера в сетевой режим. Этот параметр применим только в том случае, если для параметра dyndns_update установлено значение true. Следует обратить внимание, что наименьшее допустимое значение составляет 60 секунд: если будет указано меньшее значение, параметр примет наименьшее допустимое значение (60 секунд)	86400 (24 часа)
dyndns_force_tcp	Должна ли утилита nsupdate по умолчанию использовать TCP для обмена данными с сервером DNS	false (разрешить nsupdate выбрать протокол)

Окончание таблицы 78

Параметр	Описание	Значение по умолчанию
dyndns_update_ptr	<p>Определяет будет ли обновляться клиентская PTR-запись (защищенная с помощью GSS-TSIG) при обновлении DNS-записей клиента. Применимо, только если параметр dyndns_update имеет значение true.</p> <p>Следует обратить внимание, что параметр dyndns_update_per_family не применяется для обновлений записей PTR. Эти обновления всегда отправляются отдельно</p>	true
dyndns_auth	<p>Следует ли утилите nsupdate использовать проверку подлинности GSS-TSIG для защищенных обновлений сервера DNS. Незащищенные отправления можно отправлять, установив этот параметр в значение none</p>	GSS-TSIG
dyndns_auth_ptr	<p>Следует ли утилите nsupdate использовать проверку подлинности GSS-TSIG для защищенных обновлений PTR сервера DNS. Незащищенные отправления можно отправлять, установив этот параметр в значение none</p>	То же, что и dyndns_auth
dyndns_server	<p>Сервер DNS, который следует использовать для выполнения обновления DNS. В большинстве конфигураций рекомендуется не устанавливать значение для этого параметра.</p> <p>Установка этого параметра имеет смысл для сред, в которых сервер DNS отличается от сервера данных идентификации.</p> <p>Следует обратить внимание, что этот параметр используется только для резервной попытки, которая выполняется если предыдущая попытка с использованием автоматически определенных параметров завершилась неудачей</p>	none (разрешить nsupdate выбрать сервер)
dyndns_update_per_family	<p>По умолчанию обновление DNS выполняется за два шага: обновление IPv4, а затем обновление IPv6. В некоторых случаях может быть желательно выполнить обновление IPv4 и IPv6 за один шаг.</p>	true

Например:

```
[domain/TEST.ALT]
.....
#Включить обновление прямых записей (A/AAAA записей)
dyndns_update = true

#Включить обновление обратных записей (PTR записей)
dyndns_update_ptr = true
#Задать интервал обновления в секундах.
#По умолчанию - 0, и обновление выполняется
#только один раз при запуске службы SSSD.
#Если интервал менее 60 секунд,
#то обновление выполняется раз в 60 секунд.
#Если адрес после предыдущего обновления
#не изменялся - обновление не выполняется.
dyndns_refresh_interval = 60
```

Примечание. Чтобы загрузить новые параметры конфигурации необходимо перезапустить службу SSSD:

```
# systemctl restart sssd
```

10.6.2.5.1.1.2. Настройка через ЦУС

Некоторые настройки автоматического обновления DNS для SSSD можно настроить в модуле ЦУС «Аутентификация». Подробнее см. п. 10.6.12.2.

10.6.2.5.1.1.3. При помощи механизма control

Список control, используемых для настройки автоматического обновления DNS для SSSD, представлен в таблице 79.

Т а б л и ц а 79 – control для настройки автоматического обновления DNS для SSSD

control	Опция в файле /etc/sss/sss.conf	Описание
sss-dyndns-refresh-interval	dyndns_refresh_interval	<p>Определяет как часто серверная часть должна выполнять периодическое обновление DNS в дополнение к автоматическому обновлению, выполняемому при подключении серверной части к сети. Этот параметр применим только в том случае, если для параметра dyndns_update установлено значение true.</p> <p>Доступные режимы:</p> <ul style="list-style-type: none"> - INTERVAL – задать интервал; - disabled – значение по умолчанию (86400); - unknown
sss-dyndns-ttl	dyndns_ttl	<p>Срок жизни, применяемый к DNS-записи клиента при ее обновлении. Если dyndns_update имеет значение false, этот параметр не имеет никакого эффекта.</p> <p>Доступные режимы:</p> <ul style="list-style-type: none"> - TTL – задать TTL; - disabled – значение по умолчанию (3600); - unknown
sss-dyndns-update	dyndns_update	<p>Позволяет включить или отключить автоматическое обновление DNS-записей (защищенных с помощью GSS-TSIG) с IP-адресом клиента через SSSD.</p> <p>Доступные режимы:</p> <ul style="list-style-type: none"> - enabled – автоматическое обновление DNS-записи клиента через SSSD включено; - disabled – автоматическое обновление DNS-записи клиента через SSSD отключено; - default – настройка автоматического обновления DNS-записи клиента через SSSD задана по умолчанию в пакете; - unknown
sss-dyndns-update-ptr	dyndns_update_ptr	<p>Определяет будет ли обновляться клиентская PTR-запись при обновлении DNS-записей клиента.</p> <p>Применимо, только если параметр dyndns_update имеет значение true.</p> <p>Доступные режимы:</p> <ul style="list-style-type: none"> - enabled – автоматическое обновление DNS-записи обратной зоны через SSSD включено; - disabled – автоматическое обновление DNS-записи обратной зоны через SSSD отключено; - default – настройка автоматического обновления DNS-записи обратной зоны задана по умолчанию в пакете; - unknown

Список всех возможных настроек автоматического обновления DNS для SSSD с помощью `control` можно получить, выполнив команду:

```
# control | grep sssd-dyndns
sssd-dyndns-refresh-interval unknown          (disabled INTERVAL)
sssd-dyndns-ttl unknown                      (disabled TTL)
sssd-dyndns-update unknown                   (disabled enabled default)
sssd-dyndns-update-ptr unknown               (disabled enabled default)
```

Например, чтобы SSSD автоматически обновлял на сервере DNS AD IP-адрес клиента, необходимо включить `control sssd-dyndns-update`:

```
# control sssd-dyndns-update enabled
```

и перезапустить службу SSSD:

```
# systemctl restart sssd
```

Проверка:

```
# control sssd-dyndns-update
enabled
```

10.6.2.5.1.1.4. При помощи групповых политик

С помощью групповых политик в «Альт Домен» можно централизованно управлять настройками обновления DNS-записей на всех клиентах в сети. В настоящее время с помощью групповых политик можно сконфигурировать параметры `dyndns_update` и `dyndns_update_ptr`. Подробнее см. п. 10.4.6.4.2.

10.6.2.5.1.2. Samba Winbind

Samba Winbind не поддерживает возможность динамического обновления DNS-записей. Для обхода этой проблемы была разработана утилита, реализующая динамическое обновление адресов на DNS-сервере при использовании Winbind в качестве клиента домена – `winbind-dnsupdate`.

Для возможности работы с программой необходимо установить пакет `samba-winbind-dnsupdate`:

```
# apt-get install samba-winbind-dnsupdate
```

Активировать и запустить таймер, который в свою очередь запускает сервис:

```
# systemctl enable --now winbind-dnsupdate.timer
```

Основным функционалом утилиты `winbind-dnsupdate` является обновление IPv4 (A), IPv6 (AAAA) и соответствующих PTR DNS-записей. Для обновления DNS-записей `winbind-dnsupdate` использует файл `/etc/resolv.conf`.

Синтаксис команды winbind-dnsupdate:

```
winbind-dnsupdate [опции]
```

Опции команды winbind-dnsupdate приведены в таблице 80. При запуске без параметров скрипт обновляет А запись.

Т а б л и ц а 80 – Опции команды winbind-dnsupdate

Ключ	Описание
-h, --help	Вывести справку о команде
-v, --version	Вывести версию
-a, --all	Включить обновление всех записей
-6, --update-ipv6	Включить обновление IPv6 (AAAA) записей
-d, --daemon	Отправлять логи в journald
-t, --ttl <time>	Задать TTL («время жизни», указывает, как долго настройки DNS должны храниться в кеше, прежде чем они будут автоматически обновлены)
--allow-ipv4-ptr-update	Включить обновление обратной DNS-записи IPv4 (A) PTR
--allow-ipv6-ptr-update	Включить обновление обратной DNS-записи IPv6 (AAAA) PTR

Пример запуска скрипта winbind-dnsupdate:

```
# winbind-dnsupdate -a
[INFO]: Hostname: comp01.test.alt.
[INFO]: Check winbind status.
[INFO]: Winbind is running. Continue.
[INFO]: Trying to get the site name.
[INFO]: Site: Default-First-Site-Name.
[INFO]: Get host credentials.
[INFO]: Retrieving host credentials successfully.
[INFO]: Trying to get a list of domain controllers in site.
[INFO]: Success.
[INFO]: Trying to find an available DNS server.
[INFO]: Checking the availability of DNS server on dc1.test.alt..
[INFO]: DNS server on dc1.test.alt. available.
[INFO]: Update IPv4.
[INFO]: Trying to get IPv4 address of a domain controller.
[INFO]: Successful. DC info:
[INFO]: Domain controller name: dc1.test.alt.
[INFO]: Domain controller IPv4: 192.168.0.132.
[INFO]: Trying parse connection interface name.
[INFO]: Successful. Intraface name: enp0s3.
[INFO]: Checking the existence of A record.
[INFO]: IPv4 record exists.
[INFO]: Checking whether the IPv4 records needs to be updated.
[INFO]: Current IPv4 address: 192.168.0.195.
[INFO]: IPv4 address in DNS server: 192.168.0.195.
[INFO]: The IPv4 address of interface enp0s3 has not been
changed.
[INFO]: The update IPv4 was skipped.
```

```
[INFO]: IPv4 update was successful.
[INFO]: The update was successful.
[INFO]: Destroy host credential.
```

В пакете вместе со скриптом предоставляются systemd сервис и таймер. Таймер запускает systemd сервис для обновления DNS-записи через 5 минут после загрузки системы и затем каждый час. Просмотреть параметры таймера можно, выполнив команду:

```
# systemctl cat winbind-dnsupdate.timer
# /lib/systemd/system/winbind-dnsupdate.timer
[Unit]
Description=Update dns record Daily and on boot

[Timer]
OnBootSec=5min
OnUnitActiveSec=60min

[Install]
WantedBy=timers.target
```

Чтобы изменить частоту запуска systemd сервиса, необходимо отредактировать настройки таймера:

1) выполнить команду:

```
# systemctl edit winbind-dnsupdate.timer
```

2) добавить следующие строки после строки Anything between here and the comment below will become the new contents of the file:

```
[Timer]
OnUnitActiveSec=
OnUnitActiveSec=120min
OnUnitActiveSec= очистит предыдущее определение (60min)
OnUnitActiveSec=120min установит новое значение (120min).
```

3) сохранить внесенные изменения;

4) перезагрузить таймер для применения изменений:

```
# systemctl daemon-reload
```

Примечание. Команда `systemctl edit winbind-dnsupdate.timer` открывает текстовый редактор с конфигурацией `winbind-dnsupdate.timer`, куда можно внести изменения. Этот подход позволяет создавать или изменять так называемые «дополнения» (overrides) для systemd сервиса, не изменяя оригинальный файл сервиса, который находится в `/usr/lib/systemd/system/`. Это важно, потому что оригинальные файлы могут быть перезаписаны при обновлении пакетов. При выполнении этой команды создается каталог `/etc/systemd/system/winbind-dnsupdate.timer.d/`, в котором, после сохранения изменений, появляется файл `override.conf`. В этом файле можно задать новые параметры или изменить существующие параметры сервиса.

10.6.2.5.1.3. Windows клиент

В Windows клиенты автоматически обновляют DNS-записи, такие как A и PTR, при изменении IP-адресов или имени компьютера. Этот процесс инициируется службой DHCP-клиента, которая отправляет обновления на DNS-сервер. Обновления происходят каждые 24 часа (по умолчанию) или могут быть инициированы вручную командой `ipconfig /registerdns`. Для DHCP-клиентов DHCP-сервер может выполнять эти обновления от имени клиента, что снижает необходимость ручного администрирования.

10.6.2.6. Обновление IP-адресов вручную

Для обновления IP-адресов вручную существует несколько способов:

- с помощью команды `samba-tool` (см. п. 10.6.2.2);
- с помощью утилиты `nsupdate` (см. п. 10.6.2.3);
- оснастка DNS в RSAT (см. п. 10.6.2.4).

10.6.3. Администрирование сайтов и подсетей

Для администрирования сайтов и подсетей в «Альт Домен» можно использовать подкоманду `sites` утилиты `samba-tool`.

Примечание. Для выполнения команд на удаленном компьютере можно использовать опцию `-H` или `--URL=` с указанием URI LDAP-сервера. Например:

```
# samba-tool sites list -H ldap://<DC> -Uadministrator
```

По умолчанию в качестве значения опции `-H` передается текущий узел в формате `ldap://<имя узла>`.

Команды инструмента командной строки `samba-tool` для управления сайтами приведены в таблице 81.

Команды инструмента командной строки `samba-tool` для управления подсетями приведены в таблице 82.

Т а б л и ц а 81 – Команды управления сайтами инструмента samba-tool

Команда	Описание	Примечание
sites create <сайт> [опции]	Добавить новый сайт	В качестве аргумента (сайт) ожидается общее имя (CN) сайта. После создания сайта в него могут быть добавлены контроллеры домена, например, путем передачи имени сайта в параметре --site=SITE при выполнении операции присоединения (см. п. 10.2.3)
sites list [опции]	Вывести список сайтов	Подкоманда поддерживает два формата представления информации о сайтах: - без дополнительных параметров – список общих имен (CN) сайтов; - с параметром --json – вывод подробной информации о каждом сайте в формате JSON
sites remove <сайт> [опции]	Удалить сайт	В качестве аргумента (сайт) ожидается общее имя (CN) сайта.
sites subnet <подкоманда>	Подкоманды управления подсетью	См. таблицу 82
sites view <сайт> [опции]	Вывести информацию об отдельном сайте	В качестве аргумента (сайт) ожидается общее имя (CN) сайта. Подкоманда выводит тот же набор атрибутов сайта, что и подкоманда samba-tool sites list --json

Т а б л и ц а 82 – Команды управления подсетями инструмента samba-tool

Команда	Описание	Примечание
sites subnet create <подсеть> <сайт> [опции]	Создать новую подсеть	Параметры вызова: - подсеть – IP-адрес и маска подсети; - сайт – сайт, за которым будет закреплена подсеть
sites subnet list <сайт> [опции]	Вывести список подсетей сайта	В качестве аргумента (сайт) ожидается общее имя (CN) сайта. Подкоманда поддерживает два формата представления информации о подсетях: - без дополнительных параметров – список общих имен (CN) подсетей; - с параметром --json – вывод подробной информации о каждой подсети в формате JSON
sites subnet remove <подсеть> [опции]	Удалить подсеть	В качестве аргумента (подсеть) ожидается общее имя (CN) существующей подсети
sites subnet set- site <подсеть> <сайт> [опции]	Закрепить подсеть за сайтом	Параметры вызова: - подсеть – IP-адрес и маска подсети; - сайт – сайт, за которым будет закреплена подсеть
sites subnet view <подсеть> [опции]	Просмотр сведений о подсети	В качестве аргумента (подсеть) ожидается общее имя (CN) существующей подсети. Подкоманда выводит тот же набор атрибутов подсети, что и подкоманда samba-tool subnet list --json

Полный список параметров каждой команды можно увидеть в справке, например:

```
# samba-tool sites list -help
```

Примеры:

- получить список сайтов в формате JSON:

```
# samba-tool sites list --json
{
  "Default-First-Site-Name": {
    "cn": "Default-First-Site-Name",
    "distinguishedName": "CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt",
    "dn": "CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt",
    "instanceType": 4,
    "name": "Default-First-Site-Name",
    "objectCategory": "CN=Site,CN=Schema,CN=Configuration,DC=test,DC=alt",
    "objectClass": [
      "top",
      "site"
    ],
    "objectGUID": "4dbdb4a9-ebe9-4ff8-a047-40da60136056",
    "showInAdvancedViewOnly": true,
    "systemFlags": 1107296256
  }
}
```

- получить информацию о сайте:

```
# samba-tool sites view Default-First-Site-Name
```

- создать сайт:

```
# samba-tool sites create newSite
Site newSite created !
```

- создать подсеть:

```
# samba-tool sites subnet create 192.168.10.0/24 newSite
Subnet 192.168.10.0/24 created !
```

- получить список подсетей для сайта newSite с подробной информацией в JSON:

```
# samba-tool sites subnet list newSite --json
{
  "192.168.10.0/24": {
    "cn": "192.168.10.0/24",
    "distinguishedName": "CN=192.168.10.0/24,CN=Subnets,CN=Sites,CN=Configuration,DC=test,DC=alt",
    "dn": "CN=192.168.10.0/24,CN=Subnets,CN=Sites,CN=Configuration,DC=test,DC=alt",
    "instanceType": 4,
    "name": "192.168.10.0/24",
```



```
"objectCategory": "CN=Subnet,CN=Schema,CN=Configuration,DC=test,DC=alt",
"objectClass": [
"top",
"subnet"
],
"objectGUID": "5ebde1f9-5369-4673-a10a-b9c10310d137",
"showInAdvancedViewOnly": true,
"siteObject": "CN=newSite,CN=Sites,CN=Configuration,DC=test,DC=alt",
"systemFlags": 1073741824
}
}
```

- закрепить подсеть 192.168.10.0/24 за сайтом newSite:

```
# samba-tool sites subnet set-site 192.168.10.0/24 newSite
Subnet 192.168.10.0/24 shifted to site newSite
```

- удалить подсеть:

```
# samba-tool sites subnet remove 192.168.10.0/24
```

10.6.4. Управление парольными политиками

В «Альт Домен» настройки пароля позволяют настроить:

- минимальные требования к длине и сложности пароля;
- длину истории паролей: предотвращает повторное использование пользователем предыдущего пароля;
- минимальный и максимальный срок действия пароля: как часто пользователь может/должен менять свой пароль;
- блокировку учетной записи: пороговое значение неудачных попыток входа в систему перед блокировкой учетной записи пользователя и продолжительность блокировки.

Для управления настройками паролей используется подкоманда `passwordsettings` утилиты `samba-tool`.

Управление политиками паролей домена производится на контроллере домена.

10.6.4.1. Глобальные парольные политики

Для просмотр текущих параметров политик паролей используется команда:

```
# samba-tool domain passwordsettings show
```

Например:

```
# samba-tool domain passwordsettings show

Password information for domain 'DC=test,DC=alt'

Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 7
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

Команда изменения параметра политик паролей:

```
# samba-tool domain passwordsettings set <параметр>
```

Возможные параметры:

- --complexity=on|off|default – должен ли пароль отвечать требованиям сложности (по умолчанию on);
- --store-plaintext=on|off|default – хранить пароли используя обратимое шифрование (по умолчанию off);
- --history-length=целое число|default – число хранимых предыдущих паролей пользователей (требование неповторяемости паролей) (по умолчанию 24);
- --min-pwd-length=целое число|default – минимальное количество символов в пароле (по умолчанию 7);
- --min-pwd-age=целое число|default – минимальный срок действия пароля (по умолчанию 1);
- --max-pwd-age=целое число|default – максимальный срок действия пароля (по умолчанию 43);
- --account-lockout-duration=целое число|default – интервал времени (в минутах), в течение которого возможность аутентификации для пользователя, превысившего количество попыток входа, будет заблокирована (по умолчанию 30);

- `--account-lockout-threshold=целое` `число|default` – допустимое количество неудачных попыток ввода пароля перед блокировкой учетной записи (по умолчанию 0 – никогда не блокировать);
- `--reset-account-lockout=целое` `число|default` – интервал времени (в минутах), по истечении которого записанное количество попыток начинается заново (по умолчанию 30).

Изменить минимальную длину пароля и количество неудачных попыток входа в систему:

```
# samba-tool domain passwordsettings set --min-pwd-length=7 --
account-lockout-threshold=3
Minimum password length changed!
Account lockout threshold changed!
All changes applied successfully!
```

Примечание. Определить, что учетная запись пользователя заблокирована после нескольких неудачных попыток входа в систему можно, если `badPwdCount` достиг своего порога и для пользователя существует параметр `lockoutTime`:

```
# samba-tool user show ivanov
...
badPwdCount: 3
badPasswordTime: 133287267974607690
lockoutTime: 133287267974607690
...
```

Чтобы разблокировать пользователя, необходимо отредактировать объект учетной записи пользователя, установив для атрибута `lockoutTime` значение 0:

```
# samba-tool user edit ivanov
Modified User 'ivanov' successfully

# samba-tool user show ivanov
...
badPasswordTime: 133287277878749270
lockoutTime: 0
...
```

Разблокировать пользователя также можно в модуле удаленного управления базой данных конфигурации (ADMC) (подробнее см. п. 10.4.5) (рис. 497).

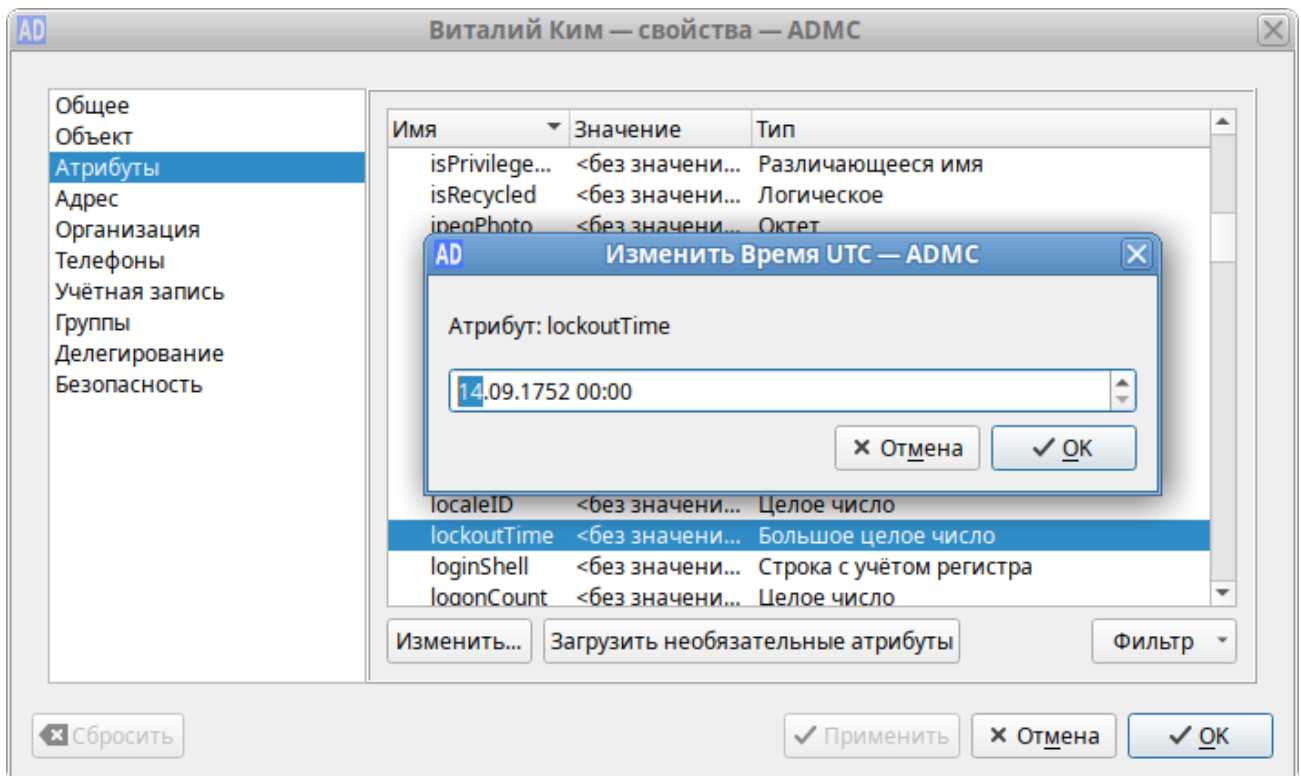


Рис. 497 – Окно модуля удаленного управления конфигурацией (ADMC)

10.6.4.2. Объекты настроек паролей (PSO)

Объекты настроек паролей (Password Settings Object, PSO) позволяют администраторам «Альт Домен» переопределять параметры политики паролей домена и настраивать более точные параметры паролей для конкретных пользователей или групп пользователей. Например, для определенных пользователей можно установить требование минимальной длины пароля, ослабить ограничения сложности для других пользователей и т. д. PSO могут применяться к группам или к отдельным пользователям.

При создании объект PSO сохраняется в LDAP по пути `CN=<имя парольной политики>,CN>Password Settings Container,CN=System,DC=<domain>`.

К одному и тому же пользователю может применяться множество различных PSO (напрямую или через группы). Если несколько PSO применяются к одному и тому же пользователю, в основном вступает в силу PSO с наименьшим приоритетом (заданный с помощью параметра `precedence`). Однако PSO, которые применяются непосредственно к пользователю, всегда превосходят PSO, унаследованные через членство в группе.

Если для пользователя не создано правила, будет применяться правило по умолчанию.

Примечание. Необходимо одновременно настраивать политику паролей для всех остальных пользователей, иначе есть риск снижения производительности при настройке PSO и применении их к пользователям. Например:

```
# samba-tool domain passwordsettings pso create PwPolicyAdmins 1 --min-pwd-length=16
# samba-tool domain passwordsettings pso apply PwPolicyAdmins "domain admins"
# samba-tool domain passwordsettings pso create PwPolicyUsers 3 --min-pwd-length=8
# samba-tool domain passwordsettings pso apply PwPolicyUsers "domain admins"
# samba-tool domain passwordsettings pso create PwPolicyService 2 --min-pwd-length=24
# samba-tool domain passwordsettings pso apply PwPolicyService "domain admins"
```

Если объектов PSO вообще нет, производительность не снижается.

Расчет PSO включает в себя расчет членства пользователя в группах, что является довольно дорогостоящим расчетом. Если PSO применяется непосредственно к пользователю (а не к группе), то дорогостоящие групповые вычисления пропускаются. Однако применение PSO непосредственно к пользователям делает управление PSO более сложным по сравнению с применением PSO к группам.

10.6.4.2.1. В ADMC

Для управления объектами настроек паролей можно использовать модуль удаленного управления базой данных конфигурации (ADMC). Подробнее см. п. 10.4.5.10.

10.6.4.2.2. С помощью samba-tool

Для работы с объектами PSO используется подкоманда `pso` утилиты `samba-tool`.

Команда изменения PSO:

```
# samba-tool domain passwordsettings pso <подкоманда>
```

Доступные подкоманды:

- `apply` – применить политику паролей PSO к пользователю или группе;
- `create` – создать новый объект настроек пароля (PSO);
- `delete` – удалить объект настроек пароля (PSO);

- `list` – вывести список всех объектов настроек пароля (PSO);
- `set` – изменить объект настроек пароля (PSO);
- `show` – показать детали объекта настроек пароля;
- `show-user` – отобразить настройки пароля, которые применяются к пользователю;
- `unapply` – обновить PSO, чтобы он больше не применялся к пользователю или группе.

Для создания нового объекта PSO используется команда:

```
# samba-tool domain passwordsettings pso create <pso-name>
<precedence> [options]
```

Подкоманда создает новую парольную политику с указанным именем (<pso-name>). Имя должно быть уникальным на уровне домена.

При создании политики может быть задан ее приоритет (<precedence>), который будет учитываться в том случае, если к пользователю или группе пользователей применяются несколько политик. Чем меньше значение параметра `precedence`, тем выше приоритет.

В качестве аргументов передаются атрибуты парольной политики с требуемыми значениями.

Примечание. Для создания политики требуется передать новое значение хотя бы для одного атрибута.

Для применения атрибутов, заданных в объекте PSO, к определенному пользователю или группе используется команда:

```
# samba-tool domain passwordsettings pso apply <pso-name> <user-
or-group-name> [options]
```

Подкоманда обеспечивает применение атрибутов парольной политики (PSO) с указанным именем (<pso-name>) к указанному пользователю или группе пользователей (<user-or-group-name>).

Пример создания и назначения парольной политики:

1) создать парольную политику:

```
# samba-tool domain passwordsettings pso create PwPolicyUser 1 \
--min-pwd-length=10
```

ЛКНВ.11100-01 90 03

Not all password policy options have been specified.

For unspecified options, the current domain password settings will be used as the default values.

```
PSO successfully created: CN=PwPolicyUser,CN>Password Settings
Container,CN=System,DC=test,DC=alt
```

```
Password information for PSO 'PwPolicyUser'
```

```
Precedence (lowest is best): 1
Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 10
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

2) назначить созданную политику пользователю ivanov:

```
# samba-tool domain passwordsettings pso apply PwPolicyUser ivanov
```

The following PSO settings apply to user 'ivanov'.

```
Password information for PSO 'PwPolicyUser'
```

```
Precedence (lowest is best): 1
Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 10
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

Note: PSO applies directly to user (any group PSOs are overridden)

Чтобы увидеть, какой PSO действует для данного пользователя, используется

команда `samba-tool pso show-user:`

```
# samba-tool domain passwordsettings pso show-user kim
```

```
No PSO applies to user 'kim'. The default domain settings apply.
Refer to 'samba-tool domain passwordsettings show'.
```

Для получения списка всех объектов PSO в домене используется команда:

```
# samba-tool domain passwordsettings pso list [options]
```

Эта подкоманда выводит список всех парольных политик (PSO), доступных в домене, в виде таблицы со столбцами Precedence и PSO name.

10.6.5. Резервное копирование и восстановление домена

10.6.5.1. Резервное копирование и восстановление из резервной копии

Инструменты резервного копирования и восстановления позволяют пересоздать домен при возникновении проблем, делающих невозможной его дальнейшую полноценную эксплуатацию.

Примером такой проблемы может служить изменение или удаление какого-либо объекта или группы объектов в базе данных службы каталогов, приводящее к неработоспособности одного из доменных сервисов. Подобное изменение реплицируется на все контроллеры домена. То есть для восстановления работоспособности такого сервиса недостаточно выполнить повторное присоединение к домену какого-либо отдельного контроллера, так как он получит копию базы данных с вызвавшим проблему изменением. В этом случае при наличии резервной копии домена без внесенного «проблемного» изменения она может быть использована для восстановления.

В процессе восстановления создается новый контроллер домена с базой данных из резервной копии. Существующие контроллеры домена должны быть остановлены и заново присоединены к нему.

Примечание. Механизм восстановления из резервной копии не должен использоваться для восстановления работоспособности отдельно взятого контроллера домена в случае возникновения на нем локальной проблемы, не затрагивающей работу всего домена. В этом случае достаточно провести диагностику и устранить проблему на контроллере домена, а затем выполнить повторное присоединение к домену для получения актуальной копии базы данных службы каталогов (см. п. 10.6.5.2).

Если контроллер домена используется и в качестве файлового сервера (что не рекомендуется), потребуется также создать отдельные резервные копии этих данных.

Поддерживаются следующие виды резервного копирования:

- online – выполняется клонирование работающей базы данных DC.

По функциональности это похоже на присоединение нового контроллера домена к сети;

- offline (локальный) – резервные копии Samba создаются в том виде, в котором они появляются на диске. Сюда входят метаданные репликации, которые являются локальными для этого конкретного контроллера домена и которые не включаются в online резервные копии. Резервную копию также можно создать, когда контроллер домена находится в автономном режиме (т. е. процесс samba фактически не запущен).
- rename (локальный) – создается файл резервной копии с переименованным доменом (предназначен только для временной замены).

Резервные копии можно создать, используя команду `samba-tool domain backup`. При этом будет создан файл резервной копии `.tar.bz2`, который будет содержать полную резервную копию домена (на основе данного контроллера домена). Этот файл резервной копии можно использовать для восстановления домена с помощью команды `samba-tool domain backup restore`.

Примечание. Следует иметь в виду, что файл резервной копии – это резервная копия домена, а не контроллера домена. Восстановление файла резервной копии создаст новый DC с информацией о домене. Чтобы восстановить последующие контроллеры домена, необходимо присоединить новые контроллеры домена к восстановленному контроллеру домена.

10.6.5.1.1. Создание резервной копии в режиме онлайн/оффлайн режимах

Схема создания резервной копии и восстановления из нее в онлайн/оффлайн режимах представлена на рис. 498.

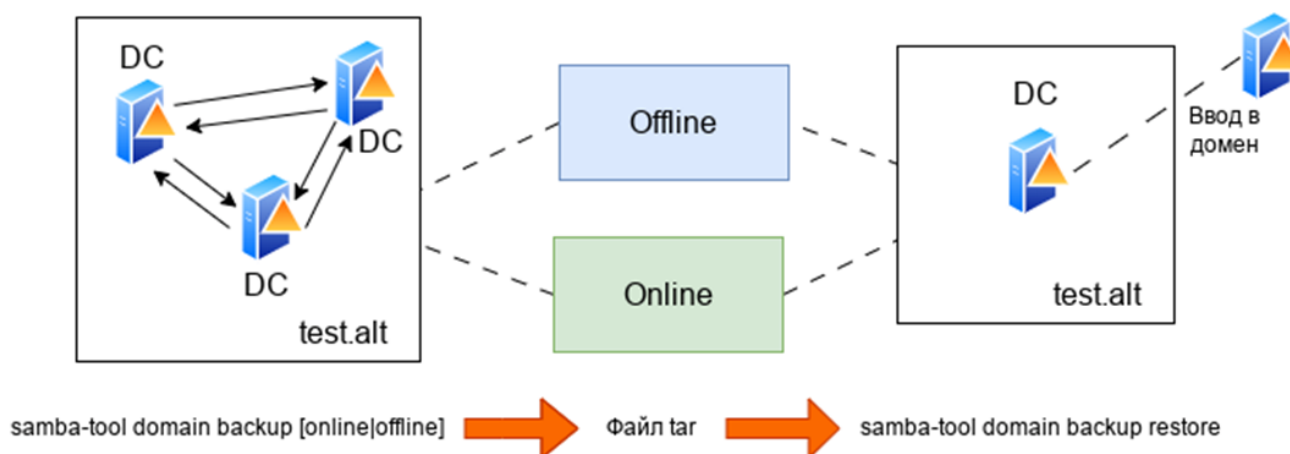


Рис. 498 – Схема создания резервной копии

10.6.5.1.1.1. Создание резервной копии в онлайн-режиме

В онлайн-режиме (online) формируется набор файлов с актуальными данными службы каталогов, не привязанными к состоянию конкретного контроллера домена.

Данный вид резервного копирования подходит в том случае, если требуется оперативно получить работоспособную долгосрочную или постоянную замену вышедшему из строя домену без детального изучения причин возникновения проблем в работе службы каталогов.

Для создания резервной копии в онлайн-режиме используется команда:

```
# samba-tool domain backup online --targetdir=<output-dir> \
--server=<DC-server> -UAdministrator
```

Эту команду можно запустить как локально на контроллере домена, так и удаленно на другом компьютере. При удаленном запуске можно указать параметр `--configfile`, чтобы в резервную копию были включены правильные настройки `smb.conf` (т. к. локальный файл `smb.conf` может не существовать или его настройки могут отличаться от настроек контроллера домена).

Пример создания резервной копии в онлайн-режиме на контроллере домена:

```
# mkdir /var/samba-backup-online
# samba-tool domain backup online \
--targetdir=/var/samba-backup-online \
--server=dcl -Uadministrator
```

```
Password for [TEST\Administrator]:
```

```
workgroup is TEST
```

```
realm is test.alt
```

```
Looking up IPv4 addresses
```

```
Looking up IPv6 addresses
```

```
Setting up share.ldb
```

```
Setting up secrets.ldb
```

```
Setting up the registry
```

```
Setting up the privileges database
```

```
Setting up idmap db
```

```
Setting up SAM db
```

```
Setting up sam.ldb partitions and settings
```

```
Setting up sam.ldb rootDSE
```

```
Pre-loading the Samba 4 and AD schema
```

A Kerberos configuration suitable for Samba AD has been generated at `/var/samba-backup-online/tmpxqc6dwts/private/krb5.conf`

Merge the contents of this file with your system `krb5.conf` or replace it with this one. Do not create a symlink!

...

```
Creating backup file /var/samba-backup-online/samba-backup-  
test.alt-2024-06-04T16-15-49.475857.tar.bz2...
```

10.6.5.1.1.2. Создание резервной копии в автономном режиме

В автономном режиме (offline) создается резервная копия локальных файлов контроллера домена, на котором запускается команда резервного копирования.

Данный вид резервного копирования оптимален для изучения причин возникновения проблем в работе службы каталогов, так как в этом режиме в резервную копию включаются дополнительные данные, как правило, не подлежащие реплицированию. В больших доменах на создание такой резервной копии требуется меньше времени, поскольку исключаются временные затраты на передачу данных из базы данных службы каталогов по сети и запись их на локальный диск.

Однако следует учитывать, что при копировании базы данных с диска потенциально повышается риск попадания в резервную копию ошибочных данных.

Примечание. Отличия автономного резервного копирования от онлайн-режима:

- резервную копию можно создать, даже если контроллер домена в данный момент не работает;
- резервная копия включает нереплицированные атрибуты, которые не сохраняются в онлайн-резервной копии;
- в копию попадают необработанные файлы базы данных, что может привести к тому, что какие-либо скрытые проблемы в БД сохранятся в резервной копии.

Для создания автономной резервной копии используется команда:

```
# samba-tool domain backup offline --targetdir=<output-dir>
```

Примечание. Несмотря на то, что этот тип резервного копирования называется автономным, контроллеру домена не нужно быть в автономном режиме при выполнении этой команды. Инструмент просто выполняет резервное копирование локальных файлов и имеет достаточную блокировку, чтобы гарантировать безопасное создание резервной копии.

Пример создания автономной резервной копии на контроллере домена:

```
# mkdir /var/samba-backup-offline  
# samba-tool domain backup offline \  
--targetdir=/var/samba-backup-offline
```

```
running backup on dirs: /var/lib/samba/private /var/lib/samba  
/etc/samba
```

```
Starting transaction on /var/lib/samba/private/secrets
Starting transaction on /var/lib/samba/private/sam.ldb
backing up /var/lib/samba/private/sam.ldb
```

...

```
adding misc file etc/lmhosts
adding misc file etc/smb.conf
Backup succeeded.
```

10.6.5.1.1.3. Восстановление домена из резервной копии

Для восстановления домена из резервной копии необходимо выполнить следующие шаги:

- 1) остановить службу каталогов (samba) на всех контроллерах домена. Этот шаг можно пропустить если используется переименованная резервная копия;
- 2) выполнить команду `samba-tool domain backup restore`, с требуемыми параметрами для восстановления базы данных домена на одном новом контроллере домена;
- 3) запустить службу каталогов на новом контроллере домена;
- 4) повторно добавить старые контроллеры домена в сеть, присоединив их к восстановленному контроллеру домена, например, выполнив команду:
`samba-tool domain join <dns-realm> DC --server=<restored-dc>`
- 5) если используется переименованная резервная копия, также потребуется перенастроить сетевые устройства, так чтобы трафик перенаправлялся в восстановленный домен, а не в неисправный/исходный домен.

Примечание. Из файла резервной копии восстанавливается весь домен, а не конкретный контроллера домена. Шаг с командой `samba-tool domain backup restore` выполняется только один раз, при этом домен воссоздается на одном контроллере домена. Затем все старые контроллеры домена должны быть повторно присоединены к восстановленному контроллеру домена.

Этап восстановления из файла резервной копии аналогичен разворачиванию домена, который выполнялся при первой настройке «Альт Домен», за исключением того, что резервная копия содержит в себе все объекты базы данных, которые были добавлены с момента создания домена. Как и при создании нового домена, при запуске команды восстановления домена потребуется указать новый контроллер

домена. Этот контроллер домена не должен был существовать ранее в сети «Альт Домен».

Команда восстановления домена из резервной копии:

```
# samba-tool domain backup restore --backup-file=<tar-file> \  
--newservername=<DC-name> --targetdir=<new-samba-dir>
```

где:

- tar-file – файл резервной копии;
- DC-name – новый контроллер домена;
- new-samba-dir – каталог, куда будут восстановлены все файлы службы каталогов (smb.conf, sam.ldb и т. п.).

Следует обратить внимание, что указанный целевой каталог должен быть пустым (или не должен существовать). Не рекомендуется восстанавливать базу данных домена в место установки по умолчанию (например, в каталог /var/lib/samba). Вместо этого рекомендуется восстановить базу данных домена в другой целевой каталог, а затем, при запуске samba, использовать параметр -s (или --configfile), например:

```
# samba -s <targetdir>/etc/smb.conf
```

Указание восстановленного smb.conf гарантирует, что Samba будет использовать файлы базы данных.

Восстановленный контроллер домена будет добавлен в сайт «Default-First-Site-Name». Если он не существует в базе данных, он будет создан. Указать альтернативный сайт для добавления восстановленного контроллера домена можно с помощью параметр --site.

Перед запуском службы каталогов на восстановленном контроллере домена следует еще раз проверить правильность восстановленных настроек smb.conf.

Пример восстановления данных из резервной копии:

```
# mkdir /var/lib/samba/new  
# samba-tool domain backup restore \  
--backup-file=/home/user/samba-backup-test.alt-2024.tar.bz2 \  
--newservername=newdc --targetdir=/var/lib/samba/new
```

```
Adding new DC to site 'Default-First-Site-Name'  
Updating basic smb.conf settings...
```

...

Backup file successfully restored to /var/lib/samba/new
Please check the smb.conf settings are correct before starting samba.

10.6.5.1.2. Переименованная резервная копия

Процедура создания резервной копии и восстановления из нее в режиме переименования показана на рис. 499.

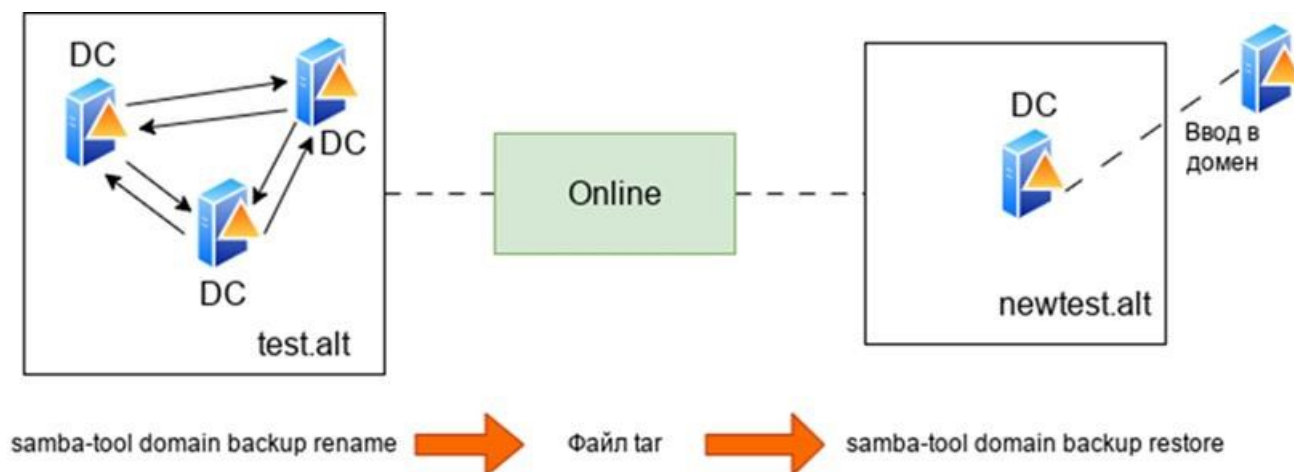


Рис. 499 – Схема создания резервной копии в режиме переименования

В режиме с переименованием (rename) формируется набор файлов с актуальными данными службы каталогов, не привязанными к состоянию конкретного контроллера домена, с переименованием домена.

Данный вид резервного копирования позволяет с минимальными усилиями временно подменить вышедший из строя домен таким образом, чтобы, с одной стороны, обеспечить работоспособность ключевых сетевых сервисов службы каталогов, а с другой – иметь возможность детально исследовать причины возникновения проблем в существующем домене.

Создание резервной копии в режиме переименования может применяться для:

- 1) запуска временного альтернативного домена на случай катастрофического отказа основного домена. На альтернативный/переименованный домен можно переключиться с минимальными усилиями. Затем можно запустить два домена одновременно, не мешая друг другу (переименованный/альтернативный домен будет предоставлять основные

сетевые службы Samba, в это же время на исходных контроллерах домена можно устранять неполадки);

- 2) создания реалистичного лабораторного домена: домен переименовывается и удаляются конфиденциальные данные (на данный момент только самые важные), чтобы создать предпроизводственную среду для тестирования.

При клонировании базы данных службы каталогов в нее вносятся изменения, обеспечивающие использование другого NetBIOS-имени и другой области DNS в новом домене. Изменяются следующие объекты:

- все DN-имена;
- объект раздела домена и его NetBIOS-имя;
- объекты зоны DNS, а также атрибуты dnsRoot.

П р и м е ч а н и е . Модифицируется только клонированный домен – исходный домен вообще не затрагивается.

Объекты, которые не меняются:

- userPrincipalName (UPN) по-прежнему будет использовать user@old-realm. Если при выполнении команды резервного копирования с переименованием домена использовался параметр `--keep-dns-realm`, пользователи могут использовать для входа в домен свои полные UPN-имена. В противном случае они могут использовать имена в формате user@new-realm (при условии, что конфигурация Kerberos корректно обрабатывает новую область);
- объекты групповой политики: атрибуты объекта групповой политики (gPCFileSysPath и gPLink) вообще не обновляются, файлы в sysvol сохраняются с прежним именем области в путях (например, sysvol/test.alt/Policies). Каталог для файлов политик в sysvol по умолчанию создается с новым именем области (например, sysvol/newtest.alt/Policies).

П р и м е ч а н и е . Обновление объектов групповой политики для обработки изменения имени домена – нетривиальный процесс. Лучший способ справиться с долгосрочным переименованием домена – вручную экспортировать файлы ГП, а затем повторно импортировать их. В краткосрочной перспективе переименованный

домен сможет продолжать использовать объекты групповой политики, относящиеся к старой области.

Переименование домена выполняется в два этапа:

1) создание переименованной резервной копии домена:

`samba-tool domain backup rename` делает клон работающей базы данных DC, в процессе клонирования переименовывает домен и создает файл резервной копии;

2) восстановление резервной копии домена:

`samba-tool domain backup restore` берет файл резервной копии и заполняет файлы, необходимые для запуска нового контроллера.


10.6.5.1.2.1. Создание переименованной резервной копии

Команда для создания переименованной резервной копии:

```
# samba-tool domain backup rename <new-domain-netbios> \  
<newdomain-dns-realm> --server=<dc-to-backup> \  
--targetdir=<output-dir> --no-secrets -UAdministrator
```

Где:

- `new-domain-netbios` – новое имя NETBIOS;
- `newdomain-dns-realm` – новая область DNS;
- `output-dir` – каталог, куда будет записан сгенерированный файл резервной копии.

 Параметр `--no-secrets` исключает из резервной копии конфиденциальную информацию о паролях (например, такие атрибуты, как `unicodePwd`, `lmPwdHistory` и т. д.) для всех пользователей в домене. При этом, файл резервной копии по-прежнему содержит конфиденциальную информацию, такую как имена учетных записей пользователей.

В результате выполнения команды формируется файл резервной копии `/var/samba-backup-rename/samba-backup-newtest.alt-<timestamp>.tar.bz2`.

В случае, если команда создания резервной копии запускается на узле, который будет использоваться в качестве нового контроллера домена (он должен быть подключен к рабочему домену), рекомендуется иметь файл `smb.conf`, максимально соответствующий производственному контроллеру домена, и передать

его команде резервного копирования (с помощью параметра `--configfile=smb.conf`).

Это гарантирует, что резервная копия будет содержать `smb.conf`, точно соответствующий домену.

Пример создания переименованной резервной копии на контроллере домена:

```
# mkdir /var/samba-backup-rename
# samba-tool domain backup rename NEWTEST newtest.alt \
--server=dc1 --targetdir=/var/samba-backup-rename \
--no-secrets -Uadministrator
```

```
New realm for backed up domain: newtest.alt
New base DN for backed up domain: DC=newtest,DC=alt
New domain NetBIOS name: NEWTEST
Password for [TEST\Administrator]:
Provisioning the new (renamed) domain...
...
```

Если команда создания резервной копии запускалась на рабочем контроллере домена, необходимо скопировать сгенерированный файл резервной копии на узел, который будет использоваться в качестве нового контроллера домена.

10.6.5.1.2.2. Восстановление данных из резервной копии

Файл резервной копии `/var/samba-backup-rename/samba-backup-newtest.alt-<timestamp>.tar.bz2` может использоваться для восстановления клонированной и переименованной базы данных на диске. В восстановленном домене будет только один новый контроллер домена с именем, указанными с помощью опции `--newservername`. В последующем к нему могут быть присоединены другие контроллеры домена. Для указания нового каталога для размещения всех файлов службы каталогов (`smb.conf`, `sam.ldb` и т. п.) может использоваться опция `--targetdir`.

Команда восстановления из переименованной резервной копии:

```
# samba-tool domain backup restore --backup-file=<tar-file> \
--targetdir=<output-dir> --newservername=<DC-name>
```

где:

- `tar-file` – файл резервной копии;

- `output-dir` – каталог, куда будут восстановлены все файлы службы каталогов (`smb.conf`, `sam.ldb` и т. п.);
- `DC-name` – новый контроллер домена.

Пример восстановления домена из переименованной резервной копии:

```
# mkdir /var/lib/samba/newtest
# samba-tool domain backup restore \
--targetdir=/var/lib/samba/newtest --newservername=NEWDC1 \
--backup-file=/home/user/samba-backup-newtest.alt.alt-2024.tar.bz2
```

Примечания:

1. Целевой каталог должен быть пустым (или не должен существовать). Не рекомендуется восстанавливать базу данных домена в место установки по умолчанию (например, в каталог `/var/lib/samba/`). Однако можно указать подкаталог (например, `/var/lib/samba/newtest/`).
2. Новый контроллер домена не может использовать то же имя сервера, что и контроллер домена в исходной сети.

10.6.5.1.2.3. Сброс пароля

Во время резервного копирования/восстановления пароль для учетной записи администратора сбрасывается на случайно сгенерированный пароль. Для его изменения можно просто обновить базу данных на локальном диске, выполнив команду:

```
# samba-tool user setpassword Administrator \
--newpassword=<пароль>-H /var/lib/samba/newtest/private/sam.ldb
```

Для тестирования аутентификации пользователей можно либо добавить дополнительные «тестовые» учетные записи пользователей/машин, либо «командовать» некоторыми учетными записями, скопированными из рабочего домена. Для учетных записей, скопированных из рабочего домена, не будут установлены пароли, поэтому на этом этапе также можно сбросить пароли для выбранных учетных записей. Или можно сделать это позже, когда служба каталогов действительно запустится на новом контроллере домена.

10.6.5.1.2.4. Запуск Samba

Перед запуском службы каталогов на новом контроллере домена, необходимо проверить корректность настроек в восстановленном файле `smb.conf` (например, `/var/lib/samba/newtest/etc/smb.conf`) и в файле `/etc/krb5.conf`, и при необходимости вручную внести в него изменения.

При запуске службы каталогов необходимо указать восстановленный `smb.conf` (это гарантирует, что Samba загрузит правильные файлы базы данных для нового домена). Например:

```
# samba -s /var/lib/samba/newtest/etc/smb.conf
```

При первом запуске `samba` могут быть зарегистрированы ошибки DNS. Это связано с тем, что `samba_dnupdate` запускается автоматически и добавляет записи DNS для нового домена.

После запуска `samba` можно проверить правильность работы нового контроллера домена, например, выполнив команду:

```
# ldbsearch -H ldap://NEWDC1 -Uadministrator
```

10.6.5.1.2.5. Обновление подсетей сайта

Новый домен будет содержать все сайты рабочего домена, но ни один из рабочих контроллеров домена. Однако подсети, которые используют эти сайты, скорее всего, больше не будут иметь смысла для экспериментального домена.

10.6.5.1.3. Рекомендуемая стратегия

Восстановление файла резервной копии имеет несколько неудобств:

- необходимость использовать другой каталог для установки по умолчанию;
- необходимо указать имя сервера DC, отличное от того, что было ранее в сети.

Свести эти неудобства к минимуму можно, используя временный сервер (или виртуальную машину) для восстановления контроллера домена. В этом случае процесс восстановления работоспособности домена состоит из следующих шагов:

- 1) выполнить восстановление из файла резервной копии на временный контроллер домена и запустить службу каталогов;
- 2) повторно, по одному, присоединить исходные контроллеры домена к временному контроллеру домена (во время присоединения можно повторно использовать одно и то же имя сервера и место установки по умолчанию);
- 3) после присоединения всех исходных контроллеров домена к восстановленному домену, можно удалить временный контроллер домена (например, с помощью команды `samba-tool domain demote`). В этом

случае новая сеть контроллеров домена будет полностью повторять существующую.

Пример разворачивания домена (SAMBA_INTERNAL) из резервной копии:

1) подготовить узел:

- установить пакет task-samba-dc:

```
# apt-get install task-samba-dc
```

- остановить конфликтующие службы:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl  
disable $service; systemctl stop $service; done
```

- очистить базы и конфигурацию Samba:

```
# rm -f /etc/samba/smb.conf  
# rm -rf /var/lib/samba/*  
# rm -rf /var/cache/samba
```

2) скопировать файл резервной копии на ВМ и выполнить восстановление домена из файла резервной копии:

```
# samba-tool domain backup restore \  
--backup-file=/home/user/samba-backup-test.alt-2024.tar.bz2 \  
--newservername=newdc --targetdir=/var/lib/samba
```

```
Adding new DC to site 'Default-First-Site-Name'
```

```
Updating basic smb.conf settings...
```

```
...
```

```
Backup file successfully restored to /var/lib/samba
```

```
Please check the smb.conf settings are correct before starting  
samba.
```

3) скопировать файл smb.conf из каталога /var/lib/samba/etc/ в каталог /etc/samba/:

```
# cp /var/lib/samba/etc/smb.conf /etc/samba/
```

4) запустить службу каталогов:

```
# systemctl enable --now samba
```

5) заменить файл /etc/krb5.conf файлом из каталога /var/lib/samba/private/:

```
# cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

6) проверить работоспособность домена (см. п. 10.2.2.7):

```
# samba-tool domain info 127.0.0.1
```

```

Forest           : test.alt
Domain           : test.alt
Netbios domain   : TEST
DC name          : newdc.test.alt
DC netbios name  : NEWDC
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name

# smbclient -L localhost -Uadministrator
Password for [TEST\administrator]:
  Sharename      Type           Comment
  -----      -
  sysvol         Disk
  netlogon       Disk
  share          Disk           Commonplace
  Free           Disk
  IPC$           IPC            IPC Service (Samba 4.19.7)
SMB1 disabled -- no workgroup available
# host -t SRV _kerberos._udp.test.alt.
_kerberos._udp.test.alt has SRV record 0 100 88 newdc.test.alt.

```

10.6.5.1.4. Отладочная информация

Если команда резервного копирования или восстановления завершится с ошибкой, то они могут оставить после себя временный каталог (указанный в параметре `--targetdir`). Необходимо удалить этот каталог перед повторным запуском команды восстановления.

Создание резервной копии:

- 1) резервное копирование следует запускать от имени пользователя `root`. Резервное копирование в онлайн-режиме может быть успешным и для пользователя без полномочий `root`, но при попытке восстановить данные из такой резервной копии могут возникнуть проблемы;
- 2) для резервных копий, выполненных в онлайн-режиме или в режиме переименования, следует проверить правильность используемых учетных данных и сведений о сервере. Например:


```
# ldbsearch -H ldap://<server> -UAdministrator
```
- 3) чтобы узнать больше информации о причине сбоя можно увеличить уровень журналирования. Например, добавить в команду параметр `--debug=3`;
- 4) работа команд для выполнения резервного копирования в онлайн-режиме или в режиме переименования очень похожа на присоединение к контроллеру домена. Если известно, что присоединение к контроллеру

домена в вашей сети не удастся, то эти команды также вероятно не будут работать. Сообщения «Committing SAM database» и «Cloned domain <domain>», говорят о том, что часть резервного копирования, подобная присоединению, скорее всего, выполнена успешно;

- 5) инструменты резервного копирования не работают напрямую с контроллером домена Windows (в основном простое резервное копирование файлов sysvol не удастся из-за блокировки службы DFSR). Если используется смешанный домен контроллера домена, следует создать резервную копию контроллера домена Samba, а не контроллера домена Windows. Если у вас домен Windows, можно на время резервного копирования на контроллере домена остановить службу DFSR «Репликация DFS».

Восстановление из резервной копии:

- 1) команду восстановления необходимо запускать от имени пользователя root;
- 2) имя, указанное в параметре --newservername, не должно существовать в исходном домене. В противном случае будет получена ошибка вида:

```
Adding CN=NEWDC,OU=Domain Controllers,DC=test,DC=alt
ERROR(ldb): uncaught exception - Entry CN=NEWDC, OU=Domain Controllers,
DC=test, DC=alt already exists
  File "/usr/lib64/samba-dc/python3.9/samba/netcmd/__init__.py", line 186, in
_run
    return self.run(*args, **kwargs)
  File "/usr/lib64/samba-dc/python3.9/samba/netcmd/domain_backup.py", line
562, in run
    ctx.join_add_objects(specified_sid=dom_sid(str(sid)))
  File "/usr/lib64/samba-dc/python3.9/samba/jjoin.py", line 674, in
join_add_objects
    ctx.sambd.add(rec, controls=controls)
```

- 3) если команда резервного копирования выполнялась локально на контроллере домена, то файл резервной копии должен содержать файл smb.conf контроллера домена. Однако smb.conf в файле резервной копии может содержать конфигурацию «интерфейсов», которая не соответствует IP-адресам на контроллере домена, на котором разворачиваются данные из резервной копии. Избежать этой проблемы можно, указав аргумент

--host-ip во время восстановления (это имеет значение только для переименованных резервных копий).

10.6.5.2. Восстановление произвольного контроллера домена после фатального сбоя

Служба каталогов использует единую распределенную базу данных, которая хранит сведения обо всех сетевых ресурсах домена. Каждый контроллер домена работает с локальной копией этой базы данных. Синхронизацию изменений между такими локальными копиями обеспечивает механизм репликации. При выполнении на существующем контроллере домена команды `samba-tool domain join DC` локальная копия базы данных полностью перезаписывается актуальной копией распределенной базы данных (происходит процесс «повторного ввода» контроллера в домен).

Возможны ситуации, когда в работе отдельного контроллера домена возникают неполадки или он полностью выходит из строя, при этом остальная часть домена продолжает функционировать корректно. Например, это может быть вызвано ошибками в нереплицируемой части локальной копии базы данных на контроллере или некорректной репликацией изменений с других контроллеров. То есть ошибки не распространяются по домену через механизм репликации и носят локальный характер.

Алгоритм восстановления контроллера домена под тем же именем, если в результате каких-либо технических проблем он пришел в неработоспособное состояние:

- 1) вывести контроллер домена из эксплуатации, путем удаления всей информации о нем. Для этого на любом работающем контроллере домена выполнить команду:

```
# samba-tool domain demote --remove-other-dead-server=dc2 -UAdministrator
```

где `dc2` – имя (hostname) не функционирующего контроллера домена;

- 2) на узле, который будет заменой вышедшего из строя контроллера домена, выполнить следующие действия:

- в файле /etc/krb5.conf указать опции default_realm = TEST.ALT и dns_lookup_realm = false;
- остановить все зависимые службы:


```
# for service in samba smb nmb krb5kdc slapd bind; do
systemctl disable $service; systemctl stop $service; done
```
- очистить всю конфигурацию Samba:


```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```
- ввести узел в домен как дополнительный контроллер домена:


```
# samba-tool domain join test.alt DC \
-Uadministrator@TEST.ALT --realm=test.alt
```
- запустить samba и обновить dns:


```
# systemctl enable --now samba
# samba_dnsupdate --use-samba-tool -verbose
```

Примечание. На других контроллерах домена в выводе команды `samba-tool drs showrepl` в секции неисправного КД некоторое время будет присутствовать сообщение `WERR_GEN_FAILURE`:

```
...
DC=DomainDnsZones,DC=test,DC=alt
Default-First-Site-Name\DC2 via RPC
DSA object GUID: b78f2c9d-5c62-4497-a5e1-4fc85aedf1cb
Last attempt @ Wed Apr 24 07:51:24 2024 MSK failed, result 31
(WERR_GEN_FAILURE)
28 consecutive failure(s).
Last success @ NTTIME(0)

DC=ForestDnsZones,DC=test,DC=alt
Default-First-Site-Name\DC2 via RPC
DSA object GUID: b78f2c9d-5c62-4497-a5e1-4fc85aedf1cb
Last attempt @ Wed Apr 24 07:51:24 2024 MSK failed, result 31
(WERR_GEN_FAILURE)
28 consecutive failure(s).
Last success @ NTTIME(0)

...
```

Это нормально, и через некоторое время после полной репликации оно исчезнет. Репликация может занять до нескольких часов.

10.6.6. Роли FSMO

FSMO, или Flexible single-master operations (операции с одним исполнителем) – это операции, выполняемые контроллерами домена, которые требуют обязательной уникальности сервера для каждой операции. В зависимости от типа операции уникальность FSMO подразумевается в пределах одного домена или леса доменов. Различные типы FSMO могут выполняться как на одном, так и на нескольких контроллерах домена. Выполнение FSMO сервером называют ролью сервера, а сами сервера – хозяевами операций.

«Альт Домен» – это центральный репозиторий, в котором хранятся все объекты и соответствующие им атрибуты. Это иерархическая база данных с поддержкой нескольких источников. Большинство операций в «Альт Домен» можно выполнять на любом контроллере домена. Служба репликации «Альт Домен» скопирует изменения на остальные контроллеры домена, обеспечив идентичность базы «Альт Домен» на всех контроллерах одного домена. Один из способов разрешения конфликтов заключается в том, что сохраняются изменения, внесенные последними. Изменения, внесенные остальными контроллерами домена, игнорируются.

Однако существует несколько операций (например, изменение схемы «Альт Домен»), при которых конфликты недопустимы. В «Альт Домен» некоторые обновления выполняются на одном специальном контроллере домена, а затем реплицируются на все остальные. «Альт Домен» использует роли, назначенные контроллерам домена, для этих специальных задач. Так как роль не привязана к одному контроллеру домена, она называется ролью FSMO. В настоящее время существует семь ролей FSMO с разными областями действия:

- эмулятор PDC/PDC Emulator (один на домен);
- хозяин RID/RID Master (один на домен);
- хозяин схемы/Schema Master (один на лес);
- хозяин именования доменов/Domain Naming Master (один на лес);
- хозяин инфраструктуры/Infrastructure Master (один на домен);
- хозяин зоны DNS домена/Domain DNS Zone Master role (один на домен);
- хозяин зоны DNS леса/Forest DNS Zone Master role (один на лес).

10.6.6.1. Семь ролей FSMO

Ниже описаны роли FSMO, их функции и требования к доступности. Эти сведения позволяют определить последствия, когда контроллер домена, владеющий этой ролью, находится в автономном режиме.

10.6.6.1.1. Эмулятор PDC

Владелец роли эмулятора PDC отвечает за следующие задачи в домене:

- 1) является сервером точного времени для клиентов в домене. Для аутентификации Kerberos необходима точная синхронизация времени. Эмулятор PDC корневого домена в лесу является по умолчанию сервером точного времени для эмуляторов PDC в дочерних доменах;
- 2) изменения паролей, внесенные другими контроллерами домена в домене, реплицируются преимущественно в эмулятор PDC. В случае недоступности эмулятора PDC информация об изменении пароля все равно распространится по домену, просто произойдет это несколько медленнее;
- 3) выполняет все функции, предоставляемые PDC в стиле NT4;
- 4) обрабатывает блокировки учетных записей. Сбои аутентификации на любом контроллере домена в домене, вызванные неправильным паролем, перенаправляются в эмулятор PDC до того, как сообщение о сбое из-за неправильного пароля будет передано пользователю. При успешной аутентификации учетной записи сразу после неудачной попытки, о ней уведомляется эмулятор PDC и сбрасывает счетчик неудачных попыток в ноль;
- 5) консоль управления групповыми политиками по умолчанию соединяется с эмулятором PDC, и изменения политик происходят на нем же. Если эмулятор PDC недоступен, то будет нужно указать редактору, к какому контроллеру домена подключиться;
- 6) в больших средах контроллер домена, которому принадлежит роль эмулятора PDC, может иметь высокую загрузку ЦП из-за сквозной аутентификации, смены пароля и синхронизации времени.

На каждый домен приходится один эмулятор PDC.

Этот контроллер домена должен, по возможности, быть доступен всегда, потому что для Kerberos требуется точное время на всех машинах в домене. Если клиенты настроены на использование другого источника времени и в сети нет клиентов до Windows 2000, временное отсутствие может быть менее критичным.

Для поиска эмулятора PDC можно использовать команду host:

```
# host -t SRV _ldap._tcp.pdc._msdcs.<домен>
```

Например:

```
# host -t SRV _ldap._tcp.pdc._msdcs.test.alt
_ldap._tcp.pdc._msdcs.test.alt has SRV record 0 100 389
dc1.test.alt.
```

10.6.6.1.2. Хозяин RID

Владелец роли FSMO хозяина RID отвечает за обработку запросов пула RID от всех DC в домене. Он также отвечает за перемещение объектов в другой домен и удаление их из домена.

Все объекты безопасности, например, учетные записи и группы пользователей/компьютеров имеют уникальный идентификатор безопасности (SID). SID объектов содержит идентификатор безопасности (SID) домена, одинаковый для всех объектов в домене, и относительный идентификатор (RID), уникальный для каждого идентификатора безопасности субъекта безопасности, созданного в домене.

Каждому контроллеру домена в домене выделяется пул относительных идентификаторов RID, которые разрешено назначать созданным субъектам безопасности. По умолчанию это диапазон из 500 уникальных RID для всего домена, назначаемых хозяином RID каждому контроллеру домена. Если объект безопасности создается на контроллере домена, то RID берется из этого пула, что гарантирует его уникальность в домене. Если выделенный пул RID контроллера домена оказывается ниже порогового значения (ниже 50 %), контроллер домена выполняет запрос дополнительных идентификаторов RID к хозяину RID в домене. Хозяин RID в домене отвечает на запрос, извлекая идентификаторы RID из невыделенного пула RID домена и назначая их пулу запрашивающего контроллера домена.

На каждый домен приходится один хозяин RID.

Этот контроллер домена должен быть активен, при создании нового контроллера домена в домене, чтобы назначить ему пул RID. Также хозяин RID должен быть доступен, когда существующие контроллеры домена обновляют свой резервный пул RID.

С другой стороны, если хозяин RID находится в автономном режиме, то на каждом контроллере домена можно создавать новые объекты безопасности, пока локальный пул RID не станет пустым. Если пулы RID на всех контроллерах домена опустеют, создание дополнительных объектов станет невозможно. Также пока хозяин RID домена находится в автономном режиме невозможно присоединиться к дополнительным контроллерам домена.

10.6.6.1.3. Хозяин схемы

Контроллер домена, обладающий ролью хозяина схемы, является единственным в лесу «Альт Домен», кому разрешено обновлять схему каталога. После завершения обновления изменения реплицируются на все другие контроллеры домена в лесу.

Схема каталога (контекст именования схемы) или LDAP://cn=schema,cn=configuration,dc=<домен> существует на всех контроллерах домена. Обновления выполняются только на хозяине схемы. После завершения обновления схема реплицируется из хозяина схемы во все остальные контроллеры домена каталога.

В каждом лесу есть один хозяин схемы.

Контроллер домена, обладающий ролью хозяина схемы, должен быть подключен к сети при выполнении обновлений схемы.

10.6.6.1.4. Хозяин именования доменов

Хозяин именования доменов отвечает за внесение изменений в пространство доменных имен в масштабах леса. Только этот контроллер домена может добавлять или удалять домены, доверительные отношения с внешними каталогами и разделами приложений в (из) леса.

Информация об именах доменов хранится в разделе «Контекст именования конфигурации» в CN=Partitions, CN=Configuration, DC=<домен>.

Этот раздел существует на всех контроллерах домена, но обновляется только на хозяине именованного домена.

На каждый лес приходится один хозяин именованного домена.

Контроллер домена, обладающий ролью хозяина именованного домена, должен быть подключен к сети, когда устанавливаются доверительные отношения с внешними каталогами и доменами, а разделы приложений добавляются или удаляются из леса.

10.6.6.1.5. Хозяин инфраструктуры

Контроллер домена, которому принадлежит роль хозяина инфраструктуры, отвечающий за обновление идентификатора безопасности (SID) и различающегося имени объекта в ссылке на междоменный объект. Это используется, например, если пользователь из одного домена добавляется в группу безопасности другого домена.

На каждый домен приходится один хозяин инфраструктуры.

Если контроллер домена, обладающий ролью хозяина инфраструктуры, временно отключен, междоменные изменения невозможны.

10.6.6.1.6. Хозяин зоны DNS домена

Контроллер домена, которому принадлежит роль хозяина зоны DNS домена, отвечает за координацию добавления или удаления любых зон DNS, интегрированных в «Альт Домен», на контроллерах домена с DNS-серверами, на которых размещен домен.

На каждый домен приходится один хозяин зоны DNS-домена.

10.6.6.1.7. Хозяин зоны DNS леса

Контроллер домена, которому принадлежит роль хозяина зоны DNS леса, отвечает за координацию добавления или удаления записей всего леса на DNS-серверах, на которых размещена зона DNS верхнего уровня. Эти записи содержат имена серверов глобального каталога (GC).

На каждый домен приходится один хозяин зоны DNS леса.

10.6.6.2. Просмотр и передача ролей FSMO

По возможности следует передавать роли FSMO штатным образом и не использовать принудительную передачу (захват роли). Для штатной передачи роли требуется, чтобы контроллер домена, которому в данный момент принадлежит роль, работал и был подключен к сети. В этом случае при передаче роли старый контроллер домена узнает, что он больше не владеет ролью.

Если контроллер домена сломан (например, из-за аппаратного дефекта) и больше никогда не будет возвращен в сеть, можно использовать принудительную передачу (захватить роль на оставшемся контроллере домена). Если старый контроллер домена будет снова подключен к сети, это вызовет конфликты и приведет к неконсистентному домену (т. к. старый контроллер домена не заметит изменения и по-прежнему будет считать себя владельцем роли).

Роли FSMO можно передавать с помощью инструмента командной строки `samba-tool` или в модуле удаленного управления базой данных конфигурации (ADMC).

10.6.6.2.1. ADCMC

См. п. 10.4.5.14.

10.6.6.2.2. Инструмент `samba-tool`

10.6.6.2.2.1. Просмотр текущих владельцев

Операция просмотра списка владельцев ролей FSMO доступна всем пользователям.

Просмотр текущего состояния (команда выполняется на контроллере домена):

```
# samba-tool fsmo show
```

```
SchemaMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
InfrastructureMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
RidAllocationMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
PdcEmulationMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
DomainNamingMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
DomainDnsZonesMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
ForestDnsZonesMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
```

10.6.6.2.2. Передача роли

Операция передачи роли FSMO доступна пользователям со следующими полномочиями:

- передача ролей уровня леса – администраторы леса (члены группы Enterprise Admins);
- передача ролей уровня домена – администраторы домена (члены группы Domain Admins);
- передача роли владельца схемы каталога – администраторы схемы (члены группы Schema Admins).

Для штатной передачи роли необходимо на контроллере домена, который должен стать новым владельцем роли выполнить команду:

```
# samba-tool fsmo transfer --role=<роль>
```

Список возможных ролей:

- rid – хозяин RID;
- pdc – эмулятор PDC;
- infrastructure – хозяин инфраструктуры;
- schema – хозяин схемы;
- naming – хозяин именования доменов;
- domaindns – хозяин зоны DNS домена;
- forestdns – хозяин зоны DNS домена;
- all – все роли.

Пример штатной передачи роли (команда выполняется на DC2):

```
# samba-tool fsmo transfer --role=infrastructure
FSMO transfer of 'infrastructure' role successful
```

Проверка:

```
# samba-tool fsmo show
```

```
SchemaMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers, CN=Default-
First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
InfrastructureMasterRole owner: CN=NTDS Settings, CN=DC2, CN=Servers,
CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
RidAllocationMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers,
CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
PdcEmulationMasterRole owner: CN=NTDS Settings, CN=DC1, CN=Servers,
CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
```

```

DomainNamingMasterRole  owner:  CN=NTDS  Settings,  CN=DC1,  CN=Servers,
CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
DomainDnsZonesMasterRole  owner:  CN=NTDS  Settings,  CN=DC1,  CN=Servers,
CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt
ForestDnsZonesMasterRole  owner:  CN=NTDS  Settings,  CN=DC1,  CN=Servers,
CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=test, DC=alt

```

10.6.6.2.2.3. Захват роли FSMO

Операция захвата роли FSMO доступна пользователям со следующими полномочиями:

- захват ролей уровня леса – администраторы леса (члены группы Enterprise Admins);
- захват ролей уровня домена – администраторы домена (члены группы Domain Admins);
- захват роли владельца схемы каталога – администраторы схемы (члены группы Schema Admins).

Для принудительной передачи роли (например, если контроллер домена вышел из строя) необходимо на контроллере домена, который должен стать новым владельцем роли выполнить команду:

```
# samba-tool fsmo seize --role=<роль>
```

Список возможных ролей:

- rid – хозяин RID;
- pdc – эмулятор PDC;
- infrastructure – хозяин инфраструктуры;
- schema – хозяин схемы;
- naming – хозяин именования доменов;
- domaindns – хозяин зоны DNS домена;
- forestdns – хозяин зоны DNS домена;
- all – все роли.

Примечания:

1. Если роль была передана принудительно, старый контроллер домена больше никогда не должен подключаться к сети.

2. При передаче ролей domaindns и forestdns необходимо предоставить аутентификацию.

3. В ранних версиях `samba-tool` была ошибка, не позволявшая захватить роль `naming`:

```
# samba-tool fsmo seize --role=naming
ERROR (ldb): uncaught exception - Failed FSMO transfer:
WERR_BADFILE
```

В этом случае необходимо использовать «еще более принудительную передачу»:

```
# samba-tool fsmo seize --force --role=naming
```

10.6.7. Репликация

Репликация «Альт Домен» – метод, посредством которого изменения в базе службы каталогов на одном контроллере домена передаются другим контроллерам.

В Samba все, что хранится внутри домена, реплицируется между контроллерами домена (пользователи, группы и записи DNS).

В настоящее время Samba не поддерживает протокол репликации распределенной файловой системы (DFS-R), используемый для репликации Sysvol.

Методы решения этой проблемы см. В п. 10.6.7.3.

10.6.7.1. Настройка репликации

⚠ Без успешной двунаправленной репликации в течение 14 дней DC исключается из домена.

⚠ Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

Начиная с версии `samba 3.5` топология репликации выстраивается автоматически.

Команда репликации:

```
# samba-tool drs replicate <destinationDC> <sourceDC> <NC> [options]
```

Процедура двусторонней репликации:

1) репликация с первого контроллера домена на второй:

```
# samba-tool drs replicate dc2.test.alt \
dc1.test.alt dc=test,dc=alt -Uadministrator
Password for [TEST\administrator]:
Replicate from dc1.test.alt to dc2.test.alt was successful.
```

Сначала указывается приемник, затем источник, после этого реплицируемая ветка в LDAP;

2) репликация на первый контроллер домена со второго:

```
# samba-tool drs replicate dc1.test.alt \
dc2.test.alt dc=test,dc=alt -Uadministrator
Password for [TEST\administrator]:
Replicate from dc2.test.alt to dc1.test.alt was successful.
```

Сначала указывается приемник, затем источник, после этого реплицируемая ветка в LDAP;

Примечание. Имя домена в именах серверов можно опустить (если они одинаковые).

3) для просмотра статуса репликации можно запустить команду на DC (подробнее см. п. 10.6.7.2):

```
# samba-tool drs showrepl
```

Примечание. Если репликация на Windows не работает, следует добавить в Active Directory Sites and Services новое соединение Active Directory, реплицировать на DC, подождать минут 5 и попробовать реплицировать с Samba на Windows.

10.6.7.2. Проверка статуса репликации

10.6.7.2.1. Отображение статуса репликации на контроллере домена Samba

Команда `samba-tool drs showrepl` отображает установленные связи с другими контроллерами домена в лесу «Альт Домен». Соединения отображаются с точки зрения контроллера домена, на котором запускается команда.

Пример:

```
# samba-tool drs showrepl
Default-First-Site-Name\DC2
DSA Options: 0x00000001
DSA object GUID: 26a8d3d0-66b3-4f6c-8457-0def172d4af3
DSA invocationId: 83fb4bbf-9f63-44d6-acbd-c0db4e9e839a

==== INBOUND NEIGHBORS ====

CN=Schema,CN=Configuration,DC=test,DC=alt
Default-First-Site-Name\DC1 via RPC
DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
Last attempt @ Wed May 22 15:38:51 2024 EET was successful
0 consecutive failure(s).
Last success @ Wed May 22 15:38:51 2024 EET
```

JKHB.11100-01 90 03

CN=Configuration,DC=test,DC=alt
Default-First-Site-Name\DC1 via RPC
DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
Last attempt @ Wed May 22 15:38:51 2024 EET was successful
0 consecutive failure(s).
Last success @ Wed May 22 15:38:51 2024 EET

DC=ForestDnsZones,DC=test,DC=alt
Default-First-Site-Name\DC1 via RPC
DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
Last attempt @ Wed May 22 15:38:50 2024 EET was successful
0 consecutive failure(s).
Last success @ Wed May 22 15:38:50 2024 EET

DC=DomainDnsZones,DC=test,DC=alt
Default-First-Site-Name\DC1 via RPC
DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
Last attempt @ Wed May 22 15:38:51 2024 EET was successful
0 consecutive failure(s).
Last success @ Wed May 22 15:38:51 2024 EET

DC=test,DC=alt
Default-First-Site-Name\DC1 via RPC
DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
Last attempt @ Wed May 22 15:38:51 2024 EET was successful
0 consecutive failure(s).
Last success @ Wed May 22 15:38:51 2024 EET

==== OUTBOUND NEIGHBORS ====

CN=Schema,CN=Configuration,DC=test,DC=alt
Default-First-Site-Name\DC1 via RPC
DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
Last attempt @ NTTIME(0) was successful
0 consecutive failure(s).
Last success @ NTTIME(0)

CN=Configuration,DC=test,DC=alt
Default-First-Site-Name\DC1 via RPC
DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
Last attempt @ NTTIME(0) was successful
0 consecutive failure(s).
Last success @ NTTIME(0)

DC=ForestDnsZones,DC=test,DC=alt
Default-First-Site-Name\DC1 via RPC

ЛКНВ.11100-01 90 03

```
DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
Last attempt @ NTTIME(0) was successful
0 consecutive failure(s).
Last success @ NTTIME(0)
```

```
DC=DomainDnsZones,DC=test,DC=alt
Default-First-Site-Name\DC1 via RPC
DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
Last attempt @ NTTIME(0) was successful
0 consecutive failure(s).
Last success @ NTTIME(0)
```

```
DC=test,DC=alt
Default-First-Site-Name\DC1 via RPC
DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
Last attempt @ NTTIME(0) was successful
0 consecutive failure(s).
Last success @ NTTIME(0)
```

==== KCC CONNECTION OBJECTS ====

```
Connection --
Connection name: 56a02972-69f5-42fb-965a-7125f09c96d1
Enabled : TRUE
Server DNS name : dc1.test.alt
Server DN name : CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
TransportType: RPC
options: 0x00000001
Warning: No NC replicated for Connection!
```

Связи отображаются в разделах INBOUND NEIGHBORS и OUTBOUND NEIGHBORS.

В каждом разделе должно быть по 5 пунктов:

```
CN=Schema,CN=Configuration,DC=test,DC=alt
DC=ForestDnsZones,DC=test,DC=alt
DC=test,DC=alt
DC=DomainDnsZones,DC=test,DC=alt
CN=Configuration,DC=test,DC=alt
```

В разделе INBOUND NEIGHBORS в пункте Last attempt ДОЛЖНЫ СТОЯТЬ актуальные дата и время, идентичные указанным в строке Last success (отображает время последней репликации).

Должно быть 0 consecutive failure(s).

Если в разделе INBOUND NEIGHBORS есть записи:

```
Last attempt @ NTTIME(0) was successful
...
Last success @ NTTIME(0)
```

необходимо подождать (соединение устанавливается).

В разделе KCC CONNECTION OBJECTS должен быть приведен список всех контроллеров домена, чьи КСС установили соглашения о репликации с текущим контроллером домена. В случае, когда контроллер домена только был добавлен в домен и запущен, может пройти до 15 минут до того, как соглашения будут установлены.

Примечание. Предупреждение:

```
No NC replicated for Connection!
```

можно игнорировать. Оно появляется из-за того, что при регистрации нового DC Samba неверно устанавливает некоторые флаги репликации.

Можно также проверить репликацию LDAP:

```
# samba-tool ldapcmp ldap://dc1.test.alt \
ldap://dc2.test.alt -Uadministrator
```

```
Password for [TEST\administrator]:
```

```
* Comparing [DOMAIN] context...
```

```
* Objects to be compared: 274
```

```
* Result for [DOMAIN]: SUCCESS
```

```
* Comparing [CONFIGURATION] context...
```

```
* Objects to be compared: 1625
```

```
* Result for [CONFIGURATION]: SUCCESS
```

```
* Comparing [SCHEMA] context...
```

```
* Objects to be compared: 1739
```

```
* Result for [SCHEMA]: SUCCESS
```

```
* Comparing [DNSDOMAIN] context...
```

```
* Objects to be compared: 41
```

```
* Result for [DNSDOMAIN]: SUCCESS
```

```
* Comparing [DNSFOREST] context...
```

* Objects to be compared: 18

* Result for [DNSFOREST]: SUCCESS

Данная команда сравнит значения атрибутов объектов всего каталога на DC1 и DC2. В ряде случаев атрибуты объектов на разных контроллерах могут отличаться, и в выводе команды, это будет видно. Но не во всех случаях это будет признаком проблемы с репликацией.

10.6.7.2.2. Отображение статусов репликации на контроллере домена Windows

Для отображения статуса входящей репликации на контроллере домена Windows можно использовать утилиту `repadmin`:

```
> repadmin /showrepl
```

Windows не поддерживает отображение статусов исходящих подключений репликации. Чтобы обойти эту проблему, можно отобразить статусы входящих подключений на контроллерах домена Samba, на которые реплицируется контроллер домена Windows:

- 1) найти в «Альт Домен» всех партнеров репликации Windows DC. Например, чтобы отобразить партнеров по репликации контроллера домена с именем WindowsDC:

```
#      ldbsearch      -H      /var/lib/samba/private/sam.ldb
' (fromServer=*CN=WindowsDC*) ' --cross-ncs dn
# record 1
dn:          CN=a46c895e-658b-463e-9ab5-a1c237fca4b1,CN=NTDS
Settings,CN=DC2,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt

# returned 1 records
# 1 entries
# 0 referrals
```

В этом примере возвращается один партнер по репликации (имя хоста: DC2). Имя хоста партнера по репликации является частью возвращаемого отличительного имени (DN);

- 2) на каждом контроллере домена Samba, полученном на предыдущем шаге, выполнить команду `samba-tool drs showrepl` для отображения статуса репликации каталога. Необходимо убедиться, что каждый реплицируемый контейнер каталогов указан для контроллера домена Windows в разделе `INBOUND NEIGHBORS` на контроллере домена Samba, а статусы успешны.

10.6.7.3. Двухнаправленная репликация SysVol

Каталог Sysvol присутствует на всех контроллерах домена и используется для хранения logon скриптов и объектов групповых политик. Отсутствие репликации этого каталога приведет к неправильной работе групповых политик и сценариев входа.

Samba в своем текущем состоянии не поддерживает репликацию SysVol через DFS-R (репликация распределенной файловой системы) или более старую FRS (службу репликации файлов), используемую в Windows Server 2000/2003 для репликации SysVol. В настоящее время для репликации SysVol можно использовать один из следующих обходных путей:

- двухнаправленная репликация SysVol на основе Rsync/Unison (только Samba DC);
- двухнаправленная репликация SysVol на основе Rsync/osync (только Samba DC).

ВАЖНО

Следует синхронизировать `idmap.ldb` из контроллера домена, имеющего роль FSMO PDC_Emulator, со всеми другими контроллерами домена. Это гарантирует, что все контроллеры домена будут использовать одни и те же идентификаторы. Если файл `idmap.ldb` не синхронизируется, на каждом контроллере домена будут разные идентификаторы.

Синхронизировать `idmap.ldb` необходимо при первом присоединении к новому контроллеру домена, а затем периодически (для того чтобы гарантировать постоянство идентификаторов не нужно синхронизировать `idmap.ldb` каждый раз при синхронизации SysVol, но это следует делать периодически).

10.6.7.3.1. Настройка двухнаправленной репликации SysVol на базе Rsync/Unison

Исходные данные:

- все команды выполняются от пользователя root;
- первый контроллер домена – DC1;
- второй контроллер домена – DC2 (уже присоединен к домену);
- sysvol расположен в `/var/lib/samba` как на DC1, так и на DC2;
- rsync расположен в `/usr/bin/rsync`;

- unison расположен в /usr/bin/unison;
- журнал sysvolsync пишется в файл /var/log/sysvol-sync.log.

Примечание. Предварительно должно быть настроено беспарольное межсерверное взаимодействие (подробнее, см. п. 10.6.17).

На первом контроллере домена (DC1):

- 1) установить пакеты rsync и unison:

```
# apt-get install rsync unison
```

- 2) при низких скоростях в сети, unison может некорректно работать, поэтому при повторной его работе будет использоваться ранее созданное подключение по ssh, для этого:

```
# mkdir ~/.ssh/ctl
# cat < < EOF > ~/.ssh/ctl/config
Host *
ControlMaster auto
ControlPath ~/.ssh/ctl/%h_%p_%r
ControlPersist 1
EOF
```

Эти строки настраивают OpenSSH на использование ControlMaster для всех SSH-соединений и сохранение сокетов управления в каталоге ~/.ssh/ctl;

- 3) создать каталог /root/.unison/:

```
# mkdir /root/.unison
```

- 4) для определения политики синхронизации создать файл конфигурации unison /root/.unison/default.prf с следующим содержимым:

```
# Список каталогов, которые будут синхронизированы
root = /var/lib/samba
root = ssh://root@DC2.test.alt//var/lib/samba
# Список подкаталогов, которые нужно синхронизировать
path = sysvol

auto=true
batch=true
perms=0
rsync=true
maxthreads=1
retry=3
confirmbigdeletes=false
servercmd=/usr/bin/unison
copythreshold=0
copyprog = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --inplace --compress
```



```
copyprogrestart = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --
partial --inplace --compress
copyquoterem = true
copymax = 1

# Сохранять журнал с результатами работы в отдельном файле
logfile = /var/log/sysvol-sync.log
```

5) создать файл для записи журнала репликации (необходимо настроить ротацию логов для этого файла, так как размер журнала не контролируется):

```
# touch /var/log/sysvol-sync.log
```

На втором контроллере домена (DC2) установить пакеты rsync и unison:

```
# apt-get install rsync unison
```

Примечание. Перед запуском команды синхронизации рекомендуется сделать резервную копию каталога sysvol.

Запустить команду синхронизации:

```
# /usr/bin/rsync -XAavz --log-file /var/log/sysvol-sync.log \
--delete-after -f"+ */" -f"- *" /var/lib/samba/sysvol\
root@dc2.test.alt:/var/lib/samba && /usr/bin/unison
```

В этой команде утилита rsync создает структуры каталогов с расширенными атрибутами, а затем утилита unison копирует только эти расширенные атрибуты файлов.

На DC1 включить синхронизацию по расписанию:

```
# crontab -e
*/5 * * * * /usr/bin/unison -silent
```

Повторная синхронизация каталога:

- отключить синхронизацию по расписанию на DC1;
- rsync и unison не должны выполняться в данный момент (можно проверить командой ps -aux);
- удалить хеш-файлы на DC1 и DC2 в /root/.unison;
- проверить sysvol и повторить синхронизацию;
- убедиться, что синхронизация выполнена успешно;
- включить синхронизацию по расписанию на DC1.

Если контроллеров домена больше чем два, можно создать больше заданий для cron на DC1:

1) скопировать файл `/root/.inison/default.prf` в другой файл, например:

```
/root/.inison/sync_dc2.prf;
```

2) в файле `/root/.inison/dc2.prf` изменить значение параметра `root`;

3) повторить шаги 1 и 2 для всех контроллеров домена;

4) изменить задание на синхронизацию по расписанию на DC1:

```
* * * * * /usr/bin/unison sync_dc2 -silent
* * * * * /usr/bin/unison sync_dc3 -silent
...
```

10.6.7.3.2. Настройка двунаправленной репликации SysVol на базе Rsync/osync

Исходные данные:

- все команды выполняются от пользователя `root`;
- первый контроллер домена – DC1;
- второй контроллер домена – DC2 (уже присоединен к домену);
- `sysvol` расположен в `/var/lib/samba` как на DC1, так и на DC2;
- `rsync` расположен в `/usr/bin/rsync`;
- `osync` расположен в `/usr/bin/osync`;
- журнал `sysvolsync` пишется в файл `/var/log/osync_*.log`;
- настроено беспарольное взаимодействие между `root`ами всех контроллеров домена (см. п. 10.6.17).

На первом контроллере домена (DC1):

1) установить пакеты `rsync` и `osync`:

```
# apt-get install rsync osync
```

2) отредактировать файл `/etc/osync/sync.conf`:

```
#!/usr/bin/env bash
INSTANCE_ID="sync_sysvol"
# Путь до SysVol на текущем сервере
INITIATOR_SYNC_DIR="/var/lib/samba/sysvol"
# Путь до SysVol на удаленном сервере
TARGET_SYNC_DIR="ssh://root@DC2:22//var/lib/samba/sysvol"
# ssh ключ root
SSH_RSA_PRIVATE_KEY="/root/.ssh/id_ed25519"
# Удаленные хосты которые osync пингует перед стартом
REMOTE_3RD_PARTY_HOSTS=""
```

```
# Сохранять xattr
PRESERVE_ACL=yes
# Сохранять xattr
PRESERVE_XATTR=yes
# Сохранять резервную копию удаленных файлов
SOFT_DELETE=yes
DESTINATION_MAILS="your@test.alt"
REMOTE_RUN_AFTER_CMD="/usr/bin/samba-tool ntacl sysvolreset"
```

На втором контроллере домена (DC2) установить пакет rsync:

```
# apt-get install rsync
```

Примечание. Перед запуском команды синхронизации рекомендуется сделать резервную копию каталога sysvol.

Запустить команду синхронизации:

```
# /usr/bin/osync.sh /etc/osync/sync.conf --dry --verbose
```

Если команда выполнилась без ошибок, можно удалить параметр `--dry` и запустить команду синхронизации снова:

```
# /usr/bin/osync.sh /etc/osync/sync.conf --verbose
```

В результате sysvol будет синхронизирован на обоих серверах.

Примечание. Если в файле sysvol параметры `SOFT_DELETE` (сохранять резервные копии удаленных файлов) и `CONFLICT_BACKUP` (сохранять резервные копии файлов на целевой реплике, если они обновлены из исходной реплики) установлены в значение `yes`, то на источнике и получателе репликации необходимо создать каталоги `.osync_workdir/deleted` и `.osync_workdir/backup`:

```
# mkdir /var/lib/samba/sysvol/.osync_workdir/deleted
# mkdir /var/lib/samba/sysvol/.osync_workdir/backup
```

На DC1 включить синхронизацию по расписанию:

```
# crontab -e
*/5 * * * * root /usr/local/bin/osync.sh /etc/osync/sync.conf --silent
```

Если при попытке синхронизировать каталог возникают проблемы необходимо:

- отключить синхронизацию по расписанию на DC1;
- убедиться, что rsync и osync не выполняются в данный момент (можно проверить, выполнив команду `ps -aux | grep sync`);
- удалить хеш-файлы `.osync_workdir` на DC1 и DC2 в `/var/lib/samba/sysvol/`;
- проверить sysvol и повторить синхронизацию;
- убедиться, что синхронизация выполнена успешно;

- включить синхронизацию по расписанию на DC1.

Если контроллеров домена больше чем два, можно создать больше заданий для cron на DC1:

- 1) скопировать файл `/etc/osync/sync.conf` в другой файл, например: `/etc/osync/sync_dc3.conf`;
- 2) в файле `/etc/osync/sync_dc3.conf` изменить значение параметра `TARGET_SYNC_DIR`;
- 3) повторить шаги 1 и 2 для всех контроллеров домена;
- 4) изменить задание на синхронизацию по расписанию на DC1:

```
# crontab -e
*/5 * * * * root /usr/local/bin/osync.sh /etc/osync/sync.conf --silent
*/5 * * * * root /usr/local/bin/osync.sh /etc/osync/sync_dc3.conf --silent
...
```

10.6.7.3.3. Сопоставление встроенных идентификаторов пользователей и групп

По умолчанию контроллер домена Samba сохраняет идентификаторы пользователей и групп в атрибутах `xidNumber` в `idmap.ldb`. Из-за особенностей работы `idmap.ldb` нельзя гарантировать, что каждый контроллер домена будет использовать один и тот же идентификатор для данного пользователя или группы.

Ниже описана процедура синхронизации `idmap.ldb` с контроллера домена, на котором установлена роль FSMO «Эмулятор PDC» (PDC Emulator), со всеми остальными контроллерами домена. Для достижения наилучших результатов следует регулярно синхронизировать `idmap.ldb`.

На контроллере домена, имеющего роль FSMO «Эмулятор PDC»:

- 1) установить пакет `ldb-tools`, если он еще не установлен:


```
# apt-get install ldb-tools
```
- 2) создать резервную копию файла `/var/lib/samba/private/idmap.ldb`:


```
# rm -f /var/lib/samba/private/idmap.ldb.bak
# tdbbackup -s .bak /var/lib/samba/private/idmap.ldb
```
- 3) создать ежедневное задание cron:


```
# Создание резервной копии idmap.ldb
```

ЛКНВ.11100-01 90 03

```
0 3 * * * rm -f /var/lib/samba/private/idmap.ldb.bak &&
tdbbackup -s .bak /var/lib/samba/private/idmap.ldb >/dev/null
2>&1
```

На контроллерах домена, которые не выполняют роль эмулятора PDC:

- 1) скопировать файл резервной копии, созданный на DC с ролью FSMO «Эмулятор PDC» (в примере dc1), в каталог /var/lib/samba/private/ с удалением суффикса .bak (заменить существующий файл):

```
# rsync -a dc1:/var/lib/samba/private/idmap.ldb.bak
/var/lib/samba/private/idmap.ldb
```

- 2) запустить очистку кеша:

```
# net cache flush
```

- 3) проверить разрешения ACL SysVol и при необходимости сбросить их:

```
# if ! samba-tool ntacl sysvolcheck; then samba-tool ntacl
sysvolreset; fi
```

- 4) если все прошло успешно, создать ежедневное задание cron:

```
#Sync idmap.ldb
15 4 * * * rsync -a dc1:/var/lib/samba/private/idmap.ldb.bak
/var/lib/samba/private/idmap.ldb && net cache flush && if !
samba-tool ntacl sysvolcheck; then samba-tool ntacl
sysvolreset; fi >/dev/null 2>&1
```

10.6.8. Настройка Samba для привязки к определенным интерфейсам

Если на сервере настроено несколько сетевых интерфейсов, можно настроить Samba для привязки только к определенным интерфейсам.

Например, для того чтобы привязать все службы Samba к устройству enp0s3 и loopback (lo) необходимо добавить следующие параметры в раздел [global] файла smb.conf:

```
bind interfaces only = yes
interfaces = lo enp0s3
```

и перезапустить службу Samba:

```
# systemctl restart samba.service
```

Примечания:

1. В параметре interfaces вместо имен интерфейсов можно указывать IP-адреса.

2. Некоторые утилиты подключаются к петлевому IP-адресу, если имя хоста не указано. Поэтому всегда нужно указывать Samba прослушивать петлевые (lo) устройства.

10.6.9. Создание keytab-файла

10.6.9.1. Назначение и формат SPN

SPN (Service Principal Name) – уникальный идентификатор экземпляра сервиса. SPN используется аутентификацией Kerberos для сопоставления экземпляра сервиса с учетной записью сервиса (service logon account). Это позволяет клиентским приложением аутентифицироваться в роли сервиса даже не зная имени пользователя.

До того, как аутентификация Kerberos сможет использовать SPN для аутентификации сервиса, SPN должен быть привязан к учетной записи, которая будет использоваться для входа. К учетной записи может быть привязано несколько SPN. SPN может быть привязан только к одной учетной записи. Если учетная запись, привязанная к SPN, изменяется, то необходимо заново выполнить привязку.

Можно иметь столько SPN, сколько необходимо. Когда клиент хочет воспользоваться сервисом, он находит экземпляр сервиса и составляет SPN для этого экземпляра, далее использует этот SPN для аутентификации. Если клиент не может найти правильный SPN, он не сможет запросить билет службы.

SPN состоит из двух обязательных элементов и двух дополнительных элементов:

```
<service class>/<host>:<port>/<service name>
```

Элементы SPN:

- `service class` (обязательный элемент) – строка, указывающая на класс, к которому относится сервис (например: HTTP, www, ldap и т. п.);
- `host` (обязательный элемент) – имя компьютера, на котором работает сервис; это может быть полное доменное имя (FQDN) или NetBIOS-имя;
- `port` – номер порта; может использоваться в том случае, если несколько экземпляров сервиса одного класса работают на одном узле; не требуется

указывать, если экземпляр сервиса один и работает на стандартном для своего класса порту;

- `service name` – имя реплицируемого сервиса, которое позволяет идентифицировать предоставляемые сервисом данные или обслуживаемый сервисом домен; в качестве имени могут использоваться DNS-имя или `objectGUID` объекта службы каталогов, DNS-имя домена (если сервис реализует определенную службу на уровне всего домена), DNS-имя записи `SRV` или `MX`.

П р и м е ч а н и е . Если клиент не может найти правильный SPN, он не сможет запросить билет службы. Поэтому формирование SPN было глобально нормализовано:

- для файлового сервера могут использоваться следующие SPN (их можно добавить столько, сколько нужно):
`HOST/fileserver.test.alt`
`HOST/fileserver`
`HOST/fileserver@TEST.ALT`
`CIFS/fileserver.test.alt`
- для веб-сервера (подробнее см. п. 10.6.10.1):
`HTTP/web.test.alt`
- для прокси-сервера:
`HTTP/proxy.test.alt`
- на практике можно сопоставить SPN с IP-адресом, но это не рекомендуется:
`HOST/192168.0.129@TEST.ALT`

Keytab-файл – это файл, содержащий пары Kerberos принципалов и их ключей (полученных с использованием Kerberos пароля). Эти файлы используются для аутентификации в системах, использующих Kerberos, без ввода пароля. Если пароль принципала изменится, то keytab-файл необходимо будет сгенерировать заново.

ВАЖНО

Каждый кто имеет разрешения на чтения keytab-файла может воспользоваться любыми ключами в нем. Чтобы предотвратить нежелательное использование, необходимо ограничивать права доступа при создании keytab-файла.

10.6.9.2. Создание SPN и генерация keytab с помощью `samba-tool`

Добавить имена SPN для пользователя можно с помощью команды `samba-tool`:

```
samba-tool spn add host/fdqn@KerberosRealm <sAMAccount name>
```

В качестве аргументов передаются значение SPN и имя учетной записи SAM (значение атрибута sAMAccountName).

После добавления SPN можно сгенерировать keytab, выполнив команду:

```
samba-tool domain exportkeytab <имя>.keytab \  
--principal=[<sAMAccount name> | <SPN>]
```

В результате выполнения этой команды будет создан keytab-файл <имя>.keytab, содержащий UPN или SPN, в зависимости от того, что было указано в параметре --principal.

Получить дополнительную информацию можно на справочной странице samba-tool (8) (man samba-tool).

Примечание. В команде нужно использовать или <sAMAccount name> или <SPN>, но не оба параметра сразу.

Пример:

- привязать к пользователю SPN:

```
# samba-tool spn add HTTP/test.alt webauth
```

- создать keytab:

```
# samba-tool domain exportkeytab /tmp/web.keytab \  
--principal=HTTP/test.alt  
Export one principal to /tmp/keytab
```

- проверка:

```
# klist -ke /tmp/web.keytab  
Keytab name: FILE:/tmp/web.keytab  
KVNO Principal  
-----  
2 HTTP/test.alt@TEST.ALT (DEPRECATED:arcfour-hmac)
```

Можно также проверить авторизацию в домене по имени SPN с помощью keytab-файла. Для этого на контроллере домена получить билет Kerberos:

```
# kinit administrator@TEST.ALT  
Password for administrator@TEST.ALT:
```

И выполнить команду:

```
# kinit -5 -V -k -t /tmp/web.keytab HTTP/test.alt  
Using default cache: /tmp/krb5cc_0  
Using principal: HTTP/test.alt@TEST.ALT  
Using keytab: /tmp/web.keytab  
Authenticated to Kerberos v5
```


Примечание. Если при проверке авторизации возникает ошибка:

```
kinit: Client not found in Kerberos database while getting initial
credentials
```

необходимо в ADMS изменить для пользователя webauth значение параметра userPrincipalName на значение servicePrincipalName + REALM (в данном примере нужно поменять webauth на HTTP/test.alt@TEST.ALТ рис. 500).

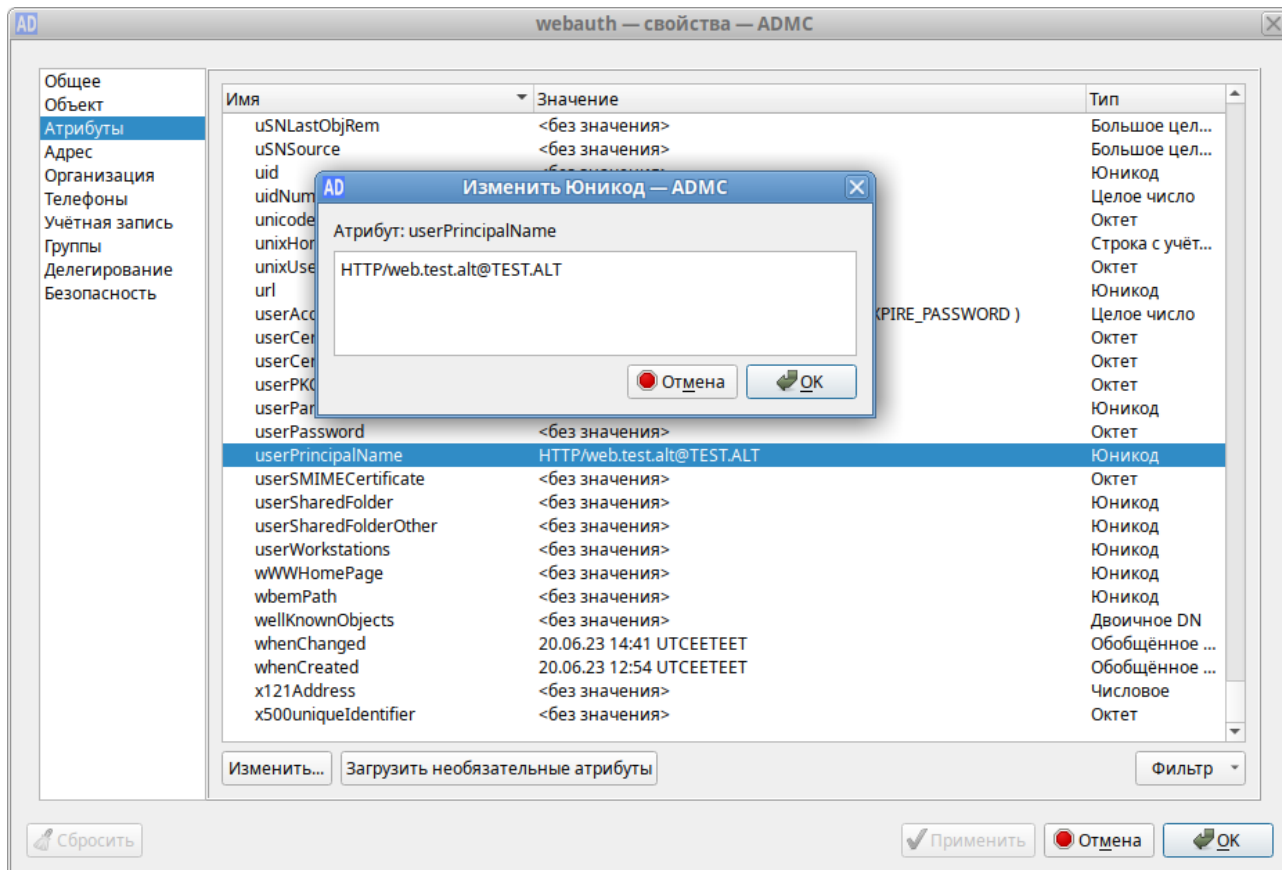


Рис. 500 – Изменение параметра userPrincipalName в ADMS

Для получения списка идентификаторов SPN, привязанных к учетной записи, используется команда:

```
samba-tool spn list <user> [options]
```

В качестве аргумента передается имя учетной записи SAM (значение атрибута sAMaccountName).

Команда удаления идентификатора SPN, привязанного к учетной записи пользователя:

```
samba-tool spn delete <name> <user> [options]
```

В качестве аргументов передаются значение SPN (name) и имя учетной записи SAM (значение атрибута sAMaccountName).

10.6.10. Аутентификация других сервисов в домене

10.6.10.1. Настройка аутентификации Kerberos для веб-сервера Apache

В этом разделе показано, как обеспечить прозрачную авторизацию пользователей домена на веб-сайте, размещенном на веб-сервере Apache2.

В качестве веб-сервера используется отдельный сервер (web.test.alt, IP-адрес 192.168.0.150), введенный в домен.

Примечание. Веб-сервер может быть присоединен или не присоединен к домену, это не имеет значения.

Для работы требуется наличие прямой и обратной записей DNS для веб-сервера. DNS, предоставленный во время настройки, поставляется только с рабочей прямой зоной (и только прямой записью для DC, поэтому понадобится добавить прямую запись для веб-сервера, в качестве веб-сервера используется не DC).

Если в качестве веб-сервера используется не DC, следует добавить A-запись для веб-сервера:

```
$ samba-tool dns add dc1 test.alt web A 192.168.0.150 -Uadministrator
Password for [TEST\administrator]:
Record added successfully
```

10.6.10.1.1. Создание keytab-файла

Нужно настроить SPN (имена участников-служб) для имени сервера, на которое разрешается любой веб-сайт. Если виртуальный хостинг не используется, веб-адрес и имя машины будут одинаковыми. Для создания SPN на контроллере домена выполнить команды:

```
# samba-tool user create --random-password webauth
# samba-tool user setexpiry webauth --noexpiry
# samba-tool spn add HTTP/web.test.alt webauth
```

Создать Kerberos keytab файл для Apache2:

```
# samba-tool domain exportkeytab /tmp/httpd.keytab \
--principal=HTTP/web.test.alt@TEST.ALT
```

```
Export one principal to /tmp/httpd.keytab
```

Перенести полученный файл `keytab` на веб-сервер в `/etc/httpd2/conf/`, установить права на него, так чтобы Apache мог читать, но не изменять `keytab`-файл:

```
# chown apache2:apache2 /etc/httpd2/conf/httpd.keytab
# chmod 0440 /etc/httpd2/conf/httpd.keytab
```

10.6.10.1.2. Настройка Apache2

Для настройки Apache2 необходимо выполнить следующие действия:

1) на веб-сервере установить пакет `apache2-mod_auth_gssapi` и включить необходимые модули:

```
# apt-get install apache2-mod_auth_gssapi
# a2enmod auth_gssapi
# a2enmod authn_core
# a2enmod authz_user
# service httpd2 condreload
```

2) добавить в конфигурацию Apache строки:

```
<Location "/login.html">
    AuthType GSSAPI
    AuthName "GSSAPI Login"
    #GssapiBasicAuth On
    GssapiCredStore keytab:/etc/httpd2/conf/httpd.keytab
    GssapiAllowedMech krb5
    Require valid-user
</Location>
```

3) добавить файл `login.html` в корень веб-сервера, например:

```
# echo '<html><body><h1>It works!</h1></body></html>' >
/var/www/html/login.html
```

4) перезапустить Apache:

```
# systemctl restart httpd2
```

10.6.10.1.3. Проверка аутентификации

Тестовый сайт должен быть доступен по адресу

`http://<полное_доменное_имя_веб-сервера>`.

На рабочей станции, введенной в домен, получить билет Kerberos:

```
$ kinit ivanov
Password for ivanov@TEST.ALT:
$ klist
Ticket cache: KEYRING:persistent:500:krb_ccache_5VitJSL
Default principal: ivanov@TEST.ALT
```

```
Valid starting          Expires                Service principal
```

```
28.04.2023 15:54:41 29.04.2023 01:54:41 krbtgt/TEST.ALT@TEST.ALT
renew until 05.05.2023 15:54:38
```

Попытаться прочитывать содержимое сайта, используя аутентификацию

Kerberos:

```
$ curl --negotiate -u : http://web.test.alt/login.html
<html><body><h1>It works!</h1></body></html>
```

Получено содержимое страницы.

Удалить билеты Kerberos:

```
$ kdestroy
$ klist
```

Попытаться прочитывать содержимое сайта используя аутентификацию

Kerberos:

```
$ curl --negotiate -u : http://web.test.alt/login.html
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">

<head>
<title>Authentication required!</title>
</head>

<body>
<h1>Authentication required!</h1>
...
<h2>Error 401</h2>
<address>
  <a href="/">web.test.alt</a><br />
  <span>Apache/2.4.62 (Unix) mod_auth_gssapi/1.6.3 OpenSSL/1.1.1u</span>
</address>
</body>
</html>
```

Содержимое страницы не доступно.

10.6.10.2. Настройка аутентификации Kerberos для веб-сервера Nginx

В этом разделе показано, как обеспечить прозрачную авторизацию пользователей домена на веб-сайте, размещенном на веб-сервере Nginx.

В качестве веб-сервера используется отдельный сервер (web.test.alt, IP-адрес 192.168.0.150), введенный в домен.

Примечание. Веб-сервер может быть присоединен или не присоединен к домену, это не имеет значения.

Добавить зону обратного просмотра для подсети 192.168.0.0/24, в которой располагается веб-сервер:

```
# samba-tool dns zonecreate dc1.test.alt 0.168.192.in-addr.arpa -Uadministrator
```

```
Password for [TEST\administrator]:
Zone 0.168.192.in-addr.arpa created successfully
```

где `dc1.test.alt` – имя контроллера домена.

Если требуется более одной обратной зоны (при использовании нескольких подсетей), следует запустить приведенную выше команду еще раз, но с данными для другой подсети.

Обратная зона работает напрямую без перезапуска Samba или BIND.

Добавить зону обратного просмотра для веб-сервера:

```
# samba-tool dns add dc1.test.alt 0.168.192.in-addr.arpa 150 PTR
web.test.alt -Uadministrator
```

10.6.10.2.1. Создание keytab-файла

Нужно настроить SPN (имена участников-служб) для имени сервера, на которое разрешается любой веб-сайт (таким образом, фактическое имя сервера, на которое указывает CNAME, является полным). Если виртуальный хостинг не используется, веб-адрес и имя машины будут одинаковыми. Для этого на контроллере домена:

```
# samba-tool user create --random-password nginxauth
# samba-tool user setexpiry nginxauth
# samba-tool spn add HTTP/web.test.alt nginxauth
```

Создать Kerberos keytab файл для Nginx:

```
# samba-tool domain exportkeytab /tmp/nginx.keytab \
--principal=HTTP/web.test.alt@TEST.ALT
```

```
Export one principal to /tmp/nginx.keytab
```

10.6.10.2.2. Настройка Nginx

Для работы прозрачной доменной аутентификации (SSO) в Nginx необходимо установить пакеты `nginx` и `nginx-spnego`:

```
# apt-get install nginx nginx-spnego
```

Модуль SPNEGO для Nginx – это программный компонент для возможности прохождения аутентификации (Single Sign-On или SSO) через сервер LDAP.

Включить модуль `http_auth_spnego`:

```
# ln -s /etc/nginx/modules-available.d/http_auth_spnego.conf
/etc/nginx/modules-enabled.d/
```

Перенести полученный на контроллере домене файл `keytab` на веб-сервер в `/etc/nginx`. Установить права на файл `keytab`:

```
# chmod 644 /etc/nginx/nginx.keytab
```

`Nginx` должен иметь права на чтение файла `keytab`, но не на его изменение.

Настроить аутентификацию в секции «`Server`» файла конфигурации сайта:

```
server {
    ...
    location /
    {
        root /var/www/html;
        auth_gss on;
        auth_gss_realm TEST.ALT; #имя kerberos области
        auth_gss_keytab /etc/nginx/nginx.keytab; #путь к keytab-файлу
        auth_gss_service_name HTTP/web.test.alt; #имя используемого SPN
        auth_gss_allow_basic_fallback off;
    }
}
```

Описание опций:

- `auth_gss` – включение/отключение аутентификации;
- `auth_gss_keytab` – абсолютный путь к файлу `keytab`, содержащему учетные данные службы;
- `auth_gss_realm` – имя области Kerberos;
- `auth_gss_service_name` – имя субъекта-службы, используемое при получении учетных данных;
- `auth_gss_allow_basic_fallback` – включить/отключить базовую аутентификацию. При включенной базовой аутентификации (по умолчанию), если SSO не проходит (машина не в домене) разрешает обычный ввод логина и пароля. Если используется SPNEGO без SSL, рекомендуется отключить базовую аутентификацию, так как в этом случае пароль будет отправлен в виде открытого текста.

Перезапустить `nginx`:

```
# systemctl restart nginx
```

Если нужно авторизовать только определенный набор пользователей, можно использовать в параметре `auth_gss_authorized_principal`. Можно указывать несколько записей, по одной на строку:

```
auth_gss_authorized_principal <username>@<realm>
auth_gss_authorized_principal <username2>@<realm>
```

Список пользователей также можно указать с помощью шаблона регулярного выражения в параметре `auth_gss_authorized_principal_regex`. Этот параметр можно использовать вместе с параметром `auth_gss_authorized_principal`:

```
auth_gss_authorized_principal <username>@<realm>
auth_gss_authorized_principal_regex ^(<username>)/(<group>)@<realm>$
```

10.6.10.2.3. Проверка аутентификации

Тестовый сайт должен быть доступен по адресу `http://<полное_доменное_имя_веб-сервера>`.

На рабочей станции, введенной в домен, получить билет Kerberos:

```
$ kinit ivanov
Password for ivanov@TEST.ALT:
$ klist
Ticket cache: KEYRING:persistent:500:krb_ccache_5VitJSL
Default principal: ivanov@TEST.ALT

Valid starting      Expires            Service principal
28.04.2023 15:54:41  29.04.2023 01:54:41  krbtgt/TEST.ALT@TEST.ALT
    renew until 05.05.2023 15:54:38
```

Попытаться прочитать содержимое сайта используя аутентификацию Kerberos:

```
$ curl --negotiate -u : http://web.test.alt
<html><body><h1>It works!</h1></body></html>
```

Получено содержимое страницы.

Удалить билеты Kerberos:

```
$ kdestroy
$ klist
```

Попытаться прочитать содержимое сайта используя аутентификацию Kerberos:

```
$ curl --negotiate -u : http://web.test.alt

<html>
<head><title>401 Authorization Required</title></head>
<body>
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.22.1</center>
</body>
```

</html>

Содержимое страницы не доступно.

10.6.10.3. Настройка веб-браузеров для SSO

Предварительно необходимо ввести компьютер в домен (см. п. 10.3) и убедиться, что доменный пользователь получает билет Kerberos.

Для работы SSO в веб-браузерах необходимо произвести некоторые настройки.

10.6.10.3.1. Настройка Mozilla Firefox

Порядок действий:

- 1) в адресной строке ввести `about:config`, чтобы отобразить список текущих параметров конфигурации (необходимо будет нажать кнопку «Принять риск и продолжить»);
- 2) в поле «Фильтр» ввести «negotiate», чтобы ограничить список параметров»;
- 3) выбрать параметр `network.negotiate-auth.trusted-uris`;
- 4) указать в этом параметре имя `kerberos` области (`realm`), включая предшествующую точку (`.`). Если нужно добавить несколько доменов, их необходимо указать через запятую (рис. 501);
- 5) в ряде случаев может потребоваться отредактировать еще несколько параметров:
 - параметр `network.automatic-ntlm-auth.trusted-uris` **ВЫСТАВИТЬ В** `kerberos realm: .test.alt`;
 - параметр `network.negotiate-auth.delegation-uris` **ВЫСТАВИТЬ В** `kerberos realm: .test.alt`;
 - параметр `network.automatic-ntlm-auth.allow-non-fqdn` **ВЫСТАВИТЬ В: true**;
 - параметр `network.negotiate-auth.allow-non-fqdn` **ВЫСТАВИТЬ В: true**.

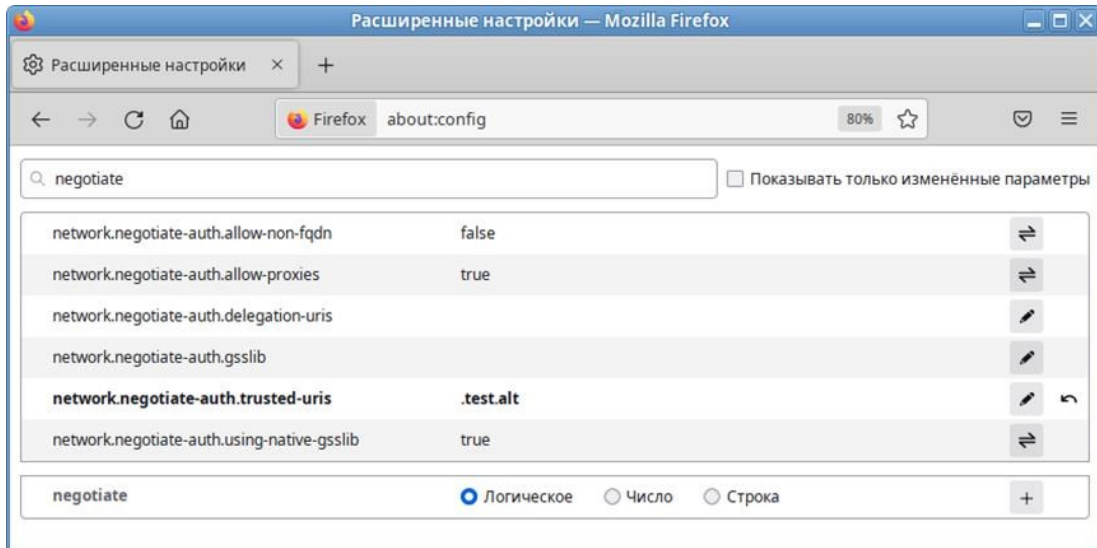


Рис. 501 – Ограниченный список параметров конфигурации

Вместо выставления этих параметров можно создать файл `/usr/lib64/firefox/browser/defaults/preferences/prefs.js` со следующим содержимым:

```
pref("network.negotiate-auth.trusted-uris", ".test.alt");
pref("network.automatic-ntlm-auth.trusted-uris", ".test.alt");
pref("network.automatic-ntlm-auth.allow-non-fqdn", "true");
pref("network.negotiate-auth.allow-non-fqdn", "true");
pref("network.negotiate-auth.delegation-uris", ".test.alt");
```

Эти параметры могут быть распространены через групповые политики для Firefox (см. п. 10.4.6.4.10):

- параметр `network.negotiate-auth.trusted-uris` – политика SPNEGO;
- параметр `network.automatic-ntlm-auth.trusted-uris` – политика NTLM;
- параметр `network.negotiate-auth.delegation-uris` – политика «Делегированная авторизация»;
- параметр `network.automatic-ntlm-auth.allow-non-fqdn` – политика «Разрешить неполное доменное имя» (Non FQDN);
- параметр `network.negotiate-auth.allow-non-fqdn` – политика «Разрешить неполное доменное имя» (Non FQDN).

10.6.10.3.2. Настройка Chromium

В файл `/etc/chromium/policies/managed/policies.json` добавить строки:

```
{
  "AuthServerAllowlist": "*.test.alt",
  "AuthNegotiateDelegateAllowlist": "*.test.alt"
}
```

где `.test.alt` – имя `kerberos` области (`realm`).

Для применения настроек необходимо перезапустить веб-браузер. Результат применения параметров политики для Chromium можно проверить, указав в адресной строке URL: `chrome://policy`.

Этот параметр может быть распространен через групповые политики для Chromium (см. п. 10.4.6.4.9): политика «Список разрешенных серверов для аутентификации» и «Список разрешенных серверов для делегирования прав по протоколу Kerberos».

Примечание. Для проверки работы аутентификации без изменения настроек веб-браузера можно запустить веб-браузер из командной строки, выполнив команду:

```
$ chromium-browser --auth-server-whitelist="*.test.alt"
```

10.6.10.3.3. Настройка «Яндекс.Браузера»

В файл `/etc/opt/yandex/browser/policies/managed/policies.json` добавить строки:

```
{
  "AuthServerAllowlist": "*.test.alt",
  "AuthNegotiateDelegateAllowlist": "*.test.alt"
}
```

где `.test.alt` – имя `Kerberos` области (`realm`).

Для применения настроек необходимо перезапустить браузер. Результат применения параметров политики для «Яндекс.Браузера» можно проверить, указав в адресной строке URL: `browser://policy`.

Эти параметры могут быть распространены через групповые политики для «Яндекс.Браузера» (см. п. 10.4.6.4.11): политики «Разрешить аутентификацию на серверах из списка» и «Разрешить делегирование прав по протоколу Kerberos на серверах».

10.6.11. Distributed File System

Распределенная файловая система (Distributed File System, DFS) – серверная технология Microsoft, предназначенная для упрощения доступа к общим файловым ресурсам, распределенным по сети. С помощью DFS можно объединять в единую логическую структуру файловые ресурсы, физически находящиеся на различных серверах, а также производить между ними репликацию. Функционал DFS образуют две составляющих: пространство DFS-имен – DFS-N (DFS-Namespace) и механизм репликации – DFS-R (DFS-Replication).

Samba поддерживает DFS-N, но пока не поддерживает DFS-R.

10.6.11.1. Пространство DFS-имен

Пространство DFS-имен – это единый виртуальный каталог, содержащий ссылки на общие каталоги, расположенные на разных файловых серверах. Пространство имен состоит из корня (root), ссылок (folders) и целевых объектов (folder targets). Пространство имен DFS может быть двух типов: автономное (Stand-alone) и доменное (Domain-based).

Автономный вариант работает на одном сервере и приводит к тому, что имена DFS содержат имя этого сервера, они выглядят как общие ресурсы, предоставляемые этим сервером (можно создать распределенную файловую систему, не используя доменные службы).

При доменном варианте имена DFS содержат только имя домена, а не имя какого-либо конкретного сервера (имя сервера пространства имен скрыто от пользователей, проще замена сервера пространства имен или перенос пространства имен на другой сервер).

Корень пространства имен (Namespace root) – это базовая точка, от которой начинается отсчет пространства имен (рис. 502). В зависимости от типа корень доступен по адресу `\\ServerName\RootName` (Stand-alone) или `\\DomainName\RootName` (Domain-based).

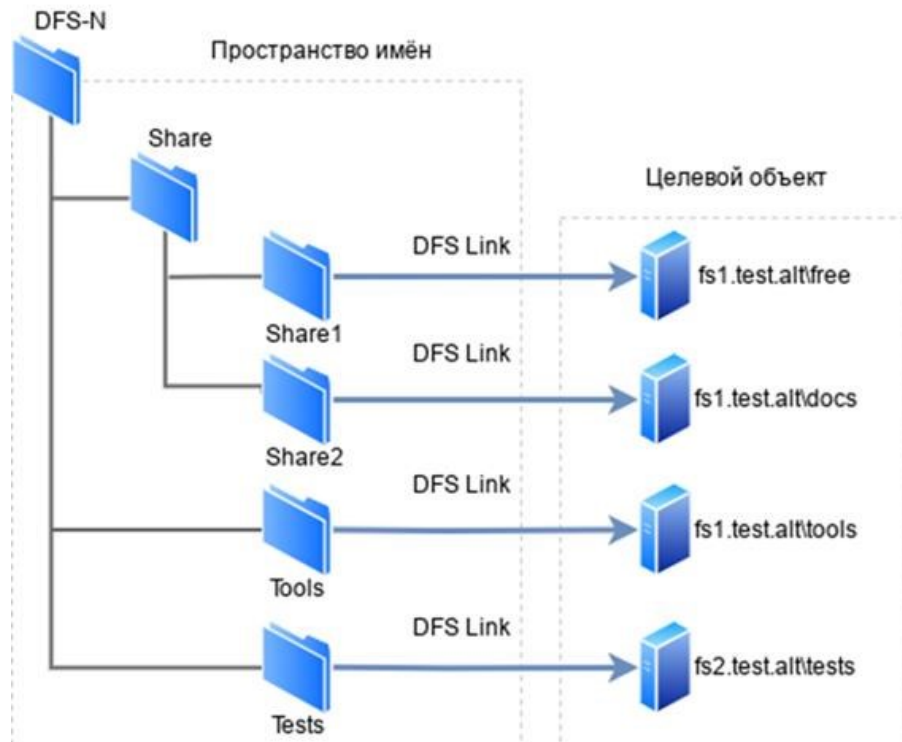


Рис. 502 – Структура дерева

Каталог – ссылка в пространстве имен DFS, указывающая на целевой объект. Каталог без конечных объектов (например, каталог Share) образуют структуру и иерархию в пространстве имен, а каталоги с целевыми объектами (например, каталог Share1) предоставляют пользователям доступ к фактическому содержимому.

Целевой объект (Folder targets) – ссылка на общий файловый ресурс, находящийся на определенном файловом сервере. Одна ссылка может указывать как на один, так и на несколько целевых объектов.

10.6.11.2. Настройка DFS на сервере Samba

Прежде, чем перейти к добавлению пространства имен, необходимо создать хотя бы один сетевой каталог на любом из серверов, добавленных в домен.

Сервер Samba можно сделать сервером DFS, задав логический параметр `host msdfs` в файле `smb.conf`.

Корень DFS назначается с помощью логического параметра `root msdfs`. Если для этого параметра установлено значение `yes`, Samba будет воспринимать открытый для общего доступа ресурс как корневой DFS. Ссылки DFS, указываемые в открытом для доступа каталоге, имеют вид:

msdfs:serverA\shareA, serverB\shareB и т. д. Корневой каталог DFS в Samba содержит ссылки DFS в виде символических ссылок.

Для создания нового пространства имен необходимо выполнить следующие действия:

- 1) создать каталог, в котором будут настроены ссылки DFS на другие серверы в сети (в примере /media/dfsroot):

```
# mkdir /media/dfsroot
```

- 2) в файле /etc/samba/smb.conf в секцию [global] добавить параметр:

```
host msdfs = yes
```

и добавить секцию [dfs], с указанием корня:

```
[dfs]
    path = /media/dfsroot
    msdfs root = yes
```

- 3) в каталоге /media/dfsroot настроить ссылки DFS на общие ресурсы в сети:

```
# cd /media/dfsroot
# ln -s msdfs:dcl.test.alt\\free linka
# ln -s msdfs:web.test.alt\\tests linkb
```

- 4) перезапустить samba:

```
# systemctl restart samba
```

- 5) дерево DFS теперь доступно по адресу //test.alt/dfs/. При доступе к ссылкам linka или linkb (которые отображаются для клиента как каталоги) пользователи напрямую переходят к соответствующим общим ресурсам в сети.

Проверка:

```
$ smbclient //test.alt/dfs/linka -U 'ivanov'
Password for [TEST\ivanov]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D                0  Mon May 22 10:13:28 2023
..               D                0  Mon May 22 10:13:06 2023
dc.txt           N                5  Mon May 22 15:57:14 2023

      48254668 blocks of size 1024. 40859796 blocks available
smb: \> exit
```

Примечание. Для доступа к ресурсам DFS по имени домена с использованием аутентификации Kerberos необходимо добавить к имени сервера псевдоним – имя домена. Это можно сделать, выполнив на контроллере домена команду:

```
# samba-tool spn add cifs/cifs/<имя_домена> <имя_сервера>$
```

Например:

```
# samba-tool spn add cifs/test.alt dc1$
```

Подключиться к данному пространству можно, набрав в адресной строке следующий адрес: `smb://<имя_домена>/<имя_пространства_имен>` (рис. 503).

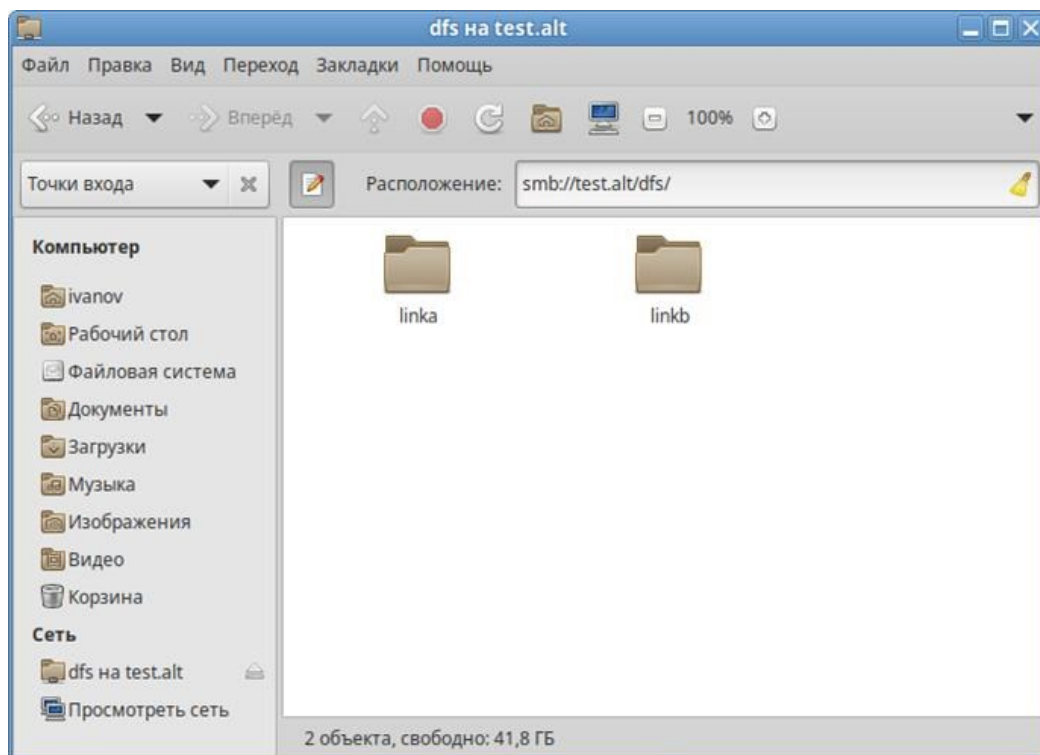


Рис. 503 – Подключение к пространству

10.6.12. Настройка SSSD

10.6.12.1. Журналирование SSSD

10.6.12.1.1. Файлы журналов SSSD

Каждая служба SSSD записывает логи в свой собственный файл журнала в каталоге `/var/log/sss/`. Например, для машины в домене `test.alt`, файлы журналов SSSD могут выглядеть следующим образом:

```
# ls -l /var/log/sss/
итого 1660
-rw----- 1 _sssd _sssd      0 мая 18 12:55 gpo_child.log
```

```

-rw----- 1 _sssd _sssd      0 мая 18 12:55 krb5_child.log
-rw----- 1 _sssd _sssd      0 мая 18 12:54 ldap_child.log
-rw----- 1 root  root      261 июн 19 10:10 sssd_ifp.log
-rw----- 1 root  root     3955 июн 19 09:34 sssd.log
-rw----- 1 _sssd _sssd 1677605 июн 19 11:18 sssd_nss.log
-rw----- 1 _sssd _sssd   1134 июн 19 09:34 sssd_pac.log
-rw----- 1 _sssd _sssd   3067 июн 19 09:34 sssd_pam.log
-rw----- 1 _sssd _sssd      0 мая 18 12:54 sssd_TEST.ALT.log

```

где:

- krb5_child.log – файл журнала для недолговечного вспомогательного процесса, участвующего в аутентификации Kerberos;
- ldap_child.log – файл журнала для недолговечного вспомогательного процесса, участвующего в получении билета Kerberos для связи с сервером LDAP\$;
- sssd_<domain.name>.log – для каждого раздела [domain] в файле sssd.conf служба SSSD записывает информацию о взаимодействии с LDAP-сервером в отдельный файл журнала;
- sssd.log – файл журнала для мониторинга SSSD и связи его с ответчиком и внутренними процессами;
- sssd_ifp.log – файл журнала для ответчика InfoPipe, который предоставляет общедоступный интерфейс D-Bus, доступный через системную шину;
- sssd_nss.log – файл журнала для ответчика Name Services Switch (NSS), который извлекает информацию о пользователях и группах;
- sssd_pac.log – файл журнала для ответчика Microsoft Privilege Attribute Certificate (PAC), который собирает PAC из билетов AD Kerberos и извлекает информацию о пользователях AD из PAC, что позволяет избежать ее запроса непосредственно из AD;
- sssd_pam.log – файл журнала для ответчика Pluggable Authentication Module (PAM);
- sssd_ssh.log – файл журнала для процесса ответчика SSH.

10.6.12.1.2. Уровни журналирования SSSD

Уровни журналирования SSSD представлены в таблице 83.

Установка уровня журнала также включает все уровни ниже него. Например, установка уровня журнала на 6 также включает уровни с 0 по 5.

Чтобы вести журнал для необходимых уровней журналирования, указанных в представлении битовых масок, следует просто сложить их номера. Например, чтобы вести журнал для фатальных, критических, серьезных ошибок и для данных функций, следует использовать значение 0x0270.

Т а б л и ц а 83 – Уровни журналирования SSSD

Уровень	Описание
0 (0x0010)	Фатальные ошибки. Ошибки, которые не позволяют запустить службу SSSD или вызывает завершение работы сервиса
1 (0x0020)	Критические ошибки. Ошибки, которые не завершают работу службы SSSD, но означает, что как минимум одна из основных функций не работает должным образом
2 (0x0040)	Серьезные ошибки. Ошибки, сообщающие о том, что определенный запрос или операция завершились неудачно. Это уровень журналирования по умолчанию
3 (0x0080)	Незначительные ошибки. Ошибки, которые могут стать причиной ошибок 2-го уровня (ошибок при выполнении действий)
4 (0x0100)	Настройки конфигурации
5 (0x0200)	Данные функций
6 (0x0400)	Сообщения трассировки для функций действий
7 (0x1000)	Сообщения трассировки для функций внутреннего управления
8 (0x2000)	Содержимое переменных внутренних функций
9 (0x4000)	Информация трассировки крайне низкого уровня
9 (0x20000)	Быстродействие и статистические данные. Из-за способа обработки запросов на внутреннем уровне, записанное в журнал время выполнения запроса может быть больше, чем оно было на самом деле
10 (0x10000)	Информация трассировки libldb еще более низкого уровня. Практически никогда не требуется

10.6.12.1.3. Настройка уровня журналирования в файле `sssd.conf`

Чтобы включить подробное журналирование, сохраняющееся при перезапуске службы SSSD, следует добавить опцию `debug_level=<целое_число>` в каждую секцию файла `/etc/sssd/sssd.conf`.

Где `<целое_число>` – число от 0 до 10. Уровни до 3 регистрируют крупные сбои, а уровни начиная с 8 и выше предоставляют большое количество подробных сообщений журнала. Уровень 6 является хорошей отправной точкой для отладки проблем.

Пример настройки уровня журналирования в файле `/etc/sss/sss.conf`:

```
[sss]
debug_level = 6
config_file_version = 2
services = nss, pam

[domain/TEST.ALT]
debug_level = 6
id_provider = ad
...

[nss]
debug_level = 6

[pam]
debug_level = 6
```

Чтобы загрузить новые параметры конфигурации необходимо перезапустить службу SSSD:

```
# systemctl restart sssd
```

10.6.12.1.4. Настройка уровня журналирования с помощью команды `sssctl`

Изменить уровень журналирования службы SSSD можно с помощью команды `sssctl debug-level <целое_число>`.

Где значение `<целое_число>` – число от 0 до 10. Уровни до 3 регистрируют крупные сбои, а уровни начиная с 8 и выше предоставляют большое количество подробных сообщений журнала. Уровень 6 является хорошей отправной точкой для отладки проблем.

Просмотр текущего уровня журналирования:

```
# sssctl debug-level
sssd                0x0070
nss                 0x0070
pam                 0x0070
pac                 0x0070
domain/TEST.ALT    0x0070
```

Установка нового уровня журналирования:

```
# sssctl debug-level 6
# sssctl debug-level
sssd                0x07f0
nss                 0x07f0
pam                 0x07f0
pac                 0x07f0
domain/TEST.ALT    0x07f0
```

Примечание. Уровень журналирования, заданный с помощью команды `sssctl debug-level` будет действовать до перезапуска службы `sssd`.

10.6.12.2. Настройки SSSD в ЦУС

Настройки SSSD в ЦУС представлены на рис. 504 и таблице 84.

Т а б л и ц а 84 – Настройки SSSD в ЦУС

Настройка	Опция в файле /etc/sss/sss.conf	Описание	Режимы
Правила применения групповых политик	ad_gpo_access_control	Определяет в каком режиме будет осуществляться контроль доступа в SSSD основанный на групповых политиках AD (GPO)	<p><code>enforced</code> (принудительный режим) – правила управления доступом в SSSD основанные на GPO выполняются, ведется логирование.</p> <p><code>permissived</code> (разрешающий режим) – правила управления доступом в SSSD основанные на GPO не выполняются, ведется только логирование. Такой режим необходим администратору, чтобы оценить, как срабатывают новые правила.</p> <p><code>disabled</code> (отключить) – правила управления доступом в SSSD основанные на GPO не логируются и не выполняются.</p> <p><code>default</code> (по умолчанию) – настройка контроля доступом в SSSD основанное на GPO сброшена на значение по умолчанию в пакете</p>

Продолжение таблицы 84

Настройка	Опция в файле /etc/sss/sss.conf	Описание	Режимы
Игнорировать, если групповые политики не читаются	ad_gpo_ignore_unreadable	Определяет будут ли проигнорированы правила управления доступом в SSSD основанные на групповых политиках, если недоступен какой-либо шаблон (GPT) объекта групповой политики (GPO)	enabled (включить) – игнорировать правила управления доступом через групповые политики, если шаблоны групповых политик не доступны для SSSD. disabled (отключить) – запретить доступ пользователям SSSD AD, которым назначены групповые политики, если шаблоны групповых политик не доступны. default (по умолчанию) – настройка игнорирования политик, при недоступности шаблонов групповых политик сброшена на значение по умолчанию
Кешировать учетные данные	cache-credentials	Определяет, будут ли учетные данные удаленных пользователей сохраняться в локальном кеше SSSD	enabled (включить) – сохранение в локальном кеше SSSD учетных данных пользователей включено. disabled (отключить) – сохранение в локальном кеше SSSD учетных данных пользователей отключено. default (по умолчанию) – настройка сохранения в локальном кеше SSSD учетных данных пользователей сброшена на значение по умолчанию
Привилегии запуска SSSD	control sss-drop-privileges	Позволяет сбросить права службы SSSD, чтобы избежать работы от имени суперпользователя (root)	privileged (привилегированный) – служба SSSD запущена от имени привилегированного суперпользователя (root). unprivileged (непривилегированный) – служба SSSD запущена от имени непривилегированного пользователя (_sss). default (по умолчанию) – режим привилегий службы SSSD задан по умолчанию в пакете

Продолжение таблицы 84

Настройка	Опция в файле /etc/sssds/sssds.conf	Описание	Режимы
Интервал обновления записей DNS	dyndns_refresh_interval	Определяет, как часто серверная часть должна выполнять периодическое обновление DNS в дополнение к автоматическому обновлению, выполняемому при подключении серверной части к сети. Этот параметр является применимым только в том случае, если для dyndns_update установлено значение true.	enabled (включить) – задать интервал. disabled (отключить) – установить значение по умолчанию (86400) unknown
TTL для клиентской записи DNS	dyndns_ttl	Срок жизни, применяемый к DNS-записи клиента при ее обновлении. Если dyndns_update имеет значение false, это не имеет никакого эффекта	enabled (включить) – задать TTL. disabled (отключить) – установить значение по умолчанию (3600) unknown
Обновлять IP-адрес машины в DNS	dyndns_update	Позволяет включить или отключить автоматическое обновление DNS-записей (защищенных с помощью GSS-TSIG) с IP-адресом клиента через SSSD	enabled (включить) – автоматическое обновление DNS-записи клиента через SSSD включено. disabled (отключить) – автоматическое обновление DNS-записи клиента через SSSD отключено. default (по умолчанию) – настройка автоматического обновления DNS-записи клиента через SSSD задана по умолчанию в пакете unknown
Обновлять PTR-запись машины в DNS-записей	dyndns_update_ptr	Определяет будет ли обновляться клиентская PTR-запись (защищенная с помощью GSS-TSIG) при обновлении DNS-записей клиента.	enabled (включить) – автоматическое обновление DNS-записи обратной зоны через SSSD включено. disabled (отключить) – автоматическое обновление DNS-записи обратной зоны через SSSD отключено.

Окончание таблицы 84

Настройка	Опция в файле /etc/sss/sss.conf	Описание	Режимы
		Применимо, только если <code>dyn dns_update</code> имеет значение <code>true</code> .	<code>default</code> (по умолчанию) – настройка автоматического обновления DNS-записи обратной зоны задана по умолчанию в пакете <code>unknown</code>

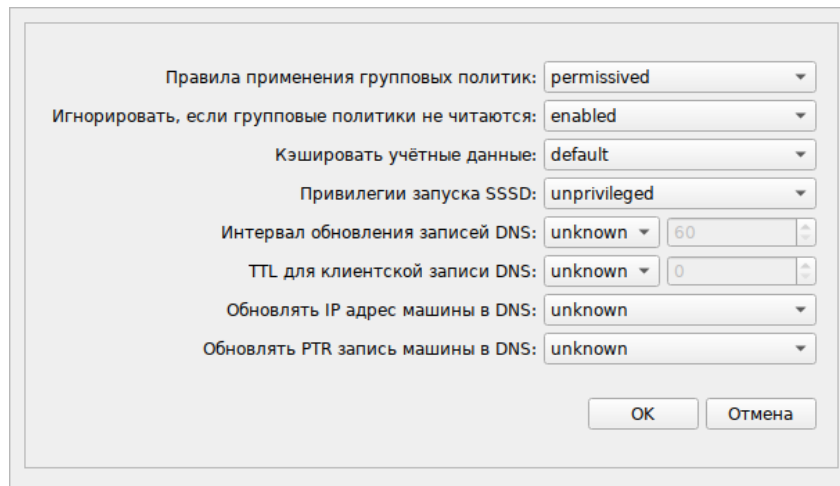


Рис. 504 – Настройки SSSD в ЦУС

10.6.12.3. Включение автономной аутентификации

По умолчанию SSSD не кэширует учетные данные пользователей. При обработке запросов на аутентификацию SSSD всегда обращается к поставщику идентификационных данных. Если провайдер недоступен, аутентификация пользователя не проходит.

Чтобы пользователи могли пройти аутентификацию, даже когда провайдер идентификации недоступен, можно включить кэширование учетных данных, установив параметр `cache_credentials` в значение `true` в файле `/etc/sss/sss.conf`.

Чтобы пользователи могли пройти аутентификацию, даже когда провайдер идентификации недоступен, можно включить кэширование учетных данных, установив параметр `cache_credentials` в значение `true` в разделе домена.

Дополнительно можно использовать параметр `offline_credentials_expiration` в разделе `[pam]`, чтобы установить ограничение

по времени (в днях), в течении которого пользователи смогут аутентифицироваться в автономном режиме с момента последнего успешного входа.

Пример настройки возможности автономной аутентификации пользователей в течение 5 дней с момента последнего успешного входа:

```
[pam]
offline_credentials_expiration = 5
[domain/TEST.ALT]
cache_credentials = true
```

Для включения/отключения кеширования учетных данных можно использовать `control sssd-cache-credentials`. Например:

- просмотреть текущее значение:

```
# control sssd-cache-credentials
default
```

- включить кеширование учетных данных:

```
# control sssd-cache-credentials enabled
```

- отключить кеширование учетных данных:

```
# control sssd-cache-credentials disabled
```

Данные настройки можно применить с помощью механизма групповых политик `control`. Подробнее см. п. 10.4.6.4.2.

10.6.13. Монтирование общих ресурсов samba

Рассматриваемые ниже способы позволяют подключать файловые ресурсы (file shares) для доменного пользователя без повторного ввода пароля (SSO, Single Sign-On).

10.6.13.1. Подключение с использованием gio

Примечание. Способ актуален для дистрибутивов, использующих gio.

Недостаток этого способа – необходимо открыть ресурс в файловом менеджере (Caja, Rmanfm). Однако можно открывать любые ресурсы на любых серверах, входящие в домен.

Процедура монтирования общих ресурсов с использованием gio:

- установить необходимые пакеты:

```
# apt-get install fuse-gvfs gvfs-backend-smb libgio
```

- включить пользователя в группу fuse:

```
# gpasswd -a <пользователь> fuse
```

- разрешить для всех доступ к fuse под root:

```
# control fusermount public
```

- войти под доменным пользователем;

- открыть ресурс в файловом менеджере (например, по адресу smb://server/sysvol). Ресурс смонтирован по пути /var/run/<uid_пользователя>/gvfs

или

```
/var/run/user/<uid_пользователя>/gvfs/smb-share:server=сервер, share=ресурс
```

- другой вариант (полезно для скриптов в автозапуске):

```
gio mount smb://server/sysvol/
```

Примечание. Если необходимо открывать что-то с ресурса в WINE, в winecfg следует добавить диск с путем /var/run/uid_пользователя/gvfs.

10.6.13.2. Подключение с использованием pam_mount

При подключении общих ресурсов с использованием pam_mount сетевой ресурс подключается с заданного сервера автоматически при каждом входе доменным пользователем.

Процедура монтирования общих ресурсов с использованием pam_mount:

- установить пакеты pam_mount и cifs-utils:

```
# apt-get install pam_mount cifs-utils
```

Примечание. Для того, чтобы файловые ресурсы, подключенные с помощью pam_mount, корректно отключались при завершении сеанса, следует установить пакет systemd-settings-enable-kill-user-processes и перезагрузить систему:

```
# apt-get install systemd-settings-enable-kill-user-processes
```

- прописать pam_mount в схему аутентификации по умолчанию. Для этого в конец файла /etc/pam.d/system-auth добавить строки:

```
session [success=1 default=ignore] pam_succeed_if.so service =
systemd-user quiet
session optional pam_mount.so disable_interactive
```

- установить правило монтирования ресурса в файле

/etc/security/pam_mount.conf.xml (перед тегом <cifsmount>):

```
<volume uid="10000-2000200000" fstype="cifs" server="dc1.test.alt"
path="sysvol" mountpoint="~/share"
options="sec=krb5i,cruid=%(USERUID),nounix,uid=%(USERUID),gid=%(USERGID)
),file_mode=0664,dir_mode=0775" />
```

где:

- а) uid="10000-2000200000" – диапазон присваиваемых для доменных пользователей UID (подходит для Winbind и для SSSD);
- б) server="dc1.test.alt" – имя сервера с ресурсом;
- в) path="sysvol" – имя файлового ресурса;
- г) mountpoint="~/share" – путь монтирования в домашней папке пользователя.

Опционально можно добавить:

sgrp="group_name" – имя группы, при членстве пользователя в которой, папка будет примонтирована.

Параметр sec=krb5i более безопасный, но требует больше вычислительных ресурсов. Вместо него можно указать sec=krb5.

⚠ В параметре server необходимо указывать настоящее имя сервера, а не имя домена.

⚠ По умолчанию для монтирования используется smb версии 1.0, если он отключен, то необходимо указать в параметрах версию 2 или 3:

```
<volume uid="10000-2000200000" fstype="cifs" server="dc1.test.alt"
path="sysvol" mountpoint="~/share"
options="sec=krb5i,vers=2.0,cruid=%(USERUID),nounix,uid=%(USERUID),gid
=%(USERGID),file_mode=0664,dir_mode=0775" />
```

⚠ Для проверки можно попробовать смонтировать ресурс в сессии:
 mount.cifs //dc1.test.alt/sysvol /mnt/ -o vers=2.0,user=Ivanov
 Доступность ресурса также можно проверить доступность ресурса с помощью smbclient, например: smbclient -L dc1.test.alt -U ivanov -m SMB2

10.6.13.3. Подключение с использованием Autofs

При этом способе заданный ресурс подключается автоматически при каждом обращении пользователя и отключается после определенного времени бездействия (определяется конфигурацией Autofs).

Принцип работы:

- задается каталог, в котором будет происходить подключение, например, `/mnt/auto/`;
- при необходимости обратиться к сетевой файловой системе, следует обратиться к каталогу с именем этой ФС в этом каталоге. Например, `/mnt/auto/server/share/`;
- при обращении будет произведена попытка смонтировать соответствующий сетевой ресурс;
- при отсутствии обращения, после заданного таймаута, сетевой ресурс будет отмонтирован;
- AutoFS использует для конфигурирования шаблоны `/etc/auto*`. Основной шаблон называется `auto.master`, он может указывать на один или несколько других шаблонов для конкретных типов носителей. Пример содержимого файла `/etc/auto.master`:

```
# Format of this file:
# mountpoint map options
# For details of the format look at autofs(8).
/mnt/auto          /etc/auto.tab    -t 5
/mnt/net           /etc/auto.avahi  -t 120
```

Первое значение в каждой строке определяет базовый каталог, в который носители будут монтироваться, второе значение – файл конфигурации или скрипт, который будет использован.

Примечание. Параметр `-t` (`--timeout`) устанавливает количество секунд, после истечения которых каталоги будут размонтированы. Значение 0 отключает таймаут. Значения параметра по умолчанию задаются в файле `/etc/autofs.conf`.

Базовый каталог будет создан, если он не существует. Он станет точкой монтирования, отображающей в себе динамически подключаемые носители, что означает, что существующее содержимое базового каталога будет недоступно пока `autofs` работает.

Пример настройки автоматического подключения сетевых файловых ресурсов Windows (Samba) при входе пользователя:

1) добавить в `/etc/auto.master` строку:

```
/mnt/samba /etc/auto.smb -t 120
```

где:

- `/mnt/samba` – каталог в котором будут подключаться сетевые файловые системы;
- `/etc/auto.smb` – стандартный скрипт, входящий в состав пакета `autofs`;
- `120` – таймаут подключения при отсутствии обращения;

2) включить и запустить сервис `autofs`:

```
# systemctl enable --now autofs
```

3) для автоматического подключения ресурсов достаточно обратиться к ресурсу по имени хоста в диспетчере файлов (рис. 505) или в командной строке, например:

```
$ ls /mnt/samba/<имя_хоста>
```

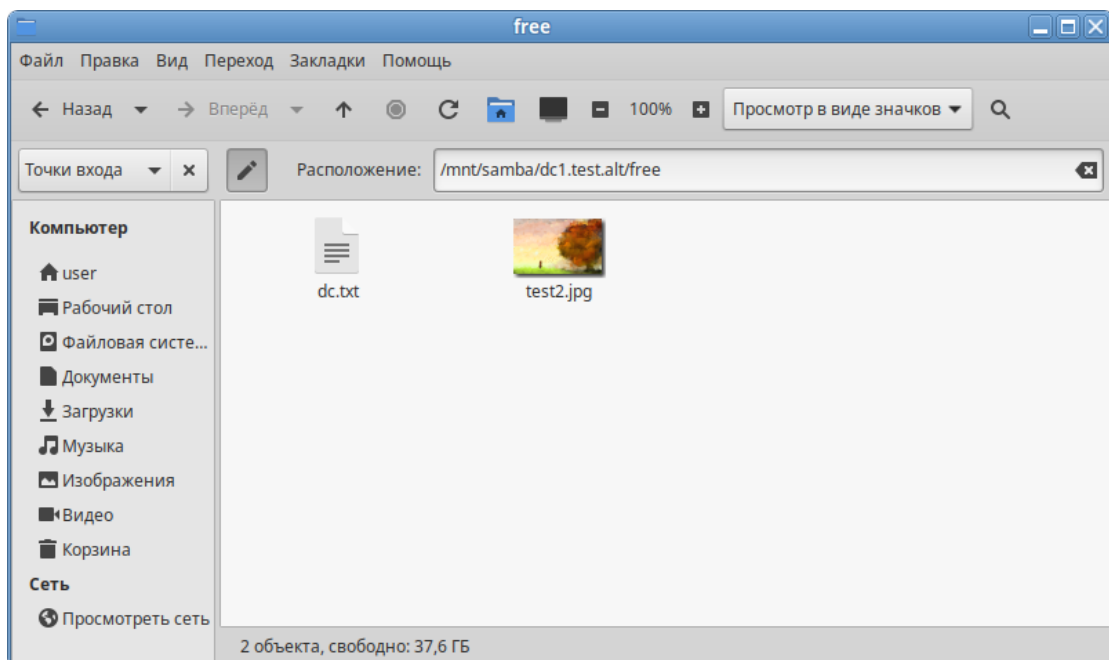


Рис. 505 – Диспетчер файлов

10.6.14. Журналирование в Samba

Сервер Samba позволяет гибко настраивать журналирование для выявления возможных проблем в работе службы каталогов, а также мониторинга событий, связанных с аутентификацией, авторизацией и внесением изменений в базу данных службы.

Файлы журналов службы Samba находятся в каталоге `/var/log/samba/`.

10.6.14.1. Настройка бэкендов

На сервере Samba одновременно может вестись журналирование с использованием нескольких бэкендов. При этом для каждого из них может быть задан свой уровень журналирования.

Установить бэкенд для Samba можно, используя параметр `logging`, который задается в разделе `[global]` файла `smb.conf`. Параметр представляет собой список бэкендов, разделенных пробелом, в формате:

```
logging = backend1[:option] [@loglevel] backendN[:option] [@loglevel]
```

где:

- `backend` – один из доступных бэкендов;
- `syslog` – запись в системный журнал;
- `file` – запись в файл, указанный в параметре `log file`, либо в стандартные файлы журналов Samba в каталоге `/var/log/samba/`;
- `systemd` – запись в журнал `systemd`;
- `ltnng` – трассировка с использованием инструментов фреймворка LTTng;
- `gpfs` – аудит файлов в кластерной файловой системе GPFS;
- `ringbuf` – запись в кольцевой буфер (`ring buffer`). Для задания размера буфера поддерживается необязательный аргумент `size` в формате:
`logging = ringbuf:size=NBYTES` (значение по умолчанию – 1 Мбайт).

Данный вариант логирования может быть полезен при анализе ошибок, которые связаны с временными эффектами и не могут быть воспроизведены при записи логов в файлы с указанием высоких уровней отладки;

- `[:option]` – дополнительные опции, специфичные для указанного бэкенда;

- [`@loglevel`] – уровень журналирования. Если для бэкенда данный параметр не установлен, в бэкенд отправляются все сообщения. Параметр `log level` определяет общие уровни журнала, а указанные здесь уровни определяют, что отправляется на отдельные бэкенды.

Примечание. Если параметр `logging` задан, то его значение переопределяет значения параметров `syslog` и `syslog only`.

По умолчанию параметр `logging` не задан.

Пример задания параметра `logging`:

```
logging = syslog@1 file
```

10.6.14.2. Настройка файлов журнала

Параметр `log file` в разделе `[global]` файла `smb.conf` позволяет переопределить файл журнала Samba.

Параметр `log file` использует стандартные подстановки, что позволят иметь отдельные файлы журналов для различных сущностей и объектов, обслуживаемых Samba.

Примеры подстановок:

- `%m` – NetBIOS-имя клиентской машины. Этот параметр недоступен, когда Samba прослушивает порт 445, поскольку клиенты больше не отправляют эту информацию. Для возможности использования этой подстановки следует установить в разделе `[global]` `smbports = 139`;
- `%M` – интернет-имя клиентской машины;
- `%I` – IP-адрес клиентской машины;
- `%i` – локальный IP-адрес, с которым установил соединение клиент;
- `%T` – текущие дата и время;
- `%U` – имя пользователя сессии.

Примечание. Получить полный список подстановок можно в разделе `VARIABLE SUBSTITUTIONS` на справочной странице `smb.conf(5)` (`man smb.conf`).

Например, для создания отдельного файла журнала для каждого подключенного узла с именем в формате `<NetBIOS_name>.log` в каталоге `/var/log/samba/` следует задать параметр следующим образом:

```
log file = /var/log/samba/%m.log
```

Параметр `max log size` в разделе `[global]` файла `smb.conf` определяет максимальный размер файла журнала. Значение параметра задается в килобайтах. Samba периодически проверяет размер файла журнала и, если он превышен, переименовывает файл, добавляя расширение `.old` и создает новый файл.

Указание значения `0` для параметра `max log size` означает отсутствие ограничений. Значение по умолчанию `5000`.

Пример уставки ограничения максимального размера файла журнала в 1 Мбайт:

```
max log size = 1000
```

Примечание. В процессе ротации Samba перезаписывает архивированный ранее файл.

10.6.14.3. Уровни журналирования

Установить уровень журналирования для Samba можно, используя параметр `log level` в разделе `[global]` файла `smb.conf`. Для разных классов отладки можно указывать разные уровни журналирования и отдельные файлы журналов.

Уровень журналирования задается в виде целого числа в диапазоне от 0 до 10, где 0 соответствует отключению вывода отладочной информации, а 10 – обеспечивает вывод полной отладочной информации об ошибках и проблемах, которые могут возникать в процессе работы Samba. Оптимальным для получения отладочной информации является уровень 3. Уровни выше 3 предназначены преимущественно для выявления внутренних ошибок Samba. Их использование может привести к существенному снижению производительности сервера.

Доступны следующие классы отладки:

- all;
- tdb;
- printdrivers;

- lanman;
- smb;
- rpc_parse;
- rpc_srv;
- rpc_cli;
- passdb;
- sam;
- auth;
- winbind;
- vfs;
- idmap;
- quota;
- acls;
- locking;
- msdfs;
- dmapi;
- registry;
- scavenger;
- dns;
- ldb;
- tevent;
- auth_audit;
- auth_json_audit;
- kerberos;
- drs_repl;
- smb2;
- smb2_credits;
- dsdb_audit;
- dsdb_json_audit;
- dsdb_password_audit;

- dsdb_password_json_audit;
- dsdb_transaction_audit;
- dsdb_transaction_json_audit;
- dsdb_group_audit;
- dsdb_group_json_audit.

Некоторые модули при первом использовании регистрируют динамические классы отладки, например:

- catia;
- dfs_samba4;
- extd_audit;
- fileid;
- fruit;
- full_audit;
- media_harmony;
- preopen;
- recycle;
- shadow_copy;
- unityed_media;
- virusfilter.

Чтобы настроить ведение журналов для определенных классов так, чтобы они входили в другой файл, а не в файл журнала, можно добавить @PATH к классу.

Примечание. Получить дополнительную информацию и список классов отладки можно на справочной странице `smb.conf(5)` (`man smb.conf`).

10.6.14.3.1. Установка уровня журналирования в файле `smb.conf`

Примеры использования параметра `log level` для настройки уровня журналирования:

- установить уровень журнала для всех классов отладки на 3:
`log level = 3`
- установить общий уровень журнала на 3 и для классов `passdb` и `auth` на 5:
`log level = 3 passdb:5 auth:5`

- установить уровень журнала для класса winbind на 1 и писать логи в файл /var/log/winbind.log:

```
log level = 3 winbind:1@/var/log/winbind.log
```

10.6.14.3.2. Установка уровня журналирования при выполнении команд

Команды Samba используют уровень журналирования, установленный в параметре `log level` в файле `smb.conf`. Это значение можно переопределить, используя следующую опцию для всех команд Samba:

```
-d DEBUGLEVEL, --debuglevel=DEBUGLEVEL
```

Например:

```
$ net usershare add Share2 /tmp/share2 -d 5  
# samba-tool group add testgroup12 -d dsdb_audit:10
```

10.6.14.4. Настройка ведения журнала аудита

Samba поддерживает ведение журнала событий аутентификации и авторизации, а также ведение журнала изменений базы данных контроллера домена. Это позволяет регистрировать, например, неудачные запросы аутентификации или сбросы пароля.

Ведение журнала аудита является локальной настройкой, эту функцию необходимо включить на каждом сервере Samba. События регистрируются на сервере Samba, на котором произошло событие. Чтобы хранить все журналы на централизованном сервере, следует настроить централизованный сервер системных журналов, настроить Samba для регистрации в `syslog` и настроить `syslog` для отправки журналов на централизованный сервер.

Для мониторинга файлов журналов и выполнения определенных действий на основе результатов их анализа могут использоваться дополнительные утилиты.

Примечание. Samba генерирует некоторые журналы на узле в конфигурации файлового сервера и члена домена, но полная поддержка доступна только на контроллере домена.

Журнал аудита Samba поддерживает стандартный формат и формат JSON. Можно включить каждый формат по отдельности или оба вместе, используя разные классы отладки журнала (например, `auth_audit` для ведения записи в стандартном формате и `auth_json_audit` для ведения записи в формате JSON).

В зависимости от уровня журналирования Samba регистрирует разные события. Чтобы ограничить количество записей в журнале, можно увеличить уровень журналирования только для классов отладки, связанных с аудитом.

10.6.14.4.1. Регистрация событий аутентификации и авторизации

Samba поддерживает протоколирование успешных событий и неуспешных событий аутентификации, а также успешных событий авторизации.

Примечания:

1. Аутентификация происходит, когда Samba проверяет комбинацию имени пользователя и пароля.
2. Авторизация происходит при запуске сеанса.

Следующие примеры показывают, в каких случаях Samba регистрирует события аутентификации и авторизации:

- 1) при входе пользователя в домен центр распространения ключей Kerberos (KDC), работающий на контроллере домена, фиксирует событие аутентификации. Если в домене работают несколько контроллеров, запрос аутентификации регистрируется только на контроллере, который обслуживает данный запрос;
- 2) при подключении к общему ресурсу на участнике домена:
 - участник домена регистрирует событие авторизации;
 - при использовании аутентификации Kerberos центр распространения ключей (KDC) на контроллере домена Samba фиксирует событие аутентификации.

В случае использования аутентификации Kerberos за нее отвечает KDC. Поэтому Samba на участнике домена не может регистрировать такое событие аутентификации;

- 3) при использовании аутентификации через NT LAN Manager (NTLM) участник домена регистрирует событие аутентификации.

Примечание. При использовании NTLM всегда регистрируется пара событий – событие аутентификации и событие авторизации. Однако при использовании Kerberos регистрируется только одно событие на контроллере домена в момент выдачи билета TGT (Ticket Granting Ticket). После этого каждый раз при получении доступа к какой-либо службе регистрируется событие авторизации.

Для регистрации событий аутентификации и авторизации используются следующие классы отладки:

- `auth_audit` – стандартный формат журнала;
- `auth_json_audit` – формат JSON.

Для классов `auth_audit` и `auth_audit_json` доступны следующие уровни журналирования (каждый последующий уровень включает все предшествующие ему):

- 2 – неуспешные события аутентификации;
- 3 – успешные события аутентификации;
- 4 – успешные события авторизации;
- 5 – успешные анонимные события аутентификации и авторизации.

Пример включения ведения журнала аудита аутентификации (установить уровень журнала по умолчанию – 1, включить регистрацию неудачных и успешных запросов аутентификации – 3):

1) установить в секции `[global]` файла `/etc/samba/smb.conf`:

```
log_level = 1 auth_audit:3 auth_json_audit:3
```

2) перезапустить службу Samba.

Пример записей о неуспешной и успешной попытках аутентификации пользователя с использованием стандартного формата журнала:

```
[2024/05/29 14:32:52.509247, 2]
../../../../auth/auth_log.c:858(log_authentication_event_human_readable)
Auth: [Kerberos KDC,ENC-TS Pre-authentication] user
[(null)]\[ivanov\@TEST@TEST.ALT] at [Wed, 29 May 2024 14:32:52.509236 EET]
with [aes256-cts-hmac-sha1-96] status [NT_STATUS_WRONG_PASSWORD] workstation
[(null)] remote host [ipv4:192.168.0.135:51947] mapped to [TEST]\[ivanov].
local host [NULL]
```

```
[2024/05/29 14:39:06.426556, 3]
../../../../auth/auth_log.c:858(log_authentication_event_human_readable)
Auth: [Kerberos KDC,ENC-TS Pre-authentication] user
[(null)]\[ivanov\@TEST@TEST.ALT] at [Wed, 29 May 2024 14:39:06.426540 EET]
with [aes256-cts-hmac-sha1-96] status [NT_STATUS_OK] workstation [(null)]
remote host [ipv4:192.168.0.135:55134] became [TEST]\[ivanov] [S-1-5-21-
578923263-1107570656-1287136478-1103]. local host [NULL]
```

Пример записей о неуспешной и успешной попытках аутентификации пользователя с использованием формата JSON:

```
{
  "timestamp": "2024-05-29T14:32:52.509393+0200",
  "type": "Authentication",
  "Authentication": {
    "version": {
      "major": 1,
      "minor": 3
    },
    "eventId": 4625,
    "logonId": "5bd240f7cc4delb5",
    "logonType": 3,
    "status": "NT_STATUS_WRONG_PASSWORD",
    "localAddress": null,
    "remoteAddress": "ipv4:192.168.0.135:51947",
    "serviceDescription": "Kerberos KDC",
    "authDescription": "ENC-TS Pre-authentication",
    "clientDomain": null,
    "clientAccount": "ivanov\\@TEST@TEST.ALT",
    "workstation": null,
    "becameAccount": "ivanov",
    "becameDomain": "TEST",
    "becameSid": "S-1-5-21-578923263-1107570656-1287136478-1103",
    "mappedAccount": "ivanov",
    "mappedDomain": "TEST",
    "netlogonComputer": null,
    "netlogonTrustAccount": null,
    "netlogonNegotiateFlags": "0x00000000",
    "netlogonSecureChannelType": 0,
    "netlogonTrustAccountSid": null,
    "passwordType": "aes256-cts-hmac-sha1-96",
    "clientPolicyAccessCheck": null,
    "serverPolicyAccessCheck": null,
    "duration": 3129
  }
}
```

```
{
  "timestamp": "2024-05-29T14:39:06.426725+0200",
  "type": "Authentication",
  "Authentication": {
    "version": {
      "major": 1,
      "minor": 3
    },
    "eventId": 4624,
    "logonId": "11424f6685e647f9",
    "logonType": 3,
    "status": "NT_STATUS_OK",
    "localAddress": null,
    "remoteAddress": "ipv4:192.168.0.135:55134",
    "serviceDescription": "Kerberos KDC",
    "authDescription": "ENC-TS Pre-authentication",
    "clientDomain": null,
    "clientAccount": "ivanov\\@TEST@TEST.ALT",
    "workstation": null,
    "becameAccount": "ivanov",
    "becameDomain": "TEST",
    "becameSid": "S-1-5-21-578923263-1107570656-1287136478-1103",
    "mappedAccount": "ivanov",
    "mappedDomain": "TEST",
    "netlogonComputer": null,
    "netlogonTrustAccount": null,
    "netlogonNegotiateFlags": "0x00000000",
    "netlogonSecureChannelType": 0,
    "netlogonTrustAccountSid": null,
    "passwordType": "aes256-cts-hmac-sha1-96",
    "clientPolicyAccessCheck": null,
    "serverPolicyAccessCheck": null,
    "duration": 5421
  }
}
```

10.6.14.4.2. Регистрация изменений в базе данных

Для регистрации изменений в базе данных контроллера домена Samba (sam.ldb) используются следующие классы отладки:

- dsdb_audit – регистрация в стандартном формате;
- dsdb_json_audit – регистрация в формате JSON.

Для регистрации изменений в составе групп используются следующие классы отладки:

- dsdb_group_audit – регистрация в стандартном формате;
- dsdb_group_json_audit – регистрация в формате JSON.

Для классов dsdb_audit, dsdb_json_audit, dsdb_group_audit и dsdb_group_json_audit доступны следующие уровни логирования:

- 5 – внесение изменений в базу данных;
- 5 – регистрация изменений, полученных через механизм репликации с другого контроллера домена.

События изменения и сброса паролей регистрируются в рамках следующих классов отладки:

- `dsdb_password_audit` – регистрация в стандартном формате;
- `dsdb_password_json_audit` – регистрация в формате JSON.

Примечание. Каждое изменение пароля также регистрируется как событие аутентификации через классы отладки `auth_audit` и `auth_audit_json`.

Для классов `dsdb_password_audit` и `dsdb_password_json_audit` доступны следующие уровни логирования:

- 5 – успешные события изменения и сброса пароля.

Для регистрации не успешных транзакций, завершающихся откатом, и событий подготовки фиксации данных (`prepare commit`) используются следующие классы отладки:

- `dsdb_transaction_audit` – регистрация в стандартном формате;
- `dsdb_transaction_json_audit` – регистрация в формате JSON.

Для классов `dsdb_transaction_audit` и `dsdb_transaction_json` доступны следующие уровни логирования:

- 5 – неуспешная транзакция (откат);
- 10 – успешная транзакция (фиксация).

В Samba возможны откаты транзакций. Они редко отражают что-либо помимо неуспешного завершения отдельной операции (например, в результате попытки создания записи, которая конфликтует с существующими). Записи о транзакции формируются и фиксируются в системных журналах до ее завершения. Такое журналирование информации о транзакциях позволяет выявлять операции с паролями и операции по внесению изменения в `sam.ldb`, которые закончились откатом и фактически не были выполнены.

Пример включения ведения журнала аудита базы данных DC (установить уровень журнала по умолчанию – 1, включить ведение журнала изменений базы данных в формате JSON):

1) установить в секции `[global]` файла `smb.conf`:

```
log_level = 1 dsdb_json_audit:5 dsdb_password_json_audit:5
dsdb_group_json_audit:5 dsdb_transaction_json_audit:5
```

2) перезапустить службу Samba.

10.6.14.5. Интерпретация журналов аудита JSON

Если включено ведение журнала аудита в формате JSON, сведения о различных событиях регистрируются в формате JSON. Каждое событие описывается определенным набором атрибутов, соответствующим его типу. Внешний слой атрибутов состоит из трех элементов: метки времени, типа события и объекта данных (в примере добавлены переносы на новую строку и отступы; реальные записи всегда форматируются в виде одной строки):

```
{
  "timestamp": 2023-04-13T11:48:45.902942+0200,
  "type": одно из значений "Authentication", "Authorization", "dsdbChange",
         "dsdbTransaction", "passwordChange", "replicatedUpdate",
         "groupChange",
  type: { data }
}
```

Примечание. Некоторые атрибуты могут присутствовать в журнале, даже если они неприменимы. Например, если NETLOGON не используется (согласно serviceDescription), для параметра netlogonComputer будет установлено значение «null», для параметра netlogonNegotiateFlags будет установлено значение «0x00000000», а другие поля сетевого входа будут иметь аналогичные пустые значения.

10.6.14.5.1. Общие атрибуты

В таблице 85 приведено описание атрибутов, которые присутствуют при регистрации любого события.

Т а б л и ц а 85 – Общие атрибуты

Атрибут	Значение
version	Номер версии формата JSON. Состоит из двух частей: <ul style="list-style-type: none"> - «major» – увеличивается, если поля меняют значение; - «minor» – увеличивается, если добавляется новое поле. Изменения в перечне возможных значений обычно не приводят к изменению версии. Это распространяется на все данные, предоставляемые клиентами. Также это относится, например, к атрибуту passwordType, набор поддерживаемых форматов которого может меняться с течением времени без изменения версии в JSON

10.6.14.5.2. Атрибуты событий аутентификации (Authentication)

В таблице 86 приведен набор атрибутов, который используется для регистрации событий аутентификации.

Т а б л и ц а 86 – Аутентификация

Атрибут	Значение
authDescription	Тип аутентификации: <ul style="list-style-type: none"> - «simple bind/TLS», «simple bind» – простая привязка LDAP с каналом TLS или без него; - «guest» – анонимный запрос SMB1; - «bare-NTLM» – запрос SMB, использующий протокол NT1; - «plaintext» – запрос SMB, в виде обычного текста; - «interactive» – аналог физического входа на конкретной рабочей станции; - «network» – проверка подлинности запроса/ответа по сети; - «Unknown Auth Description», «Unknown Pre-authentication» – события KDC; - «ServerAuthenticate» – запрос/ответ компьютера при входе с использованием NETLOGON; - «LDAP Modify» – смена пароля (не событие аутентификации, но регистрируется здесь, чтобы администратор не пропустил его)
becameAccount	Имя учетной записи, под которой выполнен вход (может отличаться от учетной записи, предоставленной клиентом)
becameDomain	Имя домена, в который произведен вход
becameSid	Идентификатор безопасности (SID) аутентифицированной учетной записи
clientAccount	Имя учетной записи, предоставленное клиентом
clientDomain	Имя домена, предоставленное клиентом
duration	Время (в микросекундах), в течение которого выполнялась аутентификация
eventId	Идентификатор события Windows, указывающий в общих чертах, что произошло
localAddress	Адрес сервера и используемый порт
logonId	Случайный 64-битный идентификатор, помогающий отслеживать события входа в систему на разных этапах
logonType	Тип входа в Windows, для Samba один из: <ul style="list-style-type: none"> - 2 – интерактивный, то есть вход выполняется на текущем компьютере; - 3 – сетевой, то есть вход выполняется по сети; - 8 – NetworkCleartext с использованием нехешированных паролей, то есть вход выполняется по сети, при этом пароль передается в пакет подтверждения подлинности в нехешированной форме (NetworkCleartext)
mappedAccount	Имя учетной записи клиента, преобразованное в имя учетной записи «Альт Домен»
mappedDomain	Имя домена клиента, преобразованное в доменное имя «Альт Домен»
netlogonComputer	Имя компьютера, заявленное при аутентификации через NETLOGON RPC
netlogonNegotiateFlags	Флаги NETLOGON, согласуемые в процессе взаимодействия клиента и сервера
netlogonSecureChannelType	Тип безопасного канала, используемого для входа по протоколу NETLOGON

Продолжение таблицы 86

Атрибут	Значение
netlogonTrustAccount	Учетная запись, используемая для аутентификации по протоколу NETLOGON
netlogonTrustAccountSid	Идентификатор безопасности (SID) учетной записи, используемый для аутентификации по протоколу NETLOGON
passwordType	Алгоритм/протокол пароля (например, «HMAC-SHA256», «NTLMv2», «arcfour-hmac-md5»)
remoteAddress	Заявленный адрес (и порт) удаленного клиента
serviceDescription	Тип службы (например, LDAP, SMB2, NETLOGON, Kerberos KDC)
status	<p>Сообщение NT STATUS. Для успешной аутентификации это будет «NT_STATUS_OK». Неудачная аутентификация может иметь здесь «NT_STATUS_OK», если аутентификация не удалась после регистрации этого сообщения, но обычно имеет код ошибки.</p> <p>Некоторые типы сообщений при неудачной аутентификации:</p> <ul style="list-style-type: none"> - NT_STATUS_ACCESS_DENIED – доступ запрещен по неустановленным причинам (наиболее вероятная причина – неправильные учетные данные); - NT_STATUS_WRONG_PASSWORD – неверный пароль; - NT_STATUS_NO_SUCH_USER – пользователь не существует; - NT_STATUS_NO_SUCH_DOMAIN – домен не существует; - NT_STATUS_ACCOUNT_RESTRICTION – учетная запись защищена или иным образом ограничена; - NT_STATUS_DOWNGRADE_DETECTED – клиент, возможно, предпринимает какие-либо действия для использования некорректных способов аутентификации; - NT_STATUS_INVALID_SERVER_STATE – сервер, возможно, используется не по назначению; - NT_STATUS_INVALID_INFO_CLASS – сервер, возможно, используется не по назначению; - NT_STATUS_INVALID_PARAMETER – клиент получил некорректные данные; - NT_STATUS_NETWORK_CREDENTIAL_CONFLICT – в процессе входа произошли изменения (возможно, имеет место гонка в рамках изменения учетных данных, либо при согласовании данных шифрования возникла ошибка); - NT_STATUS_NOT_IMPLEMENTED – тип аутентификации не реализован в Samba; - NT_STATUS_NOT_SUPPORTED – тип аутентификации, либо способ его использования со стороны клиента не поддерживается Samba; - NT_STATUS_INVALID_SYSTEM_SERVICE – выбранная служба аутентификации недоступна; - NT_STATUS_INTERNAL_ERROR – сервер не может завершить выполнение аутентификации по причине внутренней ошибки; - NT_STATUS_NO_MEMORY – сервер не может завершить аутентификацию по причине нехватки памяти

Окончание таблицы 86

Атрибут	Значение
version	См. описание в таблице 85 Текущая версия: { "major": 1, "minor": 3 }
workstation	Заявленное имя клиентской рабочей станции

Пример записи об успешной попытке аутентификации:

```
{ "timestamp": "2024-05-29T14:39:06.426725+0200", "type": "Authentication",
  "Authentication": { "version": { "major": 1, "minor": 3 }, "eventId": 4624,
  "logonId": "11424f6685e647f9", "logonType": 3, "status": "NT_STATUS_OK",
  "localAddress": null, "remoteAddress": "ipv4:192.168.0.135:55134",
  "serviceDescription": "Kerberos KDC", "authDescription": "ENC-TS Pre-
  authentication", "clientDomain": null, "clientAccount":
  "ivanov\\@TEST@TEST.ALT", "workstation": null, "becameAccount": "ivanov",
  "becameDomain": "TEST", "becameSid": "S-1-5-21-578923263-1107570656-
  1287136478-1103", "mappedAccount": "ivanov", "mappedDomain": "TEST",
  "netlogonComputer": null, "netlogonTrustAccount": null,
  "netlogonNegotiateFlags": "0x00000000", "netlogonSecureChannelType": 0,
  "netlogonTrustAccountSid": null, "passwordType": "aes256-cts-hmac-sha1-96",
  "clientPolicyAccessCheck": null, "serverPolicyAccessCheck": null, "duration":
  5421}}
```

10.6.14.5.3. Атрибуты событий авторизации (Authorization)

В таблице 87 приведен набор атрибутов, который используется для регистрации успешных событий авторизации.

Т а б л и ц а 87 – Успешные события авторизации

Атрибут	Значение
account	Имя авторизуемой учетной записи
accountFlags	Битовое поле атрибутов учетной записи
authType	Строка, описывающая тип авторизации (например, «krb5», «NTLMSSP», «simple bind»)
domain	Имя домена
localAddress	Адрес сервера и используемый порт
logonServer	Сервер, на котором выполнена аутентификация
remoteAddress	Видимый адрес клиента
serviceDescription	Тип службы (например, «LDAP», «SMB2», «DCE/RPC»)
sessionId	Уникальный идентификатор сессии (GUID)
sid	Идентификатор безопасности (SID) авторизуемой учетной записи
transportProtection	Тип защиты канала (например, «SMB», «TLS», «SEAL», «NONE»)
version	См. описание в таблице 85 Текущая версия: { "major": 1, "minor": 2 }

Пример записи об успешной попытке авторизации:

```
{ "timestamp": "2024-05-29T15:32:39.282334+0200", "type": "Authorization",
  "Authorization": { "version": { "major": 1, "minor": 2 }, "localAddress":
    "ipv4:127.0.0.1:389", "remoteAddress": "ipv4:127.0.0.1:43350",
    "serviceDescription": "LDAP", "authType": "simple bind", "domain": "NT
    AUTHORITY", "account": "ANONYMOUS LOGON", "sid": "S-1-5-7", "sessionId":
    "5accdd86-4c6e-4bd2-8ab1-7e95f641ecf2", "logonServer": "DC1",
    "transportProtection": "NONE", "accountFlags": "0x00000010",
    "clientPolicyAccessCheck": null, "serverPolicyAccessCheck": null}}
```

```
{ "timestamp": "2024-05-29T15:37:54.370408+0200", "type": "KDC Authorization",
  "KDC Authorization": { "version": { "major": 1, "minor": 0 }, "status":
    "NT_STATUS_OK", "localAddress": null, "remoteAddress":
    "ipv6:fd47:d11e:43c1:0:a00:27ff:fe9d:4de0:38254", "serviceDescription":
    "cifs/dc1.local@TEST.ALT", "authType": "TGS-REQ with Ticket-Granting Ticket",
    "domain": "TEST", "account": "ivanov", "sid": "S-1-5-21-578923263-1107570656-
    1287136478-1103", "logonServer": "DC1", "authTime": "2024-05-
    29T15:37:54.366830+0200", "serverPolicyAccessCheck": null}}
```

```
{ "timestamp": "2024-05-29T14:39:06.431833+0200", "type": "KDC Authorization",
  "KDC Authorization": { "version": { "major": 1, "minor": 0 }, "status":
    "NT_STATUS_OK", "localAddress": null, "remoteAddress":
    "ipv4:192.168.0.135:55142", "serviceDescription": "WORK135$@TEST.ALT",
    "authType": "TGS-REQ with Ticket-Granting Ticket", "domain": "TEST",
    "account": "ivanov", "sid": "S-1-5-21-578923263-1107570656-1287136478-1103",
    "logonServer": "DC1", "authTime": "2024-05-29T14:39:06.429012+0200",
    "serverPolicyAccessCheck": null}}
```

10.6.14.5.4. Атрибуты событий, связанных с изменениями в базе данных (dsdbChange)

События dsdbChange регистрируются, когда клиент вызывает существенные изменения в базе данных (известной как DSDB внутри Samba). Некоторые конкретные изменения, а именно изменения пароля, группы и изменения репликации, регистрируются отдельно как события passwordChange, groupChange и replicationUpdate.

В таблице 88 приведен набор атрибутов, который используется для регистрации событий, связанных с внесением значимых изменений в базу данных службы каталогов.

Т а б л и ц а 88 – События dsdbChange

Атрибут	Значение
attribute	Список изменяемых атрибутов
dn	Уникальное составное имя (DN) изменяемого объекта
operation	<p>Операция LDAP, соответствующая выполняемому действию по изменению данных:</p> <ul style="list-style-type: none"> - «Modify» - «Add» - «Delete»
performedAsSystem	<p>Признак системного или пользовательского действия:</p> <ul style="list-style-type: none"> - «true» – действие выполняется Samba с использованием системной учетной записи; - «false» – действие выполняется от имени пользователя
remoteAddress	Удаленный адрес пользователя, инициировавшего операцию
sessionId	Уникальный идентификатор (GUID) сессии аутентификации
status	<p>Строка, указывающая на успешное завершение действия или невозможность его выполнения по той или иной причине; выводимая информация соответствует кодам ответа LDAP, которые фиксируются в атрибуте statusCode.</p> <p>Примеры значений:</p> <ul style="list-style-type: none"> - «Success» - «Operations error» - «Protocol error» - «Time limit exceeded» - «Size limit exceeded» - «Unsupported critical extension» - «No such attribute» - «Undefined attribute type» - «Constraint violation» - «Attribute or value exists» - «Invalid attribute syntax» - «No such object» - «Alias problem» - «Invalid DN syntax» - «Insufficient access rights» - «Unwilling to perform» - «Naming violation» - «Object class violation» - «Not allowed on non-leaf» - «Not allowed on RDN» - «Entry already exists»

Окончание таблицы 88

Атрибут	Значение
Числовой код, соответствующий статусу в атрибуте status	В общем случае в качестве значения атрибута приводится код ответа LDAP в соответствии с RFC 4511
Числовой код, соответствующий статусу в атрибуте status	В общем случае в качестве значения атрибута приводится код ответа LDAP в соответствии с RFC 4511
transactionId	Уникальный идентификатор (GUID) транзакции, в рамках которой выполняется операция (если операция является частью транзакции)
userSid	Идентификатор безопасности (SID) пользователя, инициировавшего операцию
version	См. описание в таблице 85 Текущая версия: {"major": 1, "minor": 0}

Значение поля `attributes` может рассматриваться в качестве аналога описания изменения в формате LDIF.

Например, следующий JSON:

```
"dsdbChange": {
  "operation": "Modify",
  "dn": "@SAMBA_DSDB",
  "attributes": {
    "backupDate": {"actions": [
      {"action": "add",
        "values": [
          {"value": "2024-05-29T15:20:19.635275"}
        ]
      }
    ]
  }
}}
```

описывает изменение, выполненное этим LDIF:

```
dn: @SAMBA_DSDB
changetype: modify
add: backupDate
backupDate: 2024-05-29T15:20:19.635275
```

Для секретных атрибутов вместо каких-либо значений указывается тег `redacted: true`.

Если значение очень длинное (> 1024 байт), оно будет усечено с добавлением «...» и флагом `truncated: true`, например:

```
"values": [
  {truncated: true,
   "value": "It was the best of times, it was the worst of times, it was the
age..."
  }
]
```

Пример записи о внесении изменений в базу данных:

```
{
  "timestamp": "2024-05-29T09:52:14.813697+0200",
  "type": "dsdbChange",
  "dsdbChange": {
    "version": {
      "major": 1,
      "minor": 0
    },
    "statusCode": 0,
    "status": "Success",
    "operation": "Modify",
    "remoteAddress": "ipv6:fd47:d11e:43c1:0:a00:27ff:fe9d:4de0:38500",
    "performedAsSystem": false,
    "userSid": "S-1-5-21-578923263-1107570656-1287136478-500",
    "dn": "CN=Марков Кирилл,CN=Users,DC=test,DC=alt",
    "transactionId": "ce759566-8bf9-46ce-95a1-0d632232a220",
    "sessionId": "48c760f6-6cdc-4fba-b16d-1689f2cfad33",
    "attributes": {
      "unicodePwd": {
        "actions": [
          {
            "action": "replace",
            "redacted": true
          }
        ]
      }
    }
  }
}
```

10.6.14.5.5. Атрибуты событий, связанных с транзакциями (dsdbTransaction)

Транзакция связывает вместе несколько операций базы данных; либо все они происходят атомарно, либо ни одна из них не происходит. Если все операции в транзакции завершаются успешно, она фиксируется, а изменения остаются постоянными, но, если одна из операций завершается неудачей, все предыдущие операции откатываются, даже если они завершились успешно и были зарегистрированы как события dsdbChange.

Каждая транзакция имеет идентифицирующий GUID; другие операции DSDB, являющиеся частью транзакции, будут включать этот GUID в атрибут transactionId.

В таблице 89 приведен набор атрибутов, связанных с транзакциями (dsdbTransaction).

Пример регистрации событий, связанных с транзакциями:

```
{
  "timestamp": "2024-05-29T20:41:36.895027+0200",
  "type": "dsdbTransaction",
  "dsdbTransaction": {
    "version": {
      "major": 1,
      "minor": 0
    },
    "action": "commit",
    "transactionId": "a89149be-5c19-42c2-bf08-94ddc5b0eb78",
    "duration": 8819
  }
},
{
  "timestamp": "2024-05-29T20:41:37.691707+0200",
  "type": "dsdbTransaction",
  "dsdbTransaction": {
    "version": {
      "major": 1,
      "minor": 0
    },
    "action": "commit",
    "transactionId": "92a8db3a-94d4-4ac5-b929-b1e4344b12e3",
    "duration": 5697
  }
}
```

Т а б л и ц а 89 – Атрибуты событий, связанных с транзакциями

Атрибут	Значение
action	Текущий этап транзакции: - «begin» - «commit» - «rollback»
duration	Продолжительность транзакции в микросекундах (до момента записи этого поля)
transactionId	Уникальный идентификатор (GUID) транзакции
version	См. описание в таблице 85 Текущая версия: {"major": 1, "minor": 0}

10.6.14.5.6. Атрибуты событий, связанных с изменением пароля (passwordChange)

PasswordChange – это особый вид dsdbChange.

В таблице 90 приведен набор атрибутов, который используется для регистрации событий, связанных с изменением пароля (passwordChange).

Т а б л и ц а 90 – События, связанные с изменением пароля (passwordChange)

Атрибут	Значение
action	Тип операции: - «Change» – смена пароля; - «Reset» – сброс пароля
dn	Уникальное составное имя (DN) пользователя, пароль которого изменяется или сбрасывается
eventId	Идентификатор события Windows: - 4723 – соответствует событию смены пароля (Change); - 4724 – соответствует событию сброса пароля (Reset)
remoteAddress	Удаленный адрес пользователя, выполняющего операцию
sessionId	Идентификатор сессии DSDB
status	Текст ошибки
statusCode	Код ошибки
transactionId	Уникальный идентификатор (GUID) транзакции, в рамках которой выполняется операция (если операция является частью транзакции)
userSid	Идентификатор безопасности (SID) пользователя, инициировавшего операцию
version	См. описание в таблице 85 Текущая версия: {"major": 1, "minor": 1}

Пример регистрации события сброса пароля пользователя:

```
{ "timestamp": "2024-05-29T15:28:18.876663+0200", "type": "passwordChange",
  "passwordChange": { "version": { "major": 1, "minor": 1 }, "eventId": 4724,
    "statusCode": 0, "status": "Success", "remoteAddress":
    "ipv6:fd47:d11e:43c1:0:a00:27ff:fe9d:4de0:35534", "userSid": "S-1-5-21-
    578923263-1107570656-1287136478-500", "dn": "CN=Орлов
    Игорь, CN=Users, DC=test, DC=alt", "action": "Reset", "transactionId":
    "d7456cd1-6f32-4575-b530-dc22a34bdc6a", "sessionId": "ce6866f6-43ea-4665-
    a896-0d10bd3194e1" } }
```

10.6.14.5.7. Атрибуты событий, связанных с изменением группы (groupChange)

Событие groupChange указывает на изменение DSDB, которое добавляет или удаляет пользователя из группы.

В таблице 91 приведен набор атрибутов, который используется для регистрации событий, связанных с изменением группы (groupChange).

Т а б л и ц а 91 – Атрибуты событий, связанных с изменением группы (groupChange)

Атрибут	Значение
action	Тип операции: - «Removed» – удаление пользователя из группы; - «Added» – добавление пользователя в группу; - «PrimaryGroup» – смена основной группы
eventId	Идентификатор события Windows: - 4728 – пользователь добавлен в глобальную группу безопасности; - 4729 – пользователь удален из глобальной группы безопасности; - 4732 – пользователь добавлен в локальную группу безопасности; - 4733 – пользователь удален из локальной группы безопасности; - 4746 – пользователь добавлен в локальную группу; - 4747 – пользователь удален из локальной группы; - 4751 – пользователь добавлен в глобальную группу; - 4752 – пользователь удален из глобальной группы; - 4756 – пользователь добавлен в универсальную группу безопасности; - 4757 – пользователь удален из универсальной группы безопасности; - 4761 – пользователь добавлен в универсальную группу; - 4762 – пользователь удален из универсальной группы
group	Уникальное составное имя (DN) группы
remoteAddress	Удаленный адрес пользователя, выполняющего операцию
sessionId	Идентификатор сессии DSDB
status	Текст ошибки
Числовой код, соответствующий статусу в атрибуте status	В общем случае в качестве значения атрибута приводится код ответа LDAP в соответствии с RFC 4511
transactionId	Уникальный идентификатор (GUID) транзакции, в рамках которой выполняется операция (если операция является частью транзакции)
user	Уникальное составное имя (DN) пользователя, членство в группе которого изменяется в рамках операции
userSid	Идентификатор безопасности (SID) пользователя, инициировавшего операцию
version	См. описание в таблице 85 Текущая версия: { "major": 1, "minor": 1 }

Пример регистрации события добавления пользователя в группу:

```
{ "timestamp": "2024-05-29T15:20:19.634972+0200", "type": "groupChange",
"groupChange": { "version": { "major": 1, "minor": 1 }, "eventId": 4728,
"statusCode": 0, "status": "Success", "action": "Added", "remoteAddress":
"ipv6:fd47:d11e:43c1:0:a00:27ff:fe9d:4de0:59778", "userSid": "S-1-5-21-
578923263-1107570656-1287136478-500", "group":
"CN=testgroup,CN=Users,DC=test,DC=alt", "transactionId": "28372270-093c-4bca-
af45-ae3e93b71eda", "sessionId": "9518687d-8ad1-4c2c-810c-8cc18c2943f7",
"user": "CN=Марков Кирилл,CN=Users,DC=test,DC=alt"}}
```

10.6.15. Усиление безопасности DC

10.6.15.1. Возможность анонимного получения списка пользователей, групп

Samba наследует поведение домена NT4, которое больше не требуется в режиме «Альт Домен». Например, следующая команда возвращает всех пользователей домена:

```
# rpcclient -U "" -c enumdomusers dcl.test.alt
```

Для отключения такого поведения следует внести изменения в файл `/etc/samba/smb.conf`:

```
[global]
restrict anonymous = 2
```

Может также потребоваться работа с полем `dsHeuristics`:

```
# samba-tool forest directory_service dsheuristics 0000000
```

10.6.15.2. Отключение Netbios

Если конфигурация DNS выполнена правильно, старые протоколы NetBIOS, которые больше не нужны, могут быть отключены. Для этого следует внести изменения в секцию `[global]` файла `smb.conf`:

```
[global]
disable netbios = yes
smb ports = 445
```

10.6.15.3. Отключение роли сервера печати

Контроллер домена не следует настраивать с ролью сервера печати. Сервер Samba, настроенный как файловый сервер, лучше подходит для этой функции.

Для отключения роли сервера печати следует внести изменения в секцию `[global]` файла `smb.conf`:

```
[global]
printcap name = /dev/null
load printers = no
disable spoolss = yes
printing = bsd
```

10.6.15.4. Отключение NTLMv1

Протокол аутентификации NTLMv1 появился в начале 1990-х годов и был быстро заменен на NTLMv2 из-за недостатков безопасности. Он больше не полезен в современных сетях, за исключением случаев использования MS-CHAP-v2, который является протоколом по умолчанию для аутентификации 802.1x на рабочих

станциях Windows (например, аутентификация Radius для подключений Wi-Fi). В случае MS-CHAP-v2 использование NTLMv1 можно до некоторой степени допустить, поскольку он инкапсулирован в другой, более надежный протокол.

В Samba есть возможность глобально отключить NTLMv1, если он не используется для аутентификации MS-CHAP-v2. Рекомендуется добавить следующий параметр в секцию [global] файла smb.conf:

```
[global]
ntlm auth = mschapv2-and-ntlmv2-only
```

10.6.15.5. Генерация дополнительных хешей паролей

Чтобы разрешить передачу хешей в другую базу аутентификации, можно указать «Альт Домен» генерировать дополнительные хеши, когда пользователь меняет свой пароль. Для этого следует добавить в секцию [global] файла smb.conf строку:

```
[global]
password hash userPassword schemes = CryptSHA256 CryptSHA512
```

10.6.15.6. Защита DNS-записей wpad и isatap

Серверы Windows AD имеют глобальный черный список запросов DNS с двумя записями:

- wpad;
- isatap.

В разделе реестра GlobalQueryBlockList перечислены эти две записи DNS, для предотвращения создания таких записей и перенаправления сетевого трафика неавторизованным объектом, действующим в локальной сети. Протокол автоматического обнаружения веб-прокси (WPAD) по умолчанию настроен в браузерах WPAD, в частности в браузерах Internet Explorer.

Даже если конфигурации wpad и isatap не используются, все равно важно создать эти две записи, чтобы предотвратить их использование обходным путем, поскольку в «Альт Домен» нет способа заблокировать создание записей, так как это можно сделать в Microsoft AD.

Создание записей wpad и isatap в «Альт Домен»:

```
# samba-tool dns add `hostname -s` `hostname -d` wpad A 127.0.0.1 -P
# samba-tool dns add `hostname -s` `hostname -d` isatap A 127.0.0.1 -P
```


10.6.15.7. Ограничение диапазона динамических портов

По умолчанию «Альт Домен» использует очень широкий динамический диапазон для вызовов MS-RPC. Рекомендуется ограничить этот диапазон. Для этого следует добавить в секцию [global] файла smb.conf строку:

```
[global]
rpc server dynamic port range = 50000-55000
```

Примечание. Если используется фаервол, то его нужно будет перенастроить.

10.6.15.8. Аудит запросов к каталогам SYSVOL и NetLogon

Для возможности аудита запросов к каталогам SYSVOL и NetLogon следует добавить в файл smb.conf строки:

```
[global]
...
full_audit:failure = none
full_audit:success = pwrite write renameat
full_audit:prefix = IP=%I|USER=%u|MACHINE=%m|VOLUME=%S
full_audit:facility = local7
full_audit:priority = NOTICE
...
[sysvol]
...
vfs objects = dfs_samba4, acl_xattr, full_audit
...
[netlogon]
...
vfs objects = dfs_samba4, acl_xattr, full_audit
```

10.6.15.9. Отправка логов аудита в rsyslog

10.6.15.9.1. Настройка rsyslog

Установить пакет rsyslog-classic:

```
# apt-get install rsyslog-classic
```

На стороне отправителя сообщений (клиента) создать файл /etc/rsyslog.d/all.conf, в котором прописать протокол (@@ – TCP, @ – UDP) и адрес доставки сообщений:

```
*.* @@192.168.0.111:514
```

На стороне приемника сообщений (сервера) в файле

/etc/rsyslog.d/00_common.conf раскомментировать строки:

```
#для udp
module(load="imudp")
input(type="imudp" port="514")
#для tcp
module(load="imtcp")
input(type="imtcp" port="514")
```

И создать свой шаблон для логов /etc/rsyslog.d/myrules.conf:

```
$template remote-incoming-logs, "/var/log/%HOSTNAME/%PROGRAMNAME.log"
*. * ?remote-incoming-logs
```

10.6.15.9.2. rsyslog на том же хосте

В секцию [global] файла smb.conf добавить строку:

```
[global]
log level = 1 auth_json_audit:3@/var/log/samba/samba_audit.log
```

Создать файл /etc/rsyslog.d/send_samba.conf:

```
module(load="imfile" PollingInterval="10") #needs to be done just once
input(type="imfile"
File="/var/log/samba/samba_audit.log"
Tag="samba_auth"
Severity="info"
Facility="auth")
if ($syslogtag == "samba_auth") then {
action(type="omfwd" target="dcl.test.alt" port="514" protocol="tcp"
action.resumeRetryCount="100"
queue.type="LinkedList" queue.size="10000")
}
```

10.6.15.9.3. rsyslog на вышестоящем хосте

В секцию [global] файла smb.conf добавить строку:

```
[global]
log level = 1 auth_json_audit:3@/var/log/samba/samba_audit.log
```

Создать файл /etc/rsyslog.d/recv_samba.conf:

```
$ModLoad imtcp
$InputTCPServerRun 514
if ($syslogtag == "samba_auth") then /var/log/samba/audit_auth.log
```

10.6.16. Инструменты командной строки

Основные инструменты командной строки для управления доменом представлены в таблице 92.

Т а б л и ц а 92 – Основные инструменты

Утилита	Описание
samba-tool	Основная утилита управления Samba
wbinfo	Позволяет получить информацию от демона winbindd
net	Инструмент администрирования Samba и удаленных серверов CIFS
adcli	Инструмент для выполнения действий в домене Active Directory
ldapsearch	Утилита для поиска информации в LDAP
testparm	Проверка корректности содержимого основного файла конфигурации Samba – /etc/samba/smb.conf

10.6.16.1. Команда samba-tool

Основные команды утилиты samba-tool приведены в таблице 93.

Т а б л и ц а 93 – Основные команды samba-tool

Команда	Описание
computer	Управление учетными записями компьютеров
contact	Управление контактами
dbcheck	Проверка локальной базы данных домена на наличие ошибок
delegation	Управление делегированием
dns	Управление параметрами доменной службы DNS
domain	Управление параметрами домена
drs	Управление службой репликации каталогов (Directory Replication Services, DRS)
dsacl	Управление групповыми политиками
forest	Управление ролями (Flexible Single Master Operations, FSMO)
fsmo	Управление конфигурацией леса
gpo	Управление списками контроля доступа DS
group	Управление группами
ldapcmp	Сравнение двух баз данных ldap
ntacl	Вывод списка процессов
processes	Управление списками контроля доступа ACL
ou	Управление организационными подразделениями (OU)
rodc	Управление контроллером домена (Read-Only Domain Controller, RODC)
schema	Управление и запрос схемы
sites	Управление сайтами
spn	Управление службой принципалов (Service Principal Name, SPN)
testparm	Проверка конфигурационного файла на корректность синтаксиса
time	Получение показаний текущего времени сервера
user	Управление пользователями
visualize	Графическое представление состояния сети Samba

Получить дополнительную информацию можно на справочной странице samba-tool (man samba-tool).

Пример получения дополнительной информации о подкоманде:

```
$ samba-tool fsmo -help
```

Примеры:**- вывести список групповых политик:**

samba-tool gpo listall

```
GPO : {31B2F340-016D-11D2-945F-00C04FB984F9}
display name : Default Domain Policy
path : \\test.alt\sysvol\test.alt\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}
dn : CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=test,DC=alt
version : 0
flags : NONE
GPO : {FE6268E4-FDEB-4DCA-94E8-BB1170C66F45}
display name : scripts
path : \\test.alt\sysvol\test.alt\Policies\{FE6268E4-FDEB-4DCA-94E8-BB1170C66F45}
dn : CN={FE6268E4-FDEB-4DCA-94E8-BB1170C66F45},CN=Policies,CN=System,DC=test,DC=alt
version : 65536
flags : NONE
GPO : {6AC1786C-016F-11D2-945F-00C04FB984F9}
display name : Default Domain Controllers Policy
path : \\test.alt\sysvol\test.alt\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}
dn : CN={6AC1786C-016F-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=test,DC=alt
version : 0
flags : NONE
GPO : {44F1A3E9-BD0D-44D7-AC1D-CEEF2817C573}
display name : Общие каталоги
path : \\test.alt\sysvol\test.alt\Policies\{44F1A3E9-BD0D-44D7-AC1D-CEEF2817C573}
dn : CN={44F1A3E9-BD0D-44D7-AC1D-CEEF2817C573},CN=Policies,CN=System,DC=test,DC=alt
version : 0
flags : NONE
```

- вывести все связанные контейнеры для объекта групповой политики:

```
# samba-tool gpo listcontainers {44F1A3E9-BD0D-44D7-AC1D-CEEF2817C573}
```

```
Container(s) using GPO {44F1A3E9-BD0D-44D7-AC1D-CEEF2817C573}
DN: OU=OU,DC=test,DC=alt
DN: OU=KDE,DC=test,DC=alt
```

- вывести список групповых политик, связанных с контейнером:

```
# samba-tool gpo getlink OU=OU,DC=test,DC=alt
GPO(s) linked to DN OU=OU,DC=test,DC=alt
GPO : {96D5897A-CEFB-4A1B-90AF-5D83707130C4}
Name : Файлы
Options : NONE
GPO : {A12547D7-2FFA-4E37-9382-D6767489E3DF}
Name : kde
Options : NONE
GPO : {75E65DF7-56A7-48E1-A393-F5FFAA1010FD}
Name : Control_ping
```

```

Options : NONE
GPO : {FE6268E4-FDEB-4DCA-94E8-BB1170C66F45}
Name : scripts
Options : NONE
GPO : {44F1A3E9-BD0D-44D7-AC1D-CEEF2817C573}
Name : Общие каталоги
Options : NONE
GPO : {0CCFA74C-57F5-42B5-98E2-007D4A59C4C4}
Name : firefox
Options : NONE
GPO : {2CF4EB19-343E-448A-BBBC-A9EC2F7C22E9}
Name : Установка пакетов
Options : NONE

```

10.6.16.2. Команда wbinfo

Команда `wbinfo` создает запросы и возвращает информацию к (от) демона `winbindd`.

Параметры команды `wbinfo` представлены в таблице 94.

Т а б л и ц а 94 – Параметры команды `wbinfo`

Параметр	Описание	Пример
<code>-a --authenticate username %password</code>	Попытаться аутентифицировать пользователя через <code>winbindd</code> . Проверяет два метода аутентификации: <code>plaintext password</code> (применяется при входе пользователя в систему локально), <code>challenge/response password</code> (использует NTLM или Kerberos).	<pre>\$ wbinfo -a TEST\\ivanov Enter TEST\ivanov's password: plaintext password authentication succeeded Enter TEST\ivanov's password: challenge/response password authentication succeeded</pre>
<code>--allocate-gid</code>	Получить новый GID из <code>idmap</code>	
<code>--allocate-uid</code>	Получить новый UID из <code>idmap</code>	
<code>--all-domains</code>	Вывести список всех доменов (доверенных и собственный)	<pre>\$ wbinfo --all-domains BUILTIN TEST EXAMPLE</pre>
<code>-c --change-secret</code>	Изменить пароль доверительной учетной записи. Может использоваться вместе с доменом для изменения паролей учетных записей междоменного доверия.	
<code>--cache-save <имя_пользователя>%<пароль></code>	Сохранить имя пользователя и пароль для <code>cache</code>	
<code>--change-user-password <имя_пользователя></code>	Изменить пароль пользователя (будет запрошен старый и новый пароль)	<pre># wbinfo --change-user-password ivanov Enter ivanov's old password: Enter ivanov's new password:</pre>
<code>--dc-info <домен></code>	Вывести текущий контроллер домена для домена	<pre>\$ wbinfo --dc-info TEST dc1.test.alt (192.168.0.132)</pre>

Продолжение таблицы 94

Параметр	Описание	Пример
--domain <домен>	Определяет домен, в котором будут выполняться любые указанные операции	
-D --domain-info <домен>	Показать информацию об указанном домене	\$ wbinfo -D TEST Name : TEST Alt_Name : test.alt SID : S-1-5-21-578923263-1107570656-1287136478 Active Directory : Yes Native : Yes Primary : Yes
--dsgetdcname <домен>	Найти DC для домена	\$ wbinfo --dsgetdcname TEST \\dc1.test.alt \\192.168.0.132 1 d75c7b83-9472-4646-adb2-52b3d6968eb6 test.alt test.alt 0xe00013fd Default-First-Site-Name Default-First-Site-Name
--gid-info <gid>	Получить информацию о группе по gid	\$ wbinfo --gid-info 10000 domain admins:*:10000:
--group-info <группа>	Получить информацию о группе по имени группы	\$ wbinfo --group-info "TEST\\domain admins" domain admins:*:10000:
-g --domain-groups	Вывести список доменных групп	\$ wbinfo -g ... TEST\domain admins TEST\domain users TEST\domain guests TEST\domain computers ...
--get-auth-user	Эта функция была перенесена в утилиту net	
--getdcname <домен>	Вывести имя контроллера домена для указанного домена	\$ wbinfo --getdcname TEST DC1
-G --gid-to-sid <gid>	Преобразовать идентификатор группы UNIX в SID Windows NT. Если указанный gid не относится к диапазону gid idmap, операция завершится ошибкой.	\$ wbinfo -G 10000 S-1-5-21-578923263-1107570656-1287136478-512
-i --user-info <имя_пользователя>	Вывести информацию о пользователе	\$ wbinfo -i TEST\\ivanov ivanov:*:10000:10001:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash
-I --WINS-by-ip ip	Вывести NetBIOS-имя, связанное с IP-адресом	\$ wbinfo -I 192.168.0.135 192.168.0.135 WORK135
-K --krb5auth <имя_пользователя>%<пароль>	Попытаться аутентифицировать пользователя через Kerberos	\$ wbinfo -K TEST\\ivanov Enter TEST\ivanov's password: plaintext kerberos password authentication for [TEST\ivanov] succeeded (requesting cctype: FILE)

Продолжение таблицы 94

Параметр	Описание	Пример
--krb5ccname KRB5CCNAME	Запросить определенный тип кэша учетных данных Kerberos, используемый для аутентификации	
--lanman	Использовать криптографию Lanman для аутентификации пользователей	
--logoff	Выйти из системы	
--logoff-uid UID	Определяет идентификатор пользователя, используемый во время запроса на выход из системы	
--logoff-user <имя_пользователя>	Определяет имя пользователя, используемое во время запроса на выход из системы	
--lookup-sids SID1, SID2...	Поиск SID	\$ wbinfo --lookup-sids S-1-5-21-578923263-1107570656-1287136478-512 S-1-5-21-578923263-1107570656-1287136478-512 -> <none>\Domain Admins 2
-m --trusted-domains	Вывести список доверенных доменов	\$ wbinfo --trusted-domains BUILTIN TEST EXAMPLE
-n --name-to-sid <имя>	Вывести SID, связанный с указанным именем. Если домен не указан, используется домен, указанный в параметре <code>workgroup smb.conf</code>	\$ wbinfo -n TEST\\ivanov S-1-5-21-578923263-1107570656-1287136478-1103 SID_USER (1)
-N --WINS-by-name <name>	Вывести IP-адрес, связанный с именем NetBIOS, указанным в параметре <code>name</code>	\$ wbinfo -N WORK135 192.168.0.135 WORK135
--ntlmv1	Использовать криптографию NTLMv1 для аутентификации пользователей	
--ntlmv2	Использовать криптографию NTLMv2 для аутентификации пользователей	
--online-status <домен>	Показать, поддерживает ли winbind в настоящее время активное соединение или нет. Если домен не указан, будет выведен статус текущего домена	\$ wbinfo --online-status BUILTIN : active connection TEST : active connection
--own-domain	Вывести собственный домена	\$ wbinfo --own-domainTEST
--pam-logon <имя_пользователя>%<пароль>	Попытаться аутентифицировать пользователя так же, как это сделал бы <code> pam_winbind </code>	\$ wbinfo --pam-logon ivanov Enter ivanov's password: plaintext password authentication succeeded
-p --ping	Проверяет запущен ли winbindd	\$ wbinfo -p Ping to winbindd succeeded
-P --ping-dc	Проверить безопасное соединение с контроллером домена	\$ wbinfo -P checking the NETLOGON for domain[TEST] dc connection to "dcl.test.alt" succeeded

Продолжение таблицы 94

Параметр	Описание	Пример
<code>-r --user-groups <имя_пользователя></code>	Получить список идентификаторов групп, к которым принадлежит пользователь. Доступно только при наличии пользователя на контроллере домена	<code>\$ wbinfo -r ivanov</code> 10001 10003
<code>-R --lookup-rids rid1, rid2, rid3..</code>	Преобразовать RID в имена	
<code>--remove-gid-mapping GID,SID</code>	Удалить существующее сопоставление GID и SID из базы данных	
<code>--remove-uid-mapping UID,SID</code>	Удалить существующее сопоставление UID и SID из базы данных	
<code>-s --sid-to-name sid</code>	Преобразовать SID в имя	<code>\$ wbinfo -s S-1-5-21-578923263-1107570656-1287136478-1103</code> TEST\ivanov 1
<code>--separator</code>	Вывести активный разделитель winbind	<code>\$ wbinfo --separator</code> \
<code>--sequence</code>	Команда устарела, вместо нее следует использовать параметр <code>--online-status</code>	
<code>--set-auth-user <имя_пользователя>%<пароль></code>	Эта функция была перенесена в утилиту net	
<code>--set-gid-mapping GID,SID</code>	Создать сопоставление GID и SID в базе данных	
<code>--set-uid-mapping UID,SID</code>	Создать сопоставление UID и SID в базе данных	
<code>-S --sid-to-uid sid</code>	Преобразовать SID в идентификатор пользователя	<code>\$ wbinfo -S S-1-5-21-578923263-1107570656-1287136478-1103</code> 10000
<code>--sid-aliases sid</code>	Получить псевдонимы SID для заданного SID	
<code>--sid-to-fullname sid</code>	Преобразовать SID в полное имя пользователя (ДОМЕН\имя пользователя)	<code>\$ wbinfo --sid-to-fullname S-1-5-21-578923263-1107570656-1287136478-1103</code> TEST\Иван Иванов 1
<code>--sids-to-unix-ids sid1,sid2,sid3..</code>	Преобразовать SID в Unix ID	<code>\$ wbinfo --sids-to-unix-ids S-1-5-21-578923263-1107570656-1287136478-1103</code> S-1-5-21-578923263-1107570656-1287136478-1103 -> uid 10000
<code>-t --check-secret</code>	Проверить, что доверительная учетная запись рабочей станции, созданная при добавлении сервера Samba в домен Windows NT, работает. Может использоваться вместе с доменом для проверки учетных записей междоменного доверия	

Окончание таблицы 94

Параметр	Описание	Пример
<code>-u --domain-users</code>	Вывести список доменных пользователей	<pre>\$ wbinfo -u administrator krbtgt ivanov guest</pre>
<code>--uid-info uid</code>	Получить информацию о пользователе по идентификатору	<pre>\$ wbinfo --uid-info 10000 ivanov:*:10000:10001:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash</pre>
<code>--usage</code>	Вывести краткую справку о программе	
<code>--user-domgroups sid</code>	Вывести группы пользователей домена	<pre>\$ wbinfo --user-domgroups S-1-5-21-578923263-1107570656-1287136478-1103 S-1-5-21-578923263-1107570656-1287136478-1103 S-1-5-21-578923263-1107570656-1287136478-513</pre>
<code>--user-sidinfo sid</code>	Получить информацию о пользователе по sid	<pre>\$ wbinfo --user-sidinfo S-1-5-21-578923263-1107570656-1287136478-1103 ivanov:*:10000:10001:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash</pre>
<code>--user-sids sid</code>	Получить SID групп пользователя	<pre>\$ wbinfo --user-sids S-1-5-21-578923263-1107570656-1287136478-1103 S-1-5-21-578923263-1107570656-1287136478-1103 S-1-5-21-578923263-1107570656-1287136478-513 S-1-5-32-545</pre>
<code>-U --uid-to-sid uid</code>	Преобразовать идентификатор пользователя UNIX в SID	<pre>\$ wbinfo -U 10000 S-1-5-21-578923263-1107570656-1287136478-1103</pre>
<code>-Y --sid-to-gid sid</code>	Преобразовать SID в идентификатор группы UNIX	<pre>\$ wbinfo -Y S-1-5-21-578923263-1107570656-1287136478-513 10001</pre>

10.6.16.3. Команда net

net – инструмент администрирования Samba и удаленных серверов CIFS.

Синтаксис:

```
net <протокол> <функция> <дополнительные_параметры>
<параметры_цели>
```

где <протокол> – протокол, используемый при выполнении команды.

Возможные значения: ads (Active Directory), rap (Win9x/NT3) или rpc (WindowsNT4/2000/2003/2008/2012). Если протокол не указан, net пытается определить его автоматически.

Основные подкоманды команды net ads представлены в таблице 95.

Т а б л и ц а 95 – Основные подкоманды net ads

Команда	Описание
info	Вывод информации о домене
join	Присоединение машины к домену
testjoin	Проверка, действителен ли пароль учетной записи компьютера
leave	Удалить локальную машину из домена AD
status	Вывод информации об учетной записи компьютера
user	Список/изменение пользователей
group	Список/изменение групп
dns	Выполнить динамическое обновление DNS
password	Изменить пароль пользователей
changetrustpw	Изменить пароль доверительной учетной записи
printer	Список/изменение записей принтера
search	Выполнить поиск LDAP с использованием фильтра
dn	Выполнить поиск LDAP по DN
sid	Выполнить поиск LDAP по SID
workgroup	Показать имя рабочей группы
lookup	Найти контроллер домена AD с помощью поиска CLDAP
keytab	Управление локальным файлом keytab
spnset	Управление именами участников-служб (SPN)
gpo	Управление объектами групповой политики
kerberos	Управление keytab Kerberos
enctypes	Список/изменение enctypes

Получить дополнительную информацию можно на справочной странице net(8) (man net).

Пример получения дополнительной информации о подкоманде:

```
# net time --help
```

Получение информации о домене:

```
# net ads info
LDAP server: 192.168.0.132
LDAP server name: dc1.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
LDAP port: 389
Server time: Чт, 08 июн 2023 11:48:01 EET
KDC server: 192.168.0.132
Server time offset: -171
Last machine account password change: Вт, 16 мая 2023 09:26:46 EET
```

Получение информации об учетной записи компьютера:

```
# net ads status -U administrator
```

10.6.16.4. Команда `adcli`

`adcli` – инструмент для выполнения действий в домене Active Directory.

Основные команды `adcli` представлены в таблице 96.

Т а б л и ц а 96 – Основные команды `adcli`

Команда	Описание
<code>info домен</code>	Вывести информацию о домене
<code>join домен</code>	Присоединить данную машину к домену (создает учетную запись компьютера в домене и настраивает <code>keytab</code> для этой машины. Не настраивает службу аутентификации, например, <code>sssd</code>).
<code>update</code>	Обновляет пароль учетной записи компьютера на контроллере домена для локальной машины, записывает новые ключи в <code>keytab</code> и удаляет старые ключи
<code>testjoin</code>	Проверить, действителен ли пароль учетной записи компьютера
<code>create-user</code> [--domain=домен] пользователь	Создать учетную запись пользователя
<code>delete-user</code> [--domain=домен] пользователь	Удалить учетную запись пользователя
<code>passwd-user</code> [--domain=домен] пользователь	Установить (повторно) пароль пользователя
<code>create-group</code> [--domain=домен] группа	Создать группу
<code>delete-group</code> [--domain=домен] группа	Удалить группу
<code>add-member</code> [--domain=домен] группа пользователь или компьютер...	Добавить пользователей в группу
<code>remove-member</code> [--domain=домен] группа пользователь...	Удалить пользователей из группы
<code>preset-computer</code> [--domain=домен] компьютер...	Предустановить учетные записи компьютеров (предварительно создает одну или несколько учетных записей компьютеров в домене, чтобы позже компьютеры могли использовать их при присоединении к домену. При этом, машины могут присоединяться с помощью одноразового пароля или автоматически без пароля).
<code>reset-computer</code> [--domain=домен] компьютер	Сбросить учетную запись компьютера (если соответствующая машина присоединена к домену, ее членство будет нарушено).
<code>delete-computer</code> [--domain=домен] компьютер	Удалить учетную запись компьютера
<code>show-computer</code> [--domain=домен] компьютер	Показать атрибуты учетной записи компьютера, хранящиеся в AD
<code>create-msa</code> [--domain=домен]	Создать управляемую учетную запись службы (MSA) в заданном домене AD (это бывает нужно, если компьютер не должен присоединяться к домену Active Directory, но к нему необходим LDAP доступ)

Получить дополнительную информацию можно на справочной странице `adcli`.

Пример получения дополнительной информации о подкоманде:

```
# adcli testjoin --help
```

Получение информации о домене:

```
# adcli info test.alt
```

```
[domain]
```

```
domain-name = test.alt
```

```
domain-short = TEST
```

```
domain-forest = test.alt
```

```
domain-controller = dc1.test.alt
```

```
domain-controller-site = Default-First-Site-Name
```

```
domain-controller-flags = pdc gc ldap ds kdc timeserv closest  
writable good-timeserv full-secret
```

```
domain-controller-usable = yes
```

```
domain-controllers = dc1.test.alt dc2.test.alt
```

```
[computer]
```

```
computer-site = Default-First-Site-Name
```

Показать атрибуты учетной записи компьютера:

```
# adcli show-computer -D test.alt win2012
```

```
Password for Administrator@TEST.ALT:
```

```
sAMAccountName:
```

```
WIN2012$
```

```
userPrincipalName:
```

```
- not set -
```

```
msDS-KeyVersionNumber:
```

```
1
```

```
msDS-supportedEncryptionTypes:
```

```
28
```

```
dNSHostName:
```

```
win2012.test.alt
```

```
servicePrincipalName:
```

```
HOST/win2012.test.alt
```

```
RestrictedKrbHost/win2012.test.alt
```

```
HOST/WIN2012
```

```
RestrictedKrbHost/WIN2012
```

```
Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/win2012.test.alt
```

```
operatingSystem:
```

```
Windows Server 2012 R2 Standard
```

```
operatingSystemVersion:
```

```
6.3 (9600)
```

```
operatingSystemServicePack:
```

```
- not set -  
pwdLastSet:  
  133294743593838200  
userAccountControl:  
  4096  
description:  
  - not set -
```

Создать группу testldap в подразделении OU:

```
# adcli create-group -D test.alt -O OU=OU,dc=test,dc=alt testldap  
Password for Administrator@TEST.ALT
```

10.6.16.5. Утилита ldapsearch

ldapsearch – утилита для поиска информации в LDAP.

Синтаксис:

```
ldapsearch <параметры> <фильтр> <атрибуты>
```

ldapsearch открывает соединение с сервером LDAP, подключается к нему и выполняет поиск с помощью фильтра.

Если утилита ldapsearch найдет одну или несколько записей, то значения указанных атрибутов этих записей будут переданы в стандартный поток вывода. Если в этом списке указан знак *, возвращаются все пользовательские атрибуты. Если в этом списке указан знак +, возвращаются все операционные атрибуты. Если атрибуты не указаны, то возвращаются все пользовательские атрибуты.

Если утилита ldapsearch найдет одну или несколько записей, то значения указанных атрибутов этих записей будут переданы в стандартный поток вывода. Если атрибуты не указаны, то возвращаются все атрибуты.

Результаты поиска отображаются в виде расширенной версии LDIF. Формат вывода контролируется с помощью параметра -L.

Параметры команды ldapsearch представлены в таблице 97.

Т а б л и ц а 97 – Параметры команды `ldapsearch`

Параметр	Описание
Параметры поиска	
<code>-a {never always search find}</code>	Задаёт способ преобразования псевдонимов. Может принимать значения: <code>never</code> (по умолчанию), <code>always</code> , <code>search</code> или <code>find</code> , указывающие, соответственно, что псевдонимы не преобразуются, преобразуются всегда, преобразуются при поиске, либо преобразуются только при определении базового объекта для поиска
<code>-A</code>	Получить только атрибуты (без значений)
<code>-b basedn</code>	Позволяет переопределить заданную по умолчанию начальную точку поиска
<code>-c</code>	Режим продолжения операции (не останавливать поиск при ошибках)
<code>-E [!]ext [=extparam]</code>	Указывает расширения поиска. Знак «!» обозначает критичность расширения. Общие расширения: <ul style="list-style-type: none"> - [!]domainScope (диапазон домена); - !dontUseCopy; - [!]mv=<filter> (RFC 3876 фильтр совпавших значений); - [!]pr=<size>[/prompt noprompt] (RFC 2696 постраничный вывод результатов/запрос вывода); - [!]sss=[-]<attr[:OID]>[/[-]<attr[:OID]>...] (RFC 2891 сортировка на стороне сервера); - [!]subentries[=true false] (RFC 3672 подзаписи); - [!]sync=ro[/<cookie>] (RFC 4533 LDAP Sync refreshOnly); - [!]sync=rp[/<cookie>[/<slimit>]] (LDAP Sync refreshAndPersist); - [!]vlv=<before>/<after>(/<offset>/<count> :<value>) (ldapv3-vlv-09 вид виртуального списка); - [!]deref=derefAttr:attr[,...][;derefAttr:attr[,...][;...]]; - [!]<oid>[=:<b64value>] (общий контроль; нет обработки ответа)
<code>-f file</code>	Считать серию строк из файла <code>file</code> и выполнить по одному поиску LDAP для каждой строки. В этом случае заданный в командной строке фильтр <code>filter</code> интерпретируется как шаблон, в котором первое и только первое вхождение символа <code>%s</code> заменяется строкой из файла <code>file</code> . Любые другие вхождения символа <code>%</code> в шаблоне будут рассматриваться как ошибка. Если требуется, чтобы в поисковом фильтре присутствовал символ «%», он должен быть закодирован как <code>\25</code> (смотрите RFC 4515). Если в качестве значения <code>file</code> указан символ «-», то строки считываются со стандартного ввода
<code>-F prefix</code>	URL-префикс для временных файлов (по умолчанию: <code>file://path</code> , где <code>path</code> либо <code>/tmp/.private/<user></code> , либо значение, указанное в параметре <code>-T</code>)
<code>-l limit</code>	Ограничение на время поиска (в секундах). Значение 0 (ноль) или <code>none</code> означает, что ограничений нет. Значение <code>max</code> означает максимальное допустимое протоколом значение (целое число)
<code>-L [LL]</code>	Управление выводом результатов поиска в формате обмена данными LDAP (LDAP Data Interchange Format): <ul style="list-style-type: none"> - <code>-L</code> – вывести ответы в формате LDIFv1; - <code>-LL</code> – отключить вывод комментариев; - <code>-LLL</code> – отключить вывод версии LDIF
<code>-M [M]</code>	Включить элемент управления Manage DSA IT. <code>-mm</code> делает этот элемент управления критичным
<code>-P {2 3}</code>	Версия протокола LDAP (по умолчанию 3)

Продолжение таблицы 97

Параметр	Описание
-s {base one sub children}	Задаёт область поиска. Может принимать одно из следующих значений: base, one, sub (по умолчанию) или children, что означает поиск только по базовому объекту, на одном уровне, по всему поддереву и по дочерним записям соответственно
-S attr	Отсортировать возвращаемые записи по атрибуту attr. По умолчанию возвращаемые записи не сортируются. Если в качестве attr задана строка нулевой длины (""), записи сортируются по компонентам их уникального имени Distinguished Name. По умолчанию ldapsearch выводит записи по мере их получения. При использовании параметра -S все данные сначала получаются, потом сортируются, потом выводятся
-t[t]	При указании одного -t полученные непечатаемые значения записываются в набор временных файлов (полезно при работе со значениями, содержащими несимвольные данные, такими как jpegPhoto или audio). При указании второго -t все полученные значения записываются в файлы
-T path	Временные файлы записываются в указанный в path каталог (по умолчанию /tmp/.private/<user>)
-u	Включить в вывод форму удобного для пользователя имени (User Friendly Name, UFN) уникального имени (Distinguished Name, DN)
-z limit	Ограничить количество возвращаемых в результате поиска записей значением limit. Значение 0 (ноль) или none означает, что ограничений нет. Значение max означает максимальное допустимое протоколом значение (целое число)
Общие параметры	
-d debuglevel	Установить уровень отладки LDAP
-D binddn	Использовать указанное в binddn уникальное имя Distinguished Name при подсоединении к каталогу LDAP. При SASL-подсоединениях сервер будет игнорировать это значение
-e [!]ext [=extram]	Указывает общие расширения. Знак «!» обозначает критичность расширения. Общие расширения: <ul style="list-style-type: none"> - [!]assert=<filter> (RFC 4528; фильтр RFC 4515) - [!]authzid=<authzid> (RFC 4370; "dn:<dn>" или "u:<user>") - [!]chaining[=<resolveBehavior>[/<continuationBehavior>]] - [!]manageDSAit (RFC 3296) - [!]noop - ppolicy - [!]postread[=<attrs>] (RFC 4527; разделенный запятыми список атрибутов) - [!]preread[=<attrs>] (RFC 4527; разделенный запятыми список атрибутов) - [!]relax - [!]sessiontracking - abandon, cancel, ignore (сигнал SIGINT посылает abandon/cancel, либо в ответ на него посылается ignore; если расширение помечено как критичное, сигнал SIGINT не принимается; ненастоящие элементы управления

Окончание таблицы 97

Параметр	Описание
-h host	Сервер LDAP
-H URI	Указывает URI (возможно, несколько), ссылающийся на LDAP-сервер (серверы). В URI допускаются поля: протокол/хост/порт
-I	Использовать интерактивный режим SASL
-n	Демонстрируется, что будет сделано, но реальный поиск не выполняется. Используется для отладки совместно с параметром -v
-N	Не использовать обратное разрешение DNS для получения канонического имени хоста SASL
-O props	Параметры безопасности SASL
-o opt [=optparam]	Указывает опции общего назначения. Возможные опции: - nettimeout=<timeout> (в секундах, либо «none» или «max») - ldif-wrap=<width> (в символах, либо «no» для предотвращения переноса строк)
-p порт	Порт, на котором сервер LDAP принимает запросы. Номер порта по умолчанию – 389. Если номер порта не задан, и указан параметр -z, то применяется номер порта LDAP SSL по умолчанию, равный 636
-Q	Использовать тихий режим SASL. Запросы не выводятся никогда
-R realm	Задаёт realm аутентификационного идентификатора для SASL. Форма realm зависит от того, какой механизм аутентификации в действительности используется
-U authcid	Идентификатор аутентификации SASL. Форма идентификатора зависит от того, какой механизм аутентификации в действительности используется
-v	Использовать тихий режим SASL. Запросы не выводятся никогда
-V[V]	Вывести информацию о версии. При указании -VV, после вывода информации о версии осуществляется выход. При указании -V, после вывода информации о версии выполняется поиск согласно заданным критериям
-w passwd	Использовать указанное значение passwd в качестве пароля для простой аутентификации
-W	Запрашивать ввод пароля для простой аутентификации (используется для того, чтобы не указывать пароль в командной строке)
-x	Использовать простую аутентификацию
-X authzid	Идентификатор авторизации SASL («dn:<dn>» или «u:<user>»)
-y file	Считать пароль из файла file. В качестве пароля используется все содержимое файла. Поэтому файл не должен содержать символа переноса строки
-Y mech	Задаёт механизм SASL, который будет использоваться для аутентификации. Если параметр не указан, программа выберет лучший из известных серверу механизмов
-Z[Z]	Запустить запрос TLS (-ZZ для запроса успешного ответа)

10.6.16.5.1. Фильтр

Фильтр должен быть указан в строковом формате фильтров. Если фильтр не указан, используется фильтр по умолчанию (objectClass=*).

Синтаксис LDAP-фильтра имеет вид:

<Атрибут><оператор сравнения><значение>

Вместо имени атрибута можно использовать его идентификатор (Attribute-Id).

Тело фильтра должно быть заключено в скобки.

Примеры LDAP-фильтров представлены в таблице 98.

Т а б л и ц а 98 – Примеры LDAP-фильтров

Запрос	LDAP фильтр
Все пользователи:	(sAMAccountType=805306368)
Отключенные (Disabled) пользователи:	(&(sAMAccountType=805306368)(useraccountcontrol:1.2.840.113556.1.4.803:=2))
Заблокированные (Locked) пользователи:	(&(sAMAccountType=805306368)(badPwdCount>=4))
Пользователи, у которых в настройках указано «Пароль никогда не истекает»	(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=65536))
Пользователи, которые не меняли пароль с 5 мая 2023 года	(&(objectCategory=person)(pwdLastSet<=133278047990000000))
Пользователи с незаполненным полем mail	(&(objectCategory=group)!(mail=*))
Пользователи, которые должны сменить пароль при следующем входе в систему	(&(sAMAccountType=805306368)(pwdLastSet=0))
Пользователи с ограниченным сроком действия учетной записи	(&(sAMAccountType=805306368)(accountExpires>=1)(accountExpires<=9223372036854775806))
Пользователи, созданные за определенный период (формат даты: YYYY MM DD HH mm ss.s Z)	(&(sAMAccountType=805306368)(whenCreated>=20230401000000.0Z<=20230701000000.0Z))
Все компьютеры	(objectCategory=computer)
Все контроллеры домена	(&(objectCategory=computer)(userAccountControl:1.2.840.113556.1.4.803:=8192))
Контроллеры домена, доступные только для чтения	(&(objectCategory=computer)(userAccountControl:1.2.840.113556.1.4.803:=67108864))
Группы в которых нет пользователей	(&(objectCategory=group)!(member=*))
Группы с ключевым словом admin в имени	(&(objectCategory=group)(samaccountname=*admin*))
Все группы безопасности (Security)	(&(objectCategory=group)(groupType:1.2.840.113556.1.4.803:=2147483648))
Все члены группы Sales (без учета вложенности)	(memberOf=CN=Sales,CN=Users,DC=test,DC=alt)

Окончание таблицы 98

Запрос	LDAP фильтр
Все члены группы Sales (с учетом вложенности)	(memberOf:1.2.840.113556.1.4.1941:=CN=Sales,CN=Users,DC=test,DC=alt)
Все группы, в которые входит пользователь testldap	(&(objectCategory=group)(member=CN=testldap,CN=Users,DC=test,DC=alt)))
Все подразделения (OU)	(objectCategory=organizationalUnit)
Все объекты групповой политики	(objectCategory=groupPolicyContainer)
Все отношения доверия	(objectClass=trustedDomain)
Объекты, связанные с ролями FSMO	(fsMORoleOwner=*)
PDC Emulator	(&(objectClass=domainDNS)(fsMORoleOwner=*))
RID Master	(&(objectClass=rIDManager)(fsMORoleOwner=*))
Объект AD с определенным SID	(objectSID=S-1-5-21-1723588197-2340999690-1379671080-1105)

10.6.16.5.2. Формат вывода

Если найдена одна или несколько записей, то каждая запись передается в поток вывода в следующем формате:

```
Отличительное имя (DN)
имя_атрибута: значение
имя_атрибута: значение
имя_атрибута: значение
...
```

Записи разделяются пустыми строками.

Если задан параметр `-t` вместо реальных значений атрибутов будут выводиться URI временных файлов, в которые эти значения помещаются. Если задан параметр `-A`, то будут выводиться только имена атрибутов.

Примечания:

1. Значение атрибута записывается в 7-битной кодировке ASCII и отделяется от его имени символом «:». Значения, не подходящие под эту кодировку, записываются в кодировке base64 и отделяются от имени атрибута символами «::»:

```
имя_атрибута:: base64_значение_атрибута
```

Например:

```
dn::Q0490JfQsNC50YbQtdCy0LAg0J7Qu9GM0LPQsCxDTj1Vc2VycyxEQz10ZXN0LERDPWFsdA==cn:
: 0JfQsNC50YbQtdCy0LAg0J7Qu9GM0LPQsA==
```

```
...
$ echo "0JfQsNC50YbQtdCy0LAg0J7Qu9GM0LPQsA==" | base64 -d
Зайцева Ольга
```

2. Чтобы отобразить строки в кодировке base64 можно использовать следующую команду:

```
$ ldapsearch -LLL -D testldap@test.alt -x -W | perl -MMIME::Base64 -
MEncode=decode -n -00 -e 's/\n +//g;s/(?<=: ) (\S+)/decode("UTF-
8",decode_base64($1))/eg;print'
```

10.6.16.5.3. Примеры

Вывести всех пользователей, фамилия которых начинается с буквы «К»:

```
$ ldapsearch -LLL -H ldap://192.168.0.132:389 \
-D testldap@test.alt -b "dc=test,dc=alt" \
-x -W "(&(sAMAccountName=*) (sn=K*))" cn sn
где:
```

- H ldap://192.168.0.132:389 – сервер LDAP;
- D testldap@test.alt – пользователь с правом чтения в каталоге LDAP;
- b "dc=test,dc=alt" – контейнер AD, в котором будет выполняться поиск;
- x – использовать простую аутентификацию;
- W – спросить пароль;
- "(&(sAMAccountName=*) (sn=K*))" – выражение, по которому будут отфильтрованы результаты;
- cn sn – поля, которые необходимо вывести.

Параметры по умолчанию можно задать в файле `/etc/openldap/ldap.conf`, например:

```
BASE      dc=test,dc=alt
URI       ldap://dc1.test.alt
```

Команда с использованием базы поиска и URI по умолчанию:

```
$ ldapsearch -LLL -D testldap@test.alt \
-x -W "(&(sAMAccountName=*) (sn=K*))" cn sn
```

Вывести фамилию и электронную почту всех пользователей, из подразделения OU, у которых непустое поле mail:

```
$ ldapsearch -LLL -H ldap://192.168.0.132:389 \
-D testldap@test.alt -b "ou=OU,dc=test,dc=alt" -s one \
-x -W "(&(sAMAccountName=*) (mail=K*))" sn mail
```

В данном примере не будут выведены записи только из подразделения OU, но не из его дочерних подразделений.

Считать последовательность строк из файла `new.filter` и выполнить функцию поиска LDAP для каждой строки:

```
$ ldapsearch -H ldap://192.168.0.132:389 \ -D testldap@test.alt -
b "dc=test,dc=alt" -x -W -f new.filter "(samaccountname=%s)" cn
```

Содержимое файла `new.filter`:

```
z*
ivanov
k*
*k
```

Команда выполняет поиск по поддереву для каждого фильтра, начиная с `samaccountname=z*`. Когда этот поиск завершается, начинается поиск для фильтра `cn=ivanov` и т. д.

Пример вывода вышеуказанной команды с параметром `-n`:

```
LDAPv3
# base <dc=test,dc=alt> with scope subtree
# filter pattern: (samaccountname=%s)
# requesting: dn
#
#
# filter: (samaccountname=z*)
#
#
# filter: (samaccountname=ivanov)
#
#
# filter: (samaccountname=k*)
#
#
# filter: (samaccountname=*k)
#
```

10.6.16.6. Команда `sssctl`

`sssctl` — это инструмент командной строки, который предоставляет унифицированный способ получения информации о состоянии Security System Services Daemon (SSSD).

Утилиту `sssctl` можно использовать для сбора информации:

- состоянии домена;
- аутентификации пользователя;
- доступа пользователей к клиентам определенного домена;
- информация о кэшированном содержимом.

С помощью утилиты `sssctl` можно:

- управлять кэшем SSSD;
- управлять журналами;
- проверить конфигурационные файлы.

Основные команды `sssctl` представлены в таблице 99.

Т а б л и ц а 99 – Основные команды `sssctl`

Команда	Описание
Статус SSSD	
<code>domain-list</code>	Вывести список доступных доменов
<code>domain-status</code> домен	Вывести информацию о домене
<code>user-checks</code> пользователь	Вывести информацию о пользователе и проверить аутентификацию
<code>access-report</code> домен	Создание отчета о правилах управления доступом для домена, которые применяются к клиентскому компьютеру (работает только для домена FreeIPA)
Информация о кэшированном содержимом	
<code>user-show</code> пользователь	Информация о кэше пользователя
<code>group-show</code> группа	Информация о кэше группы
<code>netgroup-show</code> группа	Информация о кэше сетевой группы
Инструменты для работы с локальными данными	
<code>client-data-backup</code>	Резервное копирование локальных данных
<code>client-data-restore</code>	Восстановление локальных данных из резервной копии
<code>cache-remove</code>	Резервное копирование локальных данных и удаление кэшированного содержимого
<code>cache-upgrade</code>	Выполнить обновление кеша
<code>cache-expire</code>	Сделать недействительными кэшированные объекты
<code>cache-index</code> действие	Управление индексами кеша
Инструменты для управления журналированием	
<code>logs-remove</code>	Удалить существующие файлы журналов SSSD
<code>logs-fetch</code> файл	Архивировать файлы журналов SSSD в tarball
<code>debug-level</code> [уровень]	Изменить или вывести уровень журналирования SSSD
<code>analyze</code>	Анализ зарегистрированных данных
Инструменты для проверки файлов конфигурации	
<code>config-check</code>	Выполнить статический анализ конфигурации SSSD
<code>cert-show</code> сертификат	Вывести информацию о сертификате
<code>cert-map</code> сертификат	Показать пользователей, привязанных к сертификату

Получить дополнительную информацию можно на справочной странице `sssctl`.

Пример получения дополнительной информации о подкоманде:

```
# sssctl user-show --usage
```

или

```
# sssctl user-show --help
```

Получение информации о домене:

```
# sssctl domain-status TEST.ALT
```

```
Online status: Online
```

```
Active servers:
```

```
AD Global Catalog: dc1.test.alt
```

```
AD Domain Controller: dc1.test.alt
```

```
Discovered AD Global Catalog servers:
```

```
- dc1.test.alt
```

```
Discovered AD Domain Controller servers:
```

```
- dc1.test.alt
```

Показать информацию о кэше пользователя:

```
# sssctl user-show kim
```

```
Name: kim
```

```
Cache entry creation date: 12/28/22 13:39:46
```

```
Cache entry last update time: 06/19/23 09:55:29
```

```
Cache entry expiration time: Expired
```

```
Initgroups expiration time: Expired
```

```
Cached in InfoPipe: No
```

Проверить информацию о пользователе и его учетной записи:

```
# sssctl user-checks kim
```

```
user: kim
```

```
action: acct
```

```
service: system-auth
```

```
SSSD nss user lookup result:
```

```
- user name: kim
```

```
- user id: 1187401107
```

```
- group id: 1187400513
```

```
- gecos: Олег Ким
```

```
- home directory: /home/TEST.ALT/kim
```

```
- shell: /bin/bash
```

```
SSSD InfoPipe user lookup result:
```

```
- name: kim
```

```
- uidNumber: 1187401107
```

```
- gidNumber: 1187400513
```

```
- gecos: Олег Ким
```

```
- homeDirectory: not set
```

```
- loginShell: not set
```

```
testing pam_acct_mgmt
```

```
pam_acct_mgmt: Success
```

```
PAM Environment:
```

```
- no env -
```

10.6.16.7. Команда testparm

С помощью команды testparm можно проверить содержимое файла конфигурации /etc/samba/smb.conf.

Пример проверки настройки Samba:

```
$ testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed

Server role: ROLE_ACTIVE_DIRECTORY_DC

Press enter to see a dump of your service definitions

# Global parameters
[global]
    dns forwarder = 8.8.8.8
    ldap server require strong auth = No
    passdb backend = samba_dsdb
    realm = TEST.ALT
    server role = active directory domain controller
    workgroup = TEST
    rpc_server:tcpip = no
    rpc_daemon:spoolssd = embedded
    rpc_server:spoolss = embedded
    rpc_server:winreg = embedded
    rpc_server:ntsvcs = embedded
    rpc_server:eventlog = embedded
    rpc_server:svrsvc = embedded
    rpc_server:svcctl = embedded
    rpc_server:default = external
    winbindd:use external pipes = true
    idmap_ldb:use rfc2307 = yes
    idmap config * : backend = tdb
    map archive = No
    vfs objects = dfs_samba4 acl_xattr

[dfs]
    msdfs root = Yes
    path = /media/dfsroot

[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

[netlogon]
    path = /var/lib/samba/sysvol/test.alt/scripts
    read only = No

[free]
    guest ok = Yes
    path = /mnt/win/free
    read only = N
```

10.6.17. Конфигурационные файлы

/etc/samba/smb.conf – файл конфигурации Samba.

/etc/krb5.conf – файл конфигурации Kerberos.

10.6.17.1. Файл sssd.conf

/etc/sss/sss.conf – файл конфигурации SSSD.

Для работы с Active Directory в SSSD имеется специальный AD-провайдер sssd-ad.

Минимальный конфигурационный файл (/etc/sss/sss.conf) для sssd-ad:

```
[sss]
config_file_version = 2
services = nss, pam

# Managed by system facility command:
## control sssd-drop-privileges unprivileged|privileged|default
user = _sss

# SSSD will not start if you do not configure any domains.

domains = TEST.ALT
[nss]

[pam]
[domain/TEST.ALT]
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad
default_shell = /bin/bash
fallback_homedir = /home/%d/%u
debug_level = 0
;cache_credentials = true
ad_gpo_ignore_unreadable = true
ad_gpo_access_control = permissive
ad_update_samba_machine_account_password = true
```

Получить подробную информацию можно на справочной странице `man sss.conf`.

10.6.17.2. Файл resolv.conf

/etc/resolv.conf – файл конфигурации резолвера (механизма преобразования имен хостов в адреса IP).

Файл конфигурации резолвера (resolver) содержит информацию, которая считывается функциями разрешения имен при первом их вызове процессом.

Файл разработан в удобочитаемом формате, и содержит список ключевых слов со значениями, которые предоставляют различного рода информацию для функций разрешения имен. Файл настройки считается надежным источником информации DNS (например, информация об AD-бите DNSSEC будет возвращаться в неизменном виде из этого источника).

Если этот файл не существует, то будет опрашиваться только служба имен на локальной машине; доменное имя определяется из имени узла, а список поиска будет содержать это доменное имя.

Обычно в файле `/etc/resolv.conf` указан как минимум 1 сервер имен, на который будут перенаправляться все DNS запросы:

```
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/ifaces/<interface>/resolv.conf instead.
nameserver 192.168.197.241
```

ВАЖНО

Файл `/etc/resolv.conf` не должен редактироваться. Его автоматически генерирует `resolvconf`. Редактировать можно файл `/etc/net/ifaces/<interface>/resolv.conf`.

Поддерживаются следующие параметры настройки:

1) `nameserver` (IP-адрес сервера имен)

Интернет-адрес сервера имен, на который надо переправлять все запросы, либо адрес IPv4 (в точечной нотации), либо адрес IPv6 в нотации с двоеточием (и, возможно, с точками) в соответствии с RFC 2373. Может быть указано до `MAXNS` (в настоящее время 3) серверов имен, ключевое слово должно быть указано для каждого сервера. Если указано несколько серверов, библиотека распознавателя запрашивает их в указанном порядке. Если в файле нет строк `nameserver`, по умолчанию используется сервер имен на локальном компьютере. Используемый алгоритм заключается в том, чтобы попробовать обратиться к первому указанному серверу имен, и, если время ожидания запроса истекло, попробовать обратиться к следующему серверу, и т. д. пока не будет

исчерпан список серверов, а затем повторять попытки, пока не будет сделано максимальное количество повторных попыток;

2) options

Позволяют изменять некоторые внутренние переменные функций определения имен. Синтаксис:

options параметр ...

где параметр может иметь следующие значения:

- attempts:n

Задаёт количество попыток, которое преобразователь предпримет, отправляя запрос на свои серверы имен, прежде чем закончить работу и вернуть ошибку. По умолчанию используется RES_DFLRETRY (в настоящее время равно 2). Значение этого параметра скрыто, ограничено числом 5;

- debug

Устанавливает RES_DEBUG в `_res.options` (эффективно, только если `glibc` был собран с поддержкой отладки);

- edns0 (начиная с `glibc 2.6`)

Задаёт значение RES_USE_EDNSO в `_res.options`. Включает поддержку расширений DNS, описанных в RFC 2671;

- inet6

Задаёт значение RES_USE_INET6 в `_res.options`. Это приводит к выполнению запроса AAAA перед запросом A внутри функции `gethostbyname`, и отображению ответов IPv4 в «туннелированной форме» IPv6, если записи AAAA не были найдены, но существует набор записей A. Начиная с `glibc 2.25`, эта опция устарела; приложения должны использовать `getaddrinfo`, а не `gethostbyname`;

- ip6-bytestring (с `glibc 2.3.4` до `glibc 2.24`)

Задаёт значение RES_USE_BSTRING в `_res.options`. Это приводит к поиску обратной записи IPv6, с использованием формата значимых

битов, описанного в RFC 2673; если этот параметр не установлен (по умолчанию);

- `ndots:n`

Задаёт минимальное количество точек, которые должны обязательно присутствовать в имени, переданном функции `res_query` (см. `resolver(3)`), прежде чем будет сделан первоначальный абсолютный запрос. По умолчанию `n` равно 1, поэтому если в имени есть точки, сначала имя пытаются разрешить как абсолютное, прежде чем добавлять к нему элементы из списка поиска. Значение этой опции скрыто и ограничено числом 15;

- `no-check-names`

Задаёт значение `RES_NOCHECKNAME` в `_res.options`, что приводит к отключению в современном BIND проверки в поступающих именах узлов и почтовых именах недопустимых символов, таких как символы подчеркивания (`_`), не-ASCII или управляющие символы;

- `no-reload` (начиная с `glibc 2.16`)

Задаёт значение `RES_NORELOAD` в `_res.options`. Эта опция отключает автоматическую перезагрузку измененного файла конфигурации;

- `no-tld-query` (начиная с `glibc 2.14`)

Задаёт значение `RES_NOTLDQUERY` в `_res.options`. Этот параметр указывает `res_nsearch()` не пытаться разрешить неполное имя, как если бы оно было доменом верхнего уровня. Данный параметр может привести к проблемам, если в качестве TLD указано «localhost», а не `localhost` в одном или более элементах списка поиска.

Данный параметр не действует, если не установлен `RES_DEFNAMES` или `RES_DNSRCH`;

- rotate

Задает значение RES_ROTATE в `_res.options`, что приводит к циклическому выбору указанных серверов имен. Без этой опции распознаватель всегда будет запрашивать первый сервер имен в списке и использовать последующий сервер имен только в случае сбоя первого. Эта опция позволяет распределить нагрузку между разными серверами имен;

- single-request-reopen (начиная с glibc 2.9)

Задает RES_SNGLKUPREOP в `_res.options`. Для разрешения имен используется единый сокет для запросов А и АААА. Некоторое оборудование ошибочно возвращает только один ответ. Когда это происходит, клиент продолжает ждать второго ответа.

Указание этого параметра изменяет это поведение так, что если два запроса с одного порта не обрабатываются правильно, то сокет будет закрыт и открыт новый перед посылкой второго запроса;

- single-request (начиная с glibc 2.10)

Задает значение RES_SNGLKUP в `_res.options`. По умолчанию glibc, начиная с версии 2.9, выполняет поиск по IPv4 и IPv6 параллельно.

Некоторые приложения DNS-серверов не могут обработать такие запросы должным образом и делают паузу между ответами на запрос. Этот параметр отключает данное поведение, что заставляет glibc делать запросы IPv6 и IPv4 последовательно (за счет некоторого замедления процесса разрешения имени);

- timeout:n

Задает промежуток времени, который функции определения имен будут ждать ответа от удаленного сервера имен перед тем как повторить запрос другому серверу имен.

Это время может не совпадать с общим временем, затраченным на любой вызов API-интерфейса преобразователя, и нет гарантии, что

один вызов API-интерфейса преобразователя соответствует одному тайм-ауту. Измеряется в секундах, значение по умолчанию – RES_TIMEOUT (в настоящее время равно 5). Значение этой опции скрыто и ограничено числом 30;

- trust-ad (начиная с glibc 2.31)

Задает значение RES_TRUSTAD в `_res.options`. Этот параметр управляет поведением бита AD распознавателя-заглушки. Если проверяющий преобразователь устанавливает в ответе бит AD, это означает, что данные в ответе были проверены в соответствии с протоколом DNSSEC. Чтобы полагаться на бит AD, локальная система должна доверять как распознавателю, проверяющему DNSSEC, так и сетевому пути к нему, поэтому требуется явное согласие. Если активна опция `trust-ad`, тупиковый распознаватель устанавливает бит AD в исходящих DNS-запросах (чтобы включить поддержку бита AD) и сохраняет бит AD в ответах. Без этой опции бит AD в запросах не устанавливается и всегда удаляется из ответов, прежде чем они будут возвращены приложению. Это означает, что приложения могут доверять биту AD в ответах, если параметр `trust-ad` установлен правильно.

В glibc версии 2.30 и более ранних AD не устанавливается автоматически в запросах и без изменений передается приложениям в ответах;

- use-vc (начиная с glibc 2.14)

Задает значение RES_USEVC в `_res.options`. Данный параметр включает принудительное использование TCP для запросов DNS;

- search (список поиска)

По умолчанию список поиска содержит одну запись – имя локального домена. Он определяется по локальному имени хоста, возвращаемому функцией `gethostname`; локальным доменным именем считается все, что следует после первого знака «.». Если имя хоста не содержит «.»,

предполагается, что корневой домен является именем локального домена.

Это поведение можно изменить, перечислив имена доменов, в которых нужно вести поиск, после ключевого слова `search` через пробел или символ табуляции. При разрешении запросов имен, в которых меньше точек чем указано в `ndots` (по умолчанию 1), будет использован каждый компонент пути поиска пока не будет найдено соответствующее имя. Для сред с несколькими субдоменами см. параметры `ndots:n` выше, чтобы избежать атак типа «человек посередине» и ненужного трафика для корневых DNS-серверов. Обратите внимание, что этот процесс может быть медленным и будет генерировать много сетевого трафика, если серверы для перечисленных доменов не являются локальными, и что время ожидания запросов истечет, если сервер для одного из доменов недоступен.

При наличии нескольких директив `search` используется только список поиска из последнего экземпляра.

Список поиска может содержать не более шести доменов и не может быть длиннее 256 символов. В `glibc 2.25` и более ранних версиях список поиска мог содержать не более шести доменов и не мог быть длиннее 256 символов. Начиная с `glibc 2.26` список поиска не ограничен.

Директива `domain` – это устаревшее название директивы `search`, которая обрабатывает только одну запись в списке поиска;

- `sortlist`

Позволяет сортировать адреса, возвращаемых функцией `gethostbyname`. Список сортировки задается в виде пар IP-адрес/сетевая маска. Маску сети указывать не обязательно, по умолчанию используется естественная маска сети. IP-адрес и маска сети разделяются косой чертой. В списке можно указывать до 10 пар.

Пример:

```
sortlist 130.155.160.0/255.255.240.0 130.155.0.0
```

Ключевое слово `search` системного файла `resolv.conf` можно переопределить для каждого процесса, задав для переменной среды `LOCALDOMAIN` список доменов поиска, разделенных пробелами.

Ключевое слово `options` системного файла `resolv.conf` можно переопределить для каждого процесса, задав для переменной среды `RES_OPTIONS` список параметров преобразователя, разделенных пробелами.

Любые изменения, внесенные вручную в файл конфигурации `/etc/resolv.conf`, обязательно будут перезаписаны при изменениях в сети или перезагрузке системы.

Ключевое слово и значение должны находиться в одной строке, и кроме того, строка должна начинаться с ключевого слова (например, `nameserver`). Значение следует за ключевым словом, разделенным пробелом.

Строки, начинающиеся с точки с запятой (;) или решетки (#), считаются комментариями.

`Resolvconf` — это платформа для обновления системной информации о серверах DNS. Он настраивается как посредник между программами, которые предоставляют эту информацию и программами, которые используют эту информацию.

Обновить файл `/etc/resolv.conf`, чтобы внести изменения в DNS:

```
# resolvconf -u
```

Пример файла `/etc/resolv.conf`:

```
search test.alt example.test
nameserver 192.168.0.132
nameserver 8.8.8.8
```

Запись `search` позволяет использовать в качестве адреса только хост-имя для компьютеров в домене `test.alt`. Например, чтобы обратиться системе `work.test.alt`, пользователь должен ввести в качестве адреса только хост-имя, `work`. Когда преобразователь пытается разрешить доменное имя, например, `work`, он сначала формирует полное доменное имя, используя имя домена `test.alt`, в `work.test.alt` и выполняет DNS-запрос, используя это полное доменное имя. Если это не удастся, то преобразователь пробует следующий в очереди домен и запрашивает IP-адрес `work.example.test`.

При этом, когда преобразователь пытается разрешить доменное имя `work.ru`, он сначала запросит `work.ru` как абсолютное доменное имя. Если DNS не сможет разрешить его, то только тогда преобразователь объединит его с поисковым доменом, чтобы сформировать `work.ru.test.alt`, и повторит запрос.

Решение о том, выполняется ли первый запрос как абсолютное доменное имя или нет, полностью зависит от количества точек, присутствующих в доменном имени. По умолчанию доменное имя, содержащее по крайней мере 1 точку, заставит преобразователь запрашивать его дословно, не объединяя его с какими-либо поисковыми доменами. Количество точек для первого запроса абсолютного доменного имени настраивается в значении параметра `ndots`.

11. SOGO

SOGGo – сервер групповой работы, аналогичный Microsoft Exchange, с веб-интерфейсом и доступом по MAPI для Microsoft Outlook.

SOGGo обеспечивает веб-интерфейс на основе AJAX и поддерживает различные нативные клиенты с помощью стандартных протоколов.

Возможности SOGO:

- общие почтовые папки, календари и адресные книги;
- веб-интерфейс, аналогичный Outlook Web Access;
- поддержка протоколов CalDAV, CardDAV, GroupDAV, Microsoft ActiveSync, IMAP и SMTP;
- доступ по MAPI для Microsoft Outlook, не требующий внешних модулей;
- делегирование, уведомления, резервирование, поддержка категорий и почтовых фильтров;
- поддержка нескольких почтовых ящиков в веб-интерфейсе;
- Single sign-on с помощью CAS, WebAuth или Kerberos.

⚠ MAPI over HTTPS не поддерживается.

11.1. Установка

Для установки SOGO на ОС Альт СП Сервер (64 бит (x86_64), AArch64 (ARMv8)) нужно выполнить команду (драйвер к PostgreSQL будет установлен автоматически):

```
# apt-get install task-sogo
```

11.2. Подготовка среды

Подготовить к запуску и настроить службы PostgreSQL (первые два шага нужно делать, если системные базы еще не инициировались):

- создать системные базы данных (пароль пользователя PostgreSQL необходимо запомнить):

```
# /etc/init.d/postgresql initdb
```

Введите новый пароль суперпользователя:

Повторите его:

- запустить службу:

```
# systemctl start postgresql
```

- создать пользователя sogo и базу данных sogo (при запросе «Пароль» следует ввести пароль пользователя postgresql, созданный при создании системных баз данных):

```
# su - postgres -s /bin/sh -c 'createuser --no-superuser --no-createdb --no-createrole sogo'
```

Пароль:

```
# su - postgres -s /bin/sh -c "psql -c \"ALTER USER sogo WITH PASSWORD '1q2w3e4r';\""
```

Пароль пользователя postgres:

```
ALTER ROLE
```

```
# su - postgres -s /bin/sh -c 'createdb -O sogo sogo'
```

Пароль:

```
# systemctl restart postgresql
```

Настройка Samba DC:

1) пользователи расположены в домене AD, расположенном на контроллере с Samba DC. Сервер Samba AD DC должен быть предварительно развернут (см. раздел 10);

2) создать в домене пользователя sogo с паролем Pa\$\$word (при запросе дважды ввести пароль):

```
# samba-tool user create sogo
```

```
# samba-tool user setexpiry --noexpiry sogo
```

Настройка SOGo (настраивается на домен test.alt):

3) заполнить файл конфигурации /etc/sogo/sogo.conf:

```
{
  SOGoProfileURL = "postgresql://sogo:1q2w3e4r@localhost/sogo/sogo_user_profile";
  OCSEFolderInfoURL = "postgresql://sogo:1q2w3e4r@localhost/sogo/sogo_folder_info";
  OCSSessionsFolderURL = "postgresql://sogo:1q2w3e4r@localhost/sogo/sogo_sessions_folder";
  OCSEMailAlarmsFolderURL = "postgresql://sogo:1q2w3e4r@localhost/sogo/sogo_alarms_folder";
  SOGoEnableEMailAlarms = YES;
  SOGoDraftsFolderName = Drafts;
  SOGoSentFolderName = Sent;
  SOGoTrashFolderName = Trash;
  SOGoIMAPServer = "imaps://localhost:993/?tlsVerifyMode=allowInsecureLocalhost";
  SOGoMailingMechanism = sendmail;
  SOGoForceExternalLoginWithEmail = NO;
  NGImap4ConnectionStringSeparator = "/";
  SOGoUserSources = (
    {
      id = sambaLogin;
      displayName = "SambaLogin";
      canAuthenticate = YES;
      type = ldap;
      CNFieldName = cn;
    }
  )
}
```

```

IDFieldName = cn;
UIDFieldName = sAMAccountName;
hostname = "ldaps://127.0.0.1";
baseDN = "CN=Users,DC=test,DC=alt";
bindDN = "CN=sogo,CN=Users,DC=test,DC=alt";
bindPassword = "Pa$$word";
bindFields = (sAMAccountName);
},
{
  id = sambaShared;
  displayName = "Shared Addressbook";
  canAuthenticate = NO;
  isAddressBook = YES;
  type = ldap;
  CNFieldName = cn;
  IDFieldName = mail;
  UIDFieldName = mail;
  hostname = "ldaps://127.0.0.1";
  baseDN = "CN=Users,DC=test,DC=alt";
  bindDN = "CN=sogo,CN=Users,DC=test,DC=alt";
  bindPassword = "Pa$$word";
  filter = "(NOT isCriticalSystemObject='TRUE') AND (mail='*') AND (NOT
objectClass=contact)";
},
{
  id = sambaContacts;
  displayName = "Shared Contacts";
  canAuthenticate = NO;
  isAddressBook = YES;
  type = ldap;
  CNFieldName = cn;
  IDFieldName = mail;
  UIDFieldName = mail;
  hostname = "ldaps://127.0.0.1";
  baseDN = "CN=Users,DC=test,DC=alt";
  bindDN = "CN=sogo,CN=Users,DC=test,DC=alt";
  bindPassword = "Pa$$word";
  filter = "(((objectClass=person) AND (objectClass=contact) AND
((uidNumber>=2000) OR (mail='*')))
AND (NOT isCriticalSystemObject='TRUE') AND (NOT
showInAdvancedViewOnly='TRUE') AND (NOT uid=Guest))
OR (((objectClass=group) AND (gidNumber>=2000)) AND (NOT
isCriticalSystemObject='TRUE') AND (NOT showInAdvancedViewOnly='TRUE'))";
  mapping = {
    displayname = ("cn");
  };
}
);
SOGoSieveScriptsEnabled = YES;
SOGOLanguage = Russian;
SOGOTimeZone = Europe/Moscow;
SOGOFirstDayOfWeek = 1;
}

```

4) включить службы по умолчанию и перезапустить их:

```
# for service in samba postgresql memcached sogo httpd2; do
systemctl restart $service; done
```

Возможные ошибки будут записаны в файл журнала

/var/log/sogo/sogo.log.

11.3. Включение веб-интерфейса

Для включения веб-интерфейса нужно выполнить команды:

```
# for mod in proxy proxy_http authn_core authn_file auth_basic
authz_user env dav headers rewrite version setenvif; do a2enmod $mod;
done
# a2ensite SOGo
# systemctl restart httpd2 sogo
```

Веб-интерфейс SOGo (рис. 506) будет доступен по адресу:

`http://<адрес_сервера>/SOGo/`.



Рис. 506 – Форма входа в веб-интерфейс SOGo

Примечание. Если при входе в веб-интерфейс возникает ошибка «Неправильный логин или пароль» и в логах `/var/log/sogo/sogo.log` есть ошибки вида:

```
Jul 06 16:14:51 sogo [12257]: [ERROR]
<0x0x5578db070b40[LDAPSource]>
Could not bind to the LDAP server ldaps://127.0.0.1 (389) using
the
bind DN: CN=sogo,CN=Users,DC=test,DC=alt
```

следует в файл `/etc/openldap/ldap.conf` добавить опцию `TLS_REQCERT allow` и перезапустить службы `samba` и `sogo`:

```
# systemctl restart samba sogo
```

11.4. Настройка электронной почты

⚠ Предварительно должен быть настроен DNS (см. п. 13).

Для использования электронной почты в SOGo (рис. 507) нужно настроить аутентификацию в AD для Postfix и Dovecot.

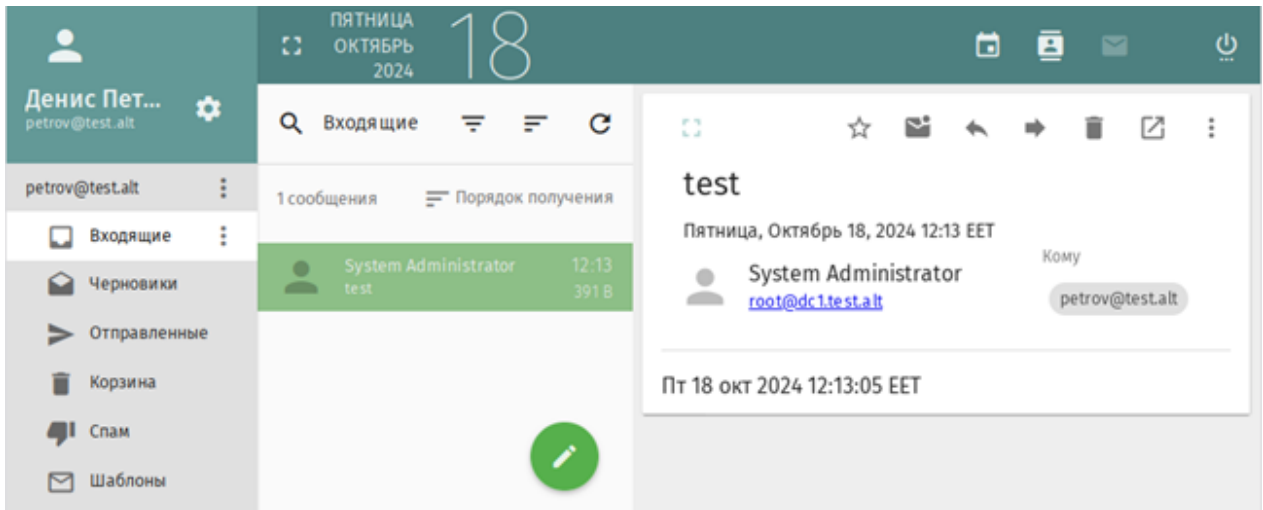


Рис. 507 – Использование электронной почты в SOGo

В примере используется следующая конфигурация:

- имя домена: test.alt;
- размещение почты: `/var/mail/<имя_домена>/<имя_пользователя>` (формат maildir);
- доступ на чтение почты: IMAP (порт 993), SSL;
- доступ на отправку почты: SMTP (порт 465), SSL/STARTTLS;
- данные аутентификации: email с доменом (например, petrov@test.alt) или имя пользователя.

Примечание. У пользователей SambaDC должен быть указан атрибут `mail-address`. Указать атрибут `mail-address` можно, например, при создании учетной записи:

```
# samba-tool user create petrov --mail-address='petrov@test.alt'
# samba-tool user create ivanov --mail-address='ivanov@test.alt'
```

⚠ Доступ к серверу LDAP осуществляется по протоколу `ldap` без шифрования. Для контроллера домена SambaDC нужно отключить `ldaps` в `/etc/samba/smb.conf` в секции `[global]`:

```
ldap server require strong auth = no и перезапустить samba:
# service samba restart
```

Предварительно нужно создать пользователя vmail (пароль Pa\$\$word) с истекающей учетной записью:

```
# samba-tool user create -W Users vmail
# samba-tool user setexpiry vmail --noexpiry
```

11.4.1. Настройка Postfix

Установить пакет postfix-ldap:

```
# apt-get install postfix-ldap
```

При настройке Postfix и Dovecot без сервиса групповой работы SOGo следует установить пакет postfix-dovecot:

```
# apt-get install postfix-dovecot
```

В каталоге /etc/postfix изменить файлы для домена test.alt:

- изменить содержимое файла main.cf:

```
# Global Postfix configuration file. This file lists only a small subset
# of all parameters. For the syntax, and for a complete parameter list,
# see the postconf(5) manual page. For a commented and more complete
# version of this file see /etc/postfix/main.cf.dist
mailbox_command = /usr/libexec/dovecot/dovecot-lda -f "$SENDER" -a
"$RECIPIENT"
inet_protocols = ipv4

# Mappings
virtual_mailbox_base = /var/mail
virtual_mailbox_domains = test.alt
virtual_mailbox_maps = ldap:/etc/postfix/ad_local_recipients.cf
virtual_alias_maps = ldap:/etc/postfix/ad_mail_groups.cf
virtual_transport = dovecot
local_transport = virtual
local_recipient_maps = $virtual_mailbox_maps

# SSL/TLS
smtpd_use_tls = yes
smtpd_tls_security_level = encrypt
#smtpd_tls_security_level = may
smtpd_sasl_auth_enable = yes
smtpd_sasl_local_domain = test.alt
smtpd_sasl_path = private/auth
smtpd_sasl_type = dovecot
smtpd_sender_login_maps = ldap:/etc/postfix/ad_sender_login.cf
smtpd_tls_auth_only = yes
smtpd_tls_cert_file = /var/lib/ssl/certs/dovecot.cert
smtpd_tls_key_file = /var/lib/ssl/private/dovecot.key
smtpd_tls_CAfile = /var/lib/ssl/certs/dovecot.pem

smtpd_recipient_restrictions = permit_mynetworks, reject_unauth_destination,
per-mit_sasl_authenticated, reject
smtpd_sender_restrictions = reject_authenticated_sender_login_mismatch
```

- файл /etc/postfix/mydestination должен быть пустым;

- в файл `master.cf` нужно добавить строки:

```
dovecot unix - n n - - pipe
  flags=DRhu user=mail:mail argv=/usr/libexec/dovecot/deliver -d
  ${recipient}
smtps inet n - n - - smtpd
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
```

- создать файл `ad_local_recipients.cf`:

```
version = 3
server_host = test.alt:389
search_base = dc=test,dc=alt
scope = sub
query_filter = (&(|(mail=%s)(otherMailbox=%u@d))(sAMAccountType=805306368))
result_filter = %s
result_attribute = mail
special_result_attribute = member

bind = yes
bind_dn = cn=vmail,cn=users,dc=test,dc=alt
bind_pw = Pa$$word
```

- создать файл `ad_mail_groups.cf`:

```
version = 3
server_host = test.alt:389
search_base = dc=test,dc=alt
timeout = 3
scope = sub
query_filter = (&(mail=%s)(sAMAccountType=268435456))
result_filter = %s
result_attribute = mail
special_result_attribute = member

bind = yes
bind_dn = cn=vmail,cn=users,dc=test,dc=alt
bind_pw = Pa$$word
```

- создать файл `ad_sender_login.cf`:

```
version = 3
server_host = test.alt:389
search_base = dc=test,dc=alt
scope = sub
query_filter = (&(objectClass=user)(|(sAMAccountName=%s)(mail=%s)))
result_attribute = mail

bind = yes
bind_dn = cn=vmail,cn=users,dc=test,dc=alt
bind_pw = Pa$$word
```

- перезапустить службу postfix:

```
# systemctl restart postfix
```

Проверка конфигурации Postfix (в выводе не должно быть никаких сообщений):

```
# postconf >/dev/null
```

Проверка пользователя почты petrov:

```
# postmap -q petrov@test.alt ldap:/etc/postfix/ad_local_recipients.cf
petrov@test.alt
```

Проверка входа:

```
# postmap -q petrov@test.alt ldap:/etc/postfix/ad_sender_login.cf
petrov@test.alt
```

Проверка общего адреса e-mail:

```
# samba-tool group add --mail-address=sales@test.alt Sales
Added group Sales
# samba-tool group addmembers Sales ivanov,petrov
Added members to group Sales
# postmap -q sales@test.alt ldap:/etc/postfix/ad_mail_groups.cf
sales@test.alt,ivanov@test.alt,petrov@test.alt
```

11.4.2. Настройка Dovecot

Установить Dovecot:

```
# apt-get install dovecot
```

Изменить файлы для домена test.alt:

- создать файл /etc/dovecot/dovecot-ldap.conf.ext:

```
hosts          = test.alt:3268
ldap_version   = 3
auth_bind      = yes
dn             = cn=vmail,cn=Users,dc=test,dc=alt
dnpass         = Pa$$word
base          = cn=Users,dc=test,dc=alt
scope         = subtree
deref         = never
user_filter    = (&(objectClass=user)(|(mail=%Lu)(sAMAccountName=%Lu)))
user_attrs    = =uid=8,gid=12,mail=user
pass_filter    = (&(objectClass=user)(|(mail=%Lu)(sAMAccountName=%Lu)))
pass_attrs    = mail=user
```

- изменить файл /etc/dovecot/conf.d/10-auth.conf:

```
auth_mechanisms = plain
!include auth-ldap.conf.ext
```

- изменить файл /etc/dovecot/conf.d/10-mail.conf:

```
mail_location = maildir:/var/mail/%d/%n:UTF-8:INBOX=/var/mail/%d/%n/Inbox
mail_uid      = mail
mail_gid      = mail
first_valid_uid = 5
first_valid_gid = 5
```


- **изменить файл** /etc/dovecot/conf.d/10-master.conf:

```
service imap-login {
    inet_listener imap {
        port = 0
    }
    inet_listener imaps {
    }
}
service pop3-login {
    inet_listener pop3 {
        port = 0
    }
    inet_listener pop3s {
        port = 0
    }
}
service lmtp {
    unix_listener lmtp {
    }
}
service imap {
}
service pop3 {
}
service auth {
    unix_listener auth-userdb {
    }
    unix_listener /var/spool/postfix/private/auth {
        mode = 0600
        user = postfix
        group = postfix
    }
}
service auth-worker {
}
service dict {
    unix_listener dict {
    }
}
```

- **изменить файл** /etc/dovecot/conf.d/15-lda.conf:

```
protocol lda {
    hostname = test.alt
    postmaster_address = administrator@test.alt
}
```

- **изменить файл** /etc/dovecot/conf.d/15-mailboxes.conf:

```
namespace inbox {
    inbox = yes
    mailbox Drafts {
        auto = subscribe
        special_use = \Drafts
    }
    mailbox Junk {
        auto = subscribe
        special_use = \Junk
    }
}
```

```

}
mailbox Trash {
    auto = subscribe
    special_use = \Trash
}
mailbox Sent {
    auto = subscribe
    special_use = \Sent
}
mailbox "Sent Messages" {
    special_use = \Sent
}
}

```

- создать файл /etc/dovecot/conf.d/10-stats.conf:

```

service stats {
    unix_listener stats-reader {
        user = mail
        group = mail
        mode = 0660
    }

    unix_listener stats-writer {
        user = mail
        group = mail
        mode = 0660
    }
}

```

- перезапустить службу dovecot:

```
# systemctl restart dovecot
```

Проверка конфигурации Dovecot (в выводе не должно быть никаких сообщений):

```
# doveconf >/dev/null
```

11.4.3. Безопасность

Так как конфигурационные файлы содержат пароль пользователя LDAP, их нужно сделать недоступным для чтения прочим пользователям:

```

# chown dovecot:root /etc/dovecot/dovecot-ldap.conf.ext
# chmod 0640 /etc/dovecot/dovecot-ldap.conf.ext
# chown root:postfix /etc/postfix/ad_local_recipients.cf
/etc/postfix/ad_mail_groups.cf /etc/postfix/ad_sender_login.cf
# chmod 0640 /etc/postfix/ad_local_recipients.cf
/etc/postfix/ad_mail_groups.cf /etc/postfix/ad_sender_login.cf

```

Перезапустить службы:

```
# systemctl restart dovecot postfix
```

11.4.4. Проверка конфигурации

Проверка SMTP:

```
# date | mail -s test petrov@test.alt
# mailq
Mail queue is empty
```

Проверка IMAP (выход по «Ctrl+D»):

```
# openssl s_client -crlf -connect test.alt:993
...
tag login petrov@test.alt Pa$$word
tag OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID
ENABLE
IDLE      SORT      SORT=DISPLAY      THREAD=REFERENCES      THREAD=REFS
THREAD=ORDEREDSUBJECT
MULTIAPPEND  URL-PARTIAL  CATENATE  UNSELECT  CHILDREN  NAMESPACE
UIDPLUS
LIST-EXTENDED  I18NLEVEL=1  CONDSTORE  QRESYNC  ESEARCH  ESORT
SEARCHRES
WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE] Logged in
```

где `dc1.test.alt` – имя узла сервера SOGo.

11.4.5. Настройка автоответчика, переадресации и фильтрации

В данном разделе рассмотрен процесс конфигурирования Dovecot с плагином Sieve, для возможности фильтрации и переадресации писем.

Настройка Dovecot:

- в файле `/etc/dovecot/conf.d/dovecot.conf` указать используемые протоколы:

```
protocols = imap lmtp submission sieve
```

- в файл `/etc/dovecot/conf.d/10-mail.conf` добавить опцию `mail_home` с указанием пути до каталогов с почтой:

```
mail_location = maildir:/var/mail/%d/%n:UTF-8:INBOX=/var/mail/%d/%n/Inbox
mail_uid = mail
mail_gid = mail
first_valid_uid = 5
first_valid_gid = 5
mail_home = /var/mail/%d/%n
```

переменные %d и %u указывают на имя домена и имя учетной записи;

- в файле /etc/dovecot/conf.d/15-lda.conf в раздел protocol lda добавить плагин sieve:

```
mail_plugins = $mail_plugins sieve
```

- в файле /etc/dovecot/conf.d/20-lmtp.conf в разделе protocol lmtp также указать плагин sieve:

```
mail_plugins = $mail_plugins sieve
```

- в файле /etc/dovecot/conf.d/20-managesieve.conf раскомментировать строку:

```
protocols = $protocols sieve
```

- в файле /etc/dovecot/conf.d/90-sieve.conf закомментировать строку sieve = file:~/sieve;active=~/.dovecot.sieve и добавить новое ее значение:

```
#sieve = file:~/sieve;active=~/.dovecot.sieve
```

```
sieve = file:/var/mail/%Ld/%n/sieve;active=/var/mail/%Ld/%n/active.sieve
```

- в этом же файле раскомментировать опцию sieve_extensions и привести ее к виду:

```
sieve_extensions = +notify +imapflags +vacation-seconds  
+vacation +date +relational
```

- в файле /etc/dovecot/conf.d/10-auth.conf подключить master-users:

```
!include auth-master.conf.ext
```

- в файле /etc/dovecot/master-users создать запись:

```
my_master_user@non-exist.com:{PLAIN}password:::::
```

Должно быть обязательно указано несуществующее имя домена. В реальных условиях необходимо использовать хеш пароля (например, doveadm pw -s SSHA512).

- в файле /etc/sogo/sieve.creds указать эти данные в виде:

```
my_master_user@non-exist.com:password
```

- в начало файла /etc/cron.d/sogo дописать:

```
MAILTO=""
```

- в этом же файле раскомментировать строку:

```
*/5 * * * * _sogo /usr/sbin/sogo-tool update-autoreply -p  
/etc/sogo/sieve.creds
```

В SOGo необходимо активировать окно настроек почтовых фильтров (параметр `SOGoSieveScriptsEnabled`), окно настроек сообщений об отпуске (параметр `SOGoVacationEnabled`), а также окно настроек адресов электронной почты для пересылки (параметр `SOGoForwardEnabled`). Для этого в файл конфигурации `/etc/sogo/sogo.conf` добавить строки:

```
SOGoSieveScriptsEnabled = YES;  
SOGoVacationEnabled = YES;  
SOGoForwardEnabled = YES;  
SOGoSieveFolderEncoding = UTF-8;
```

Перезапустить службы:

```
# systemctl restart postfix dovecot sogo
```

В результате в веб-интерфейсе SOGo в настройках почты появятся три дополнительные вкладки (рис. 508). На вкладке «Фильтры» (рис. 509) можно создавать фильтры и устанавливать критерии, по которым они должны работать. На вкладке «Отпуск» (рис. 510) можно настроить автоответ на время отпуска. На вкладке «Пересылка» (рис. 511) настраивается переадресация электронной почты.

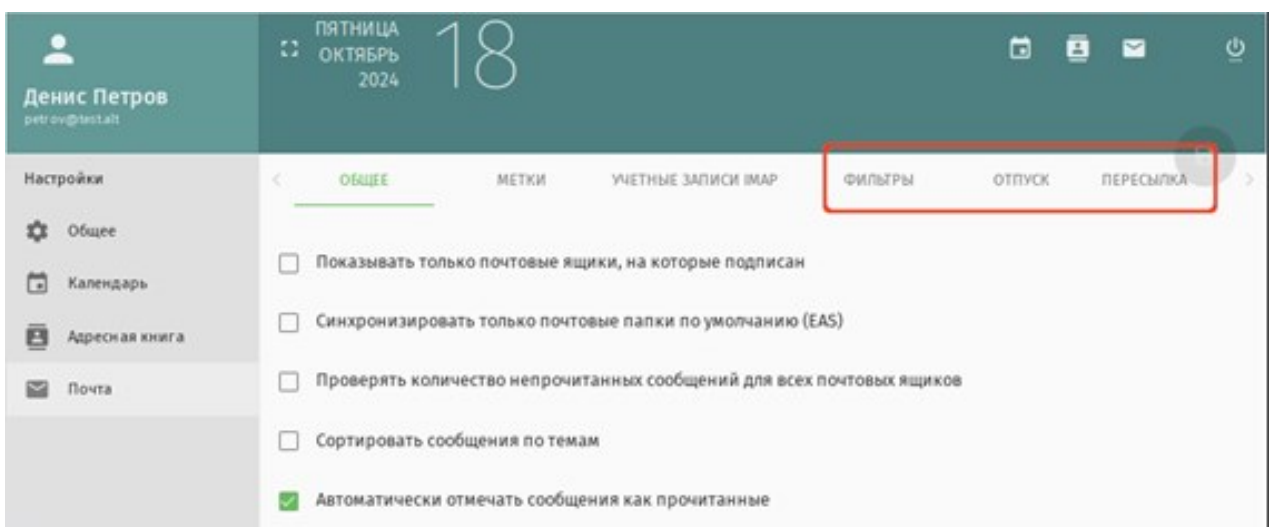


Рис. 508 – SOGo. Настройки почты

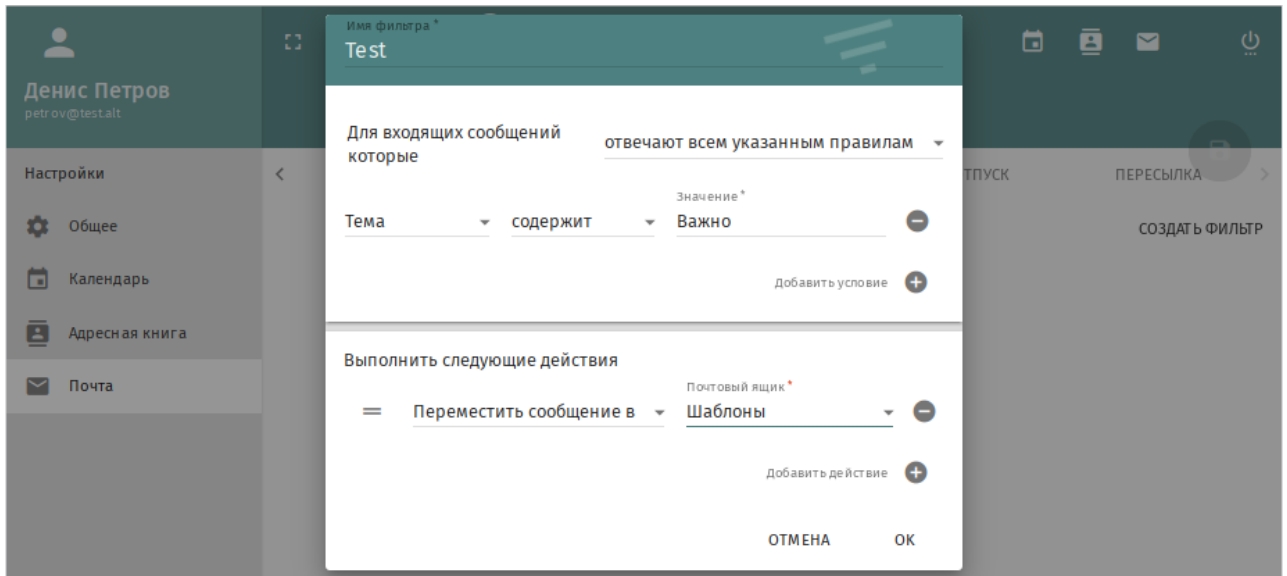


Рис. 509 – SOGo. Настройка фильтра

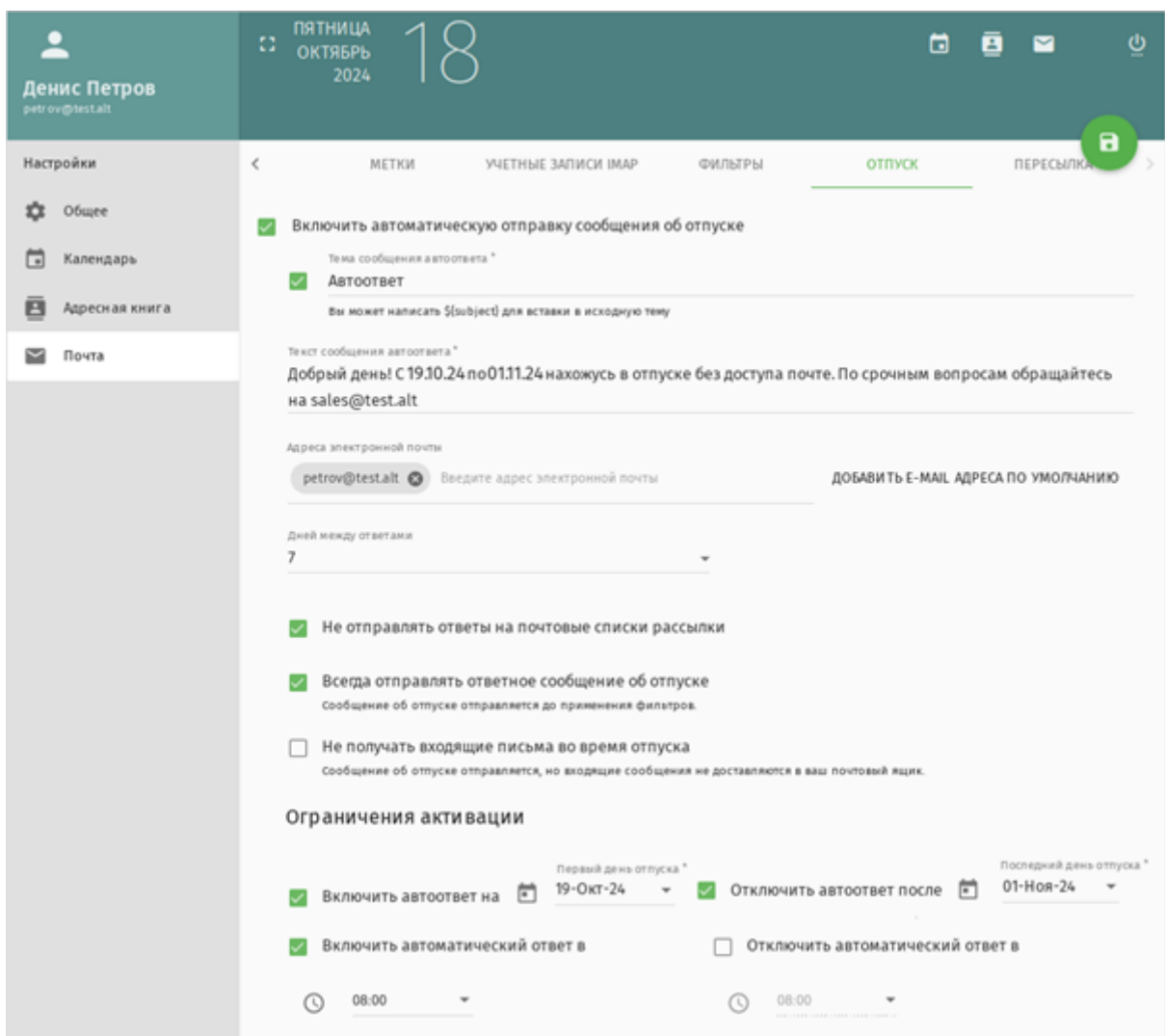


Рис. 510 – SOGo. Настройки автоответа на период отпуска

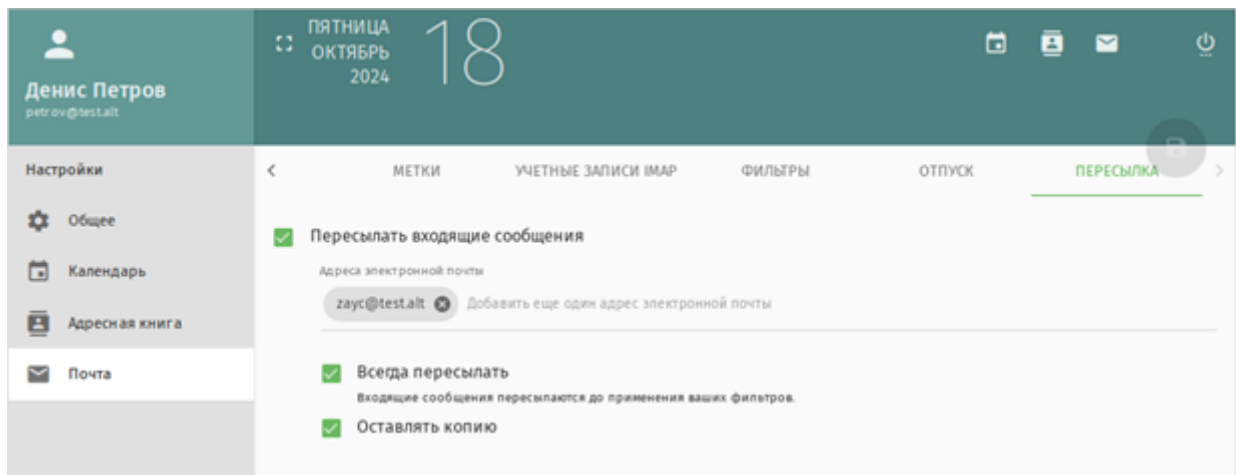


Рис. 511 – SOGo. Настройка переадресации электронной почты

12. FREEIPA

FreeIPA – это комплексное решение по управлению безопасностью Linux-систем, 389 Directory Server, MIT Kerberos, NTP, DNS, Dogtag, состоит из веб-интерфейса и интерфейса командной строки.

FreeIPA является интегрированной системой проверки подлинности и авторизации в сетевой среде Linux, FreeIPA-сервер обеспечивает централизованную проверку подлинности, авторизацию и контроль за аккаунтами пользователей сохраняя сведения о пользователе, группах, узлах и других объектах, которые требуются для обеспечения сетевой безопасности.

12.1. Установка сервера FreeIPA

В качестве примера показана установка сервера FreeIPA со встроенным DNS сервером и доменом EXAMPLE.TEST в локальной сети 192.168.0.0/24. В примере для установки сервера используется узел: ipa.example.test (192.168.0.113).

Для корректной работы сервера должны соблюдаться следующие условия:

- для сервера должно быть задано полное доменное имя (FQDN);
- IP-адрес сервера не должен изменяться;
- в настройках сетевого интерфейса должен быть указан собственный IP-адрес в качестве первичного DNS.

Если настройка FreeIPA выполняется не сразу после установки ОС, во избежание конфликтов с разворачиваемым tomcat необходимо отключить ahttpd, работающий на порту 8080, а также отключить HTTPS в Apache2 (если Apache2 установлен):

```
# systemctl stop ahttpd
# a2dissite 000-default_https
# a2disport https
# service httpd2 condreload
```

Установить пакеты:

```
# apt-get install freeipa-server freeipa-server-dns
```

Задать имя сервера:

```
# hostnamectl set-hostname ipa.example.test
```


Примечание. После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы нужно перезагрузить систему.

Команда установки сервера FreeIPA, со встроенным DNS-сервером, автоматическим обнаружением обратных зон DNS и с настройкой сервера пересылок, в пакетном режиме:

```
# ipa-server-install -U --hostname=$(hostname) \  
-r EXAMPLE.TEST -n example.test -p 12345678 -a 12345678 \  
--setup-dns --forwarder 8.8.8.8 --auto-reverse
```

Для пакетной установки необходимо указать следующие параметры:

- -r REALM_NAME – имя области Kerberos для сервера FreeIPA;
- -n DOMAIN_NAME – доменное имя;
- -p DM_PASSWORD – пароль, который будет использоваться сервером каталогов для менеджера каталогов (DM);
- -a ADMIN_PASSWORD – пароль пользователя admin, администратора FreeIPA;
- -U – позволить процессу установки выбрать параметры по умолчанию, не запрашивая у пользователя информацию;
- --hostname=HOST_NAME – полное DNS-имя этого сервера.

Чтобы установить сервер со встроенным DNS, должны также быть добавлены следующие параметры:

- --setup-dns – создать зону DNS, если она еще не существует, и настроить DNS-сервер;
- --forwarder или --no-forwarders – в зависимости от того, нужно ли настроить серверы пересылки DNS или нет;
- --auto-reverse или --no-reverse – в зависимости от того, нужно ли настроить автоматическое обнаружение обратных зон DNS, которые должны быть созданы в FreeIPA DNS, или отключить автоматическое определение обратных зон.

ВНИМАНИЕ!

Пароли должны быть не менее 8 символов.

Для запуска интерактивной установки следует выполнить команду:

```
# ipa-server-install
```

Обратите внимание на ответы на вопрос, не совпадающий с предложенными:

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```

Остальные вопросы нужно выбрать по умолчанию (можно просто нажать <Enter>). При установке также нужно ввести пароль администратора системы и пароль администратора каталогов.

После завершения процесса конфигурации будет выведена подсказка со следующими шагами:

```
=====  
Setup complete
```

Next steps:

1. You must make sure these network ports are open:

TCP Ports:

- * 80, 443: HTTP/HTTPS
- * 389, 636: LDAP/LDAPS
- * 88, 464: kerberos
- * 53: bind

UDP Ports:

- * 88, 464: kerberos
- * 53: bind
- * 123: ntp

2. You can now obtain a kerberos ticket using the command:
'kinit admin'

This ticket will allow you to use the IPA tools (e.g., ipa user-add)

and the web user interface.

The ipa-server-install command was successful

Для возможности управлять FreeIPA-сервером из командной строки нужно получить билет Kerberos:

```
# kinit admin
```

Добавить в DNS запись о сервере времени, чтобы компьютеры в локальной сети могли к нему подключаться:

```
# ipa dnsrecord-add example.test _ntp._udp --srv-priority=0 \  
--srv-weight=100 --srv-port=123 --srv-target=ipa.example.test
```

Проверить работу ntp сервера можно командой:

```
# ntpdate -q localhost  
server 127.0.0.1, stratum 4, offset -0.000201, delay 0.02571
```

```
20 Nov 19:04:00 ntpdate[7971]: adjust time server 127.0.0.1
offset -0.000201 sec
```

Проверить наличие прямой и обратной зон можно, выполнив команды:

```
# ipa dnszone-show example.test
Имя зоны: example.test.
Активная зона: True
Полномочный сервер имён: ipa.example.test.
```

...

```
# ipa dnszone-show 0.168.192.in-addr.arpa.
Имя зоны: 0.168.192.in-addr.arpa.
Активная зона: True
Полномочный сервер имён: ipa.example.test.
```

...

Примечание. Если в выводе присутствуют ошибки следующего вида:

```
[error] CalledProcessError: Command '/sbin/systemctl restart
httpd2.service' returned non-zero exit status 1
```

Выполнить команду:

```
# systemctl restart httpd2
```

Отменить установку:

```
# ipa-server-install -U --uninstall
```

и повторить снова.

Примечание. В случае сбоя установки сервера FreeIPA некоторые файлы конфигурации могут быть уже сконфигурированы. В этом случае дополнительные попытки установить сервер FreeIPA завершатся неудачно. Чтобы решить эту проблему, перед повторной попыткой запуска процесса установки, следует удалить частичную конфигурацию сервера FreeIPA:

```
# ipa-server-install --uninstall
```

Если ошибки при установке сервера FreeIPA остаются, следует переустановить ОС. Одним из требований для установки сервера FreeIPA является чистая система без каких-либо настроек.

Веб-интерфейс FreeIPA будет доступен по адресу:

```
https://ipa.example.test/ipa/ui/
```

12.2. Установка сервера FreeIPA в режиме CA-less

В этом разделе описывается, как можно установить сервер FreeIPA (Сервер 64 бит (x86_64), AArch64 (ARMv8)) со встроенным DNS-сервером без центра сертификации (CA).

CA-less конфигурация требуется в тех случаях, когда по какой-либо причине нет возможности развернуть на FreeIPA сервис PKI dogtag. Например, на данный момент это невозможно сделать в некоторых сертифицированных конфигурациях.

Предварительные действия:

1) установить пакеты:

```
# apt-get install freeipa-server freeipa-server-dns
```

2) задать имя сервера:

```
# hostnamectl set-hostname ipa.example.test
```

Примечание. После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы нужно перезагрузить систему.

Подготовить сертификаты для сервера FreeIPA:

1) создать каталог для сертификатов:

```
# mkdir ~/test_ca
```

2) создать файл password.txt с паролем к закрытому ключу (длина пароля должна быть не меньше 8 символов):

```
# echo "SEcRet.123" > ~/test_ca/password.txt
```

3) создать базу данных NSS:

```
# certutil -d ~/test_ca -N -f ~/test_ca/password.txt
```

4) создать noise файл, заполненный случайными числами:

```
# head -c20 /dev/random > ~/test_ca/noise.txt
```

5) выполнить экспорт переменной CERT_SERIAL:

```
# export CERT_SERIAL=1
```

6) создать CA сертификат:

```
# SKID="0x`openssl rand -hex 20`"
```

```
# echo $SKID
```

```
0xfa012b30b9407b0750b786ff5ed9f49ce3998622
```

```
# certutil -d ~/test_ca -S -n "CA" -s "CN=Certificate Authority" -x -t CT,,C -1 -2 -5 -m $CERT_SERIAL -v 120 -z ~/test_ca/noise.txt -f ~/test_ca/password.txt --extSKID
```

В ответ на запросы команды дать следующие ответы (на запрос «Enter value for the key identifier fields», следует ввести вывод команды echo \$SKID):

```
0 - Digital Signature
```

```
1 - Non-repudiation
```

```
5 - Cert signing key
```

```
9 - done
```

```
Is this a critical extension [y/N]? y
```

ЛКНВ.11100-01 90 03

```

Is this a CA certificate [y/N]? y
Enter the path length constraint, enter to skip [<0 for
unlimited path] 0
Is this a critical extension [y/N]? y
Enter value for the key identifier fields,enter to omit:
0xfa012b30b9407b0750b786ff5ed9f49ce3998622
Is this a critical extension [y/N]? n
5 - SSL CA
6 - S/MIME CA
7 - Object Signing CA
9 - done
Is this a critical extension [y/N]? n

```

7) создать noise файл, заполненный случайными числами:

```
# head -c20 /dev/random > ~/test_ca/noise.txt
```

8) создать запрос на сертификат (на запрос «Enter value for the key identifier fields», следует ввести вывод команды echo \$SKID):

```

# SKID="0x`openssl rand -hex 20`"
# echo $SKID
0xb17caf72b46288bcc9c887c89894dc917e06f724
# certutil -d ~/test_ca -R -s CN=$HOSTNAME,O=IPA -o
/tmp/servercert.req -k rsa -g 2048 -z ~/test_ca/noise.txt -f
~/test_ca/password.txt -a --extSKID
Generating key. This may take a few moments...

```

```
Adding Subject Key ID extension.
```

```
Enter value for the key identifier fields,enter to omit:
```

```
0xb17caf72b46288bcc9c887c89894dc917e06f724
```

```
Is this a critical extension [y/N]?
```

```
n
```

9) подписать запрос на сертификат:

```

# export CERT_SERIAL=$(( $CERT_SERIAL + 1 ))
# certutil -d ~/test_ca -C -c "CA" -i /tmp/servercert.req -o
/tmp/servercert.pem -m $CERT_SERIAL -v 120 -f
~/test_ca/password.txt -1 -5 -a

```

В ответ на запросы команды дать следующие ответы:

```
2 - Key encipherment
```

```
9 - done
```

```
Is this a critical extension [y/N]? n
```

```
1 - SSL Server
```

```
9 - done
```

```
Is this a critical extension [y/N]? n
```

Примечание. Можно также создать отдельные сертификаты для серверов HTTP и Directory.

Произвести экспорт сертификатов в правильные форматы:

- 1) импортировать полученный сертификат (на запрос команды следует ввести пароль к закрытому ключу, указанный в файле ~/test_ca/password.txt):

```
# certutil -d ~/test_ca -A -i /tmp/servercert.pem -n Server-
Cert -a -t ,,
Enter Password or Pin for "NSS Certificate DB":
```

- 2) экспортировать сертификат в PKCS#12:

```
# pk12util -o ~/test_ca/servercert.p12 -n Server-Cert -d
~/test_ca -k ~/test_ca/password.txt -w ~/test_ca/password.txt
pk12util: PKCS12 EXPORT SUCCESSFUL
```

- 3) экспортировать сертификат СА в формат PEM:

```
# certutil -d ~/test_ca -L -n "CA" -a > ~/test_ca/cacert.pem
```

Установка CA-less IPA:

- 1) установить пароль к закрытому ключу в значение переменной PSWD:

```
# export PSWD=$(cat ~/test_ca/password.txt)
```

- 2) проверить правильность создания сертификата:

```
# openssl verify -CAfile ~/test_ca/cacert.pem /tmp/servercert.pem
/tmp/servercert.pem: OK
```

- 3) установить CA-less IPA:

```
# ipa-server-install \
  --http-cert-file ~/test_ca/servercert.p12 \
  --http-pin $PSWD \
  --dirsrv-cert-file ~/test_ca/servercert.p12 \
  --dirsrv-pin $PSWD \
  --ca-cert-file ~/test_ca/cacert.pem \
  --no-pkinit
```

```
The log file for this installation can be found in
/var/log/ipaserver-install.log
```

```
=====
```

```
This program will set up the IPA Server.
```

```
Version 4.9.14
```

```
This includes:
```

- * Configure the NTP client (CHRONY)

ЛКНВ.11100-01 90 03

- * Create and configure an instance of Directory Server
- * Create and configure a Kerberos Key Distribution Center (KDC)
- * Configure Apache (httpd)
- * Configure SID generation

To accept the default shown in brackets, press the Enter key.

На вопрос, нужно ли сконфигурировать DNS-сервер BIND ответить утвердительно:

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```

и на вопрос о продолжении настройки системы с указанными значениями ответить утвердительно:

```
Continue to configure the system with these values? [no]: yes
```

Остальные вопросы нужно выбрать по умолчанию (можно просто нажать <Enter>). При установке также нужно ввести пароль администратора системы и пароль администратора каталогов.

После завершения процесса конфигурации будет выведена подсказка со следующими шагами:

```
=====
Setup complete
Next steps:
 1. You must make sure these network ports are open:
    TCP Ports:
    * 80, 443: HTTP/HTTPS
    * 389, 636: LDAP/LDAPS
    * 88, 464: kerberos
    * 53: bind
    UDP Ports:
    * 88, 464: kerberos
    * 53: bind
    * 123: ntp
 2. You can now obtain a kerberos ticket using the command: 'kinit
admin'
    This ticket will allow you to use the IPA tools (e.g., ipa user-add)
    and the web user interface.
```

The ipa-server-install command was successful

Примечание. Можно указать при установке опции `--pkinit-cert-file=файл` – файл, содержащий сертификат SSL Kerberos KDC и закрытый ключ и `--pkinit-pin=Пароль` – пароль от закрытого ключа Kerberos KDC.

Для возможности управлять FreeIPA-сервером из командной строки нужно получить билет Kerberos:

```
# kinit admin
```

Веб-интерфейс FreeIPA будет доступен по адресу:

`https://ipa.example.test/ipa/ui/`

12.3. Добавление новых пользователей домена

Для добавления новых пользователей можно воспользоваться веб-интерфейсом FreeIPA. Для этого нужно открыть в веб-браузере адрес `https://ipa.example.test/ipa/ui` и ввести данные администратора для входа в систему (рис. 512). Для входа в веб-интерфейс следует использовать имя `admin`, и пароль, введенный при установке сервера FreeIPA.

После успешной авторизации можно создать нового пользователя домена. Для этого в окне «Пользователи домена» нужно нажать на кнопку «Добавить» (рис. 513).

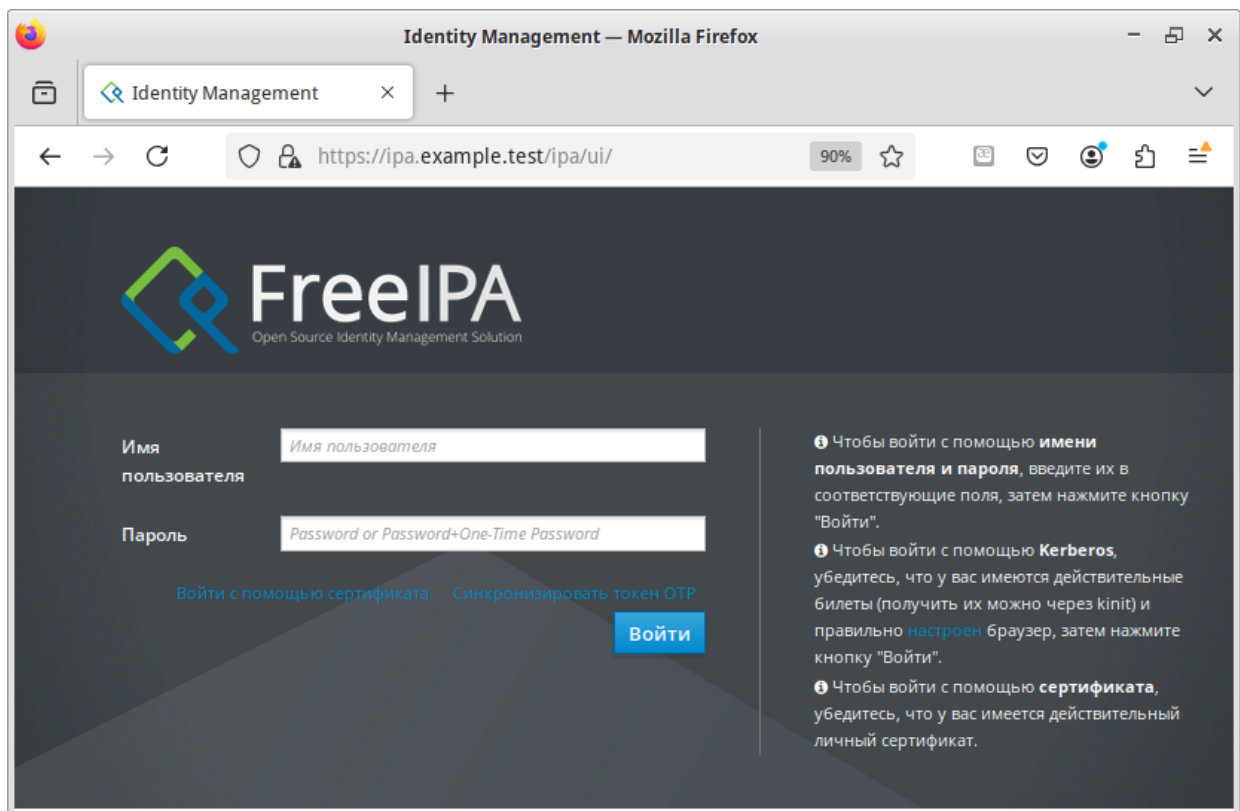


Рис. 512 – Веб-интерфейс FreeIPA

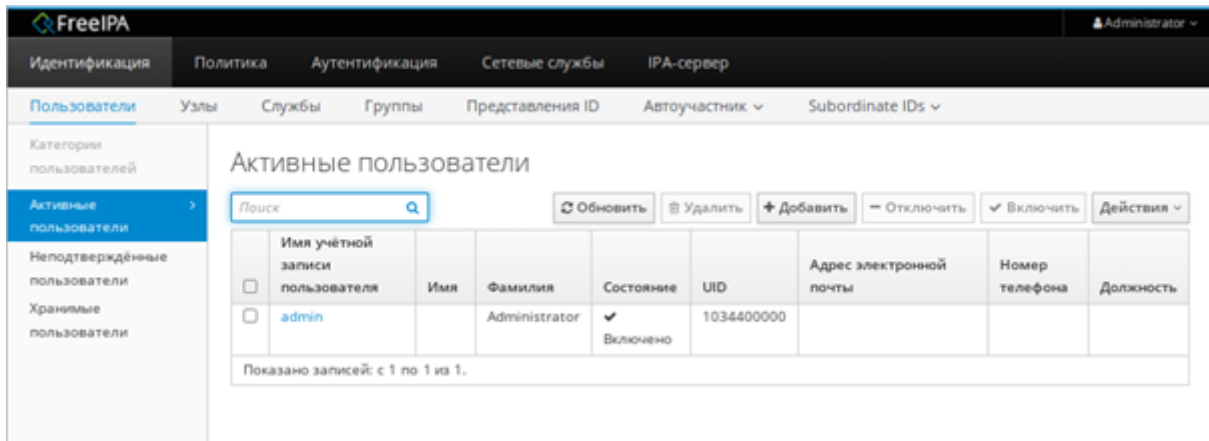


Рис. 513 – Окно «Пользователи домена»

В открывшемся окне нужно ввести данные пользователя и нажать на кнопку «Добавить» (рис. 514).

Рис. 514 – Окно добавления нового пользователя домена

Созданный пользователь появится в списке пользователей (рис. 515).

Активные пользователи

Поиск <input type="text"/>								
<input type="button" value="Обновить"/> <input type="button" value="Удалить"/> <input type="button" value="Добавить"/> <input type="button" value="Отключить"/> <input type="button" value="Включить"/> <input type="button" value="Действия"/>								
<input type="checkbox"/>	Имя учётной записи пользователя	Имя	Фамилия	Состояние	UID	Адрес электронной почты	Номер телефона	Должность
<input type="checkbox"/>	admin		Administrator	✓ Включено	948000000			
<input checked="" type="checkbox"/>	isakova	Ольга	Исакова	✓ Включено	948000007	isakova@example.test		
<input type="checkbox"/>	ivanov	Илья	Иванов	✓ Включено	948000003	ivanov@example.test		

Рис. 515 – Список пользователей домена

12.4. Ввод рабочей станции в домен FreeIPA – установка клиента и подключение к серверу

Инструкция по вводу рабочей станции под управлением ОС Альт СП Рабочая станция в домен FreeIPA.

12.4.1. Установка FreeIPA клиента

Установить пакеты:

```
# apt-get install freeipa-client libsss_sudo krb5-kinit bind-
utils libbind zip
```

Примечание. На рабочей станции 64/32 бит установить также пакет task-auth-freeipa.

Примечание. Очистить конфигурацию freeipa-client невозможно. В случае если это нужно (например, для удаления, переустановки freeipa-client) следует переустановить систему.

12.4.2. Настройка сети. FreeIPA

Клиентские компьютеры должны быть настроены на использование DNS-сервера, который был сконфигурирован на сервере FreeIPA во время его установки. При получении IP-адреса по DHCP данные о сервере DNS также должны быть получены от сервера DHCP. Ниже приведен пример настройки сетевого интерфейса со статическим IP-адресом.

В сетевых настройках нужно указать использовать сервер FreeIPA для разрешения имен. Эти настройки можно выполнить как в графическом интерфейсе, так и в консоли:

1) в ЦУС в разделе «Сеть» → «Ethernet-интерфейсы» задать имя компьютера, указать в поле DNS-серверы IP-адрес FreeIPA-сервера и в поле «Домены поиска» – домен для поиска (рис. 516);

2) в консоли:

- задать имя компьютера:

```
# hostnamectl set-hostname comp01.example.test
```

- добавить DNS-сервер, для этого нужно создать файл /etc/net/ifaces/eth0/resolv.conf со следующим содержимым:

```
nameserver 192.168.0.113
```

где 192.168.0.113 – IP-адрес FreeIPA-сервера;

- указать службе resolvconf использовать DNS FreeIPA и домен для поиска. Для этого в файле /etc/resolvconf.conf добавить/отредактировать следующие параметры:

```
interface_order='lo lo[0-9]* lo.* eth0'
```

```
search_domains=example.test
```

где:

а) eth0 – интерфейс на котором доступен FreeIPA-сервер;

б) example.test – домен;

- обновить DNS-адреса:

```
# resolvconf -u
```

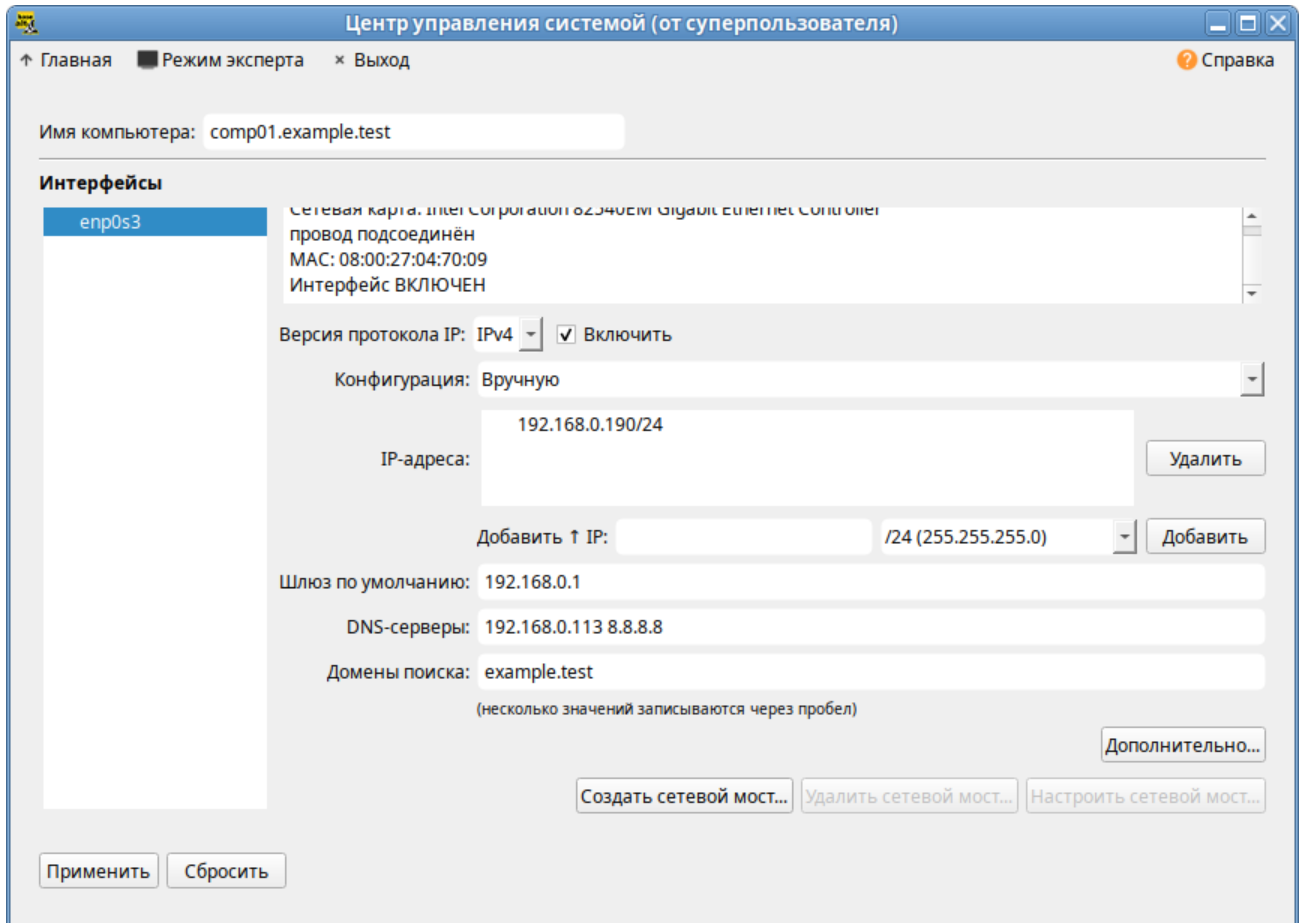


Рис. 516 – Настройка на использование DNS-сервера домена

Примечание. После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы нужно перезагрузить систему.

В результате выполненных действий в файле `/etc/resolv.conf` должны появиться строки:

```
search example.test
nameserver 192.168.0.113
```

12.4.3. Подключение к серверу в ЦУС

Для ввода рабочей станции в домен FreeIPA, нужно в ЦУС перейти в раздел «Пользователи» → «Аутентификация» (пакет `alterator-auth`).

В открывшемся окне следует выбрать пункт «Домен FreeIPA», заполнить поля «Домен» и «Имя компьютера», затем нажать на кнопку «Применить» (рис. 517).

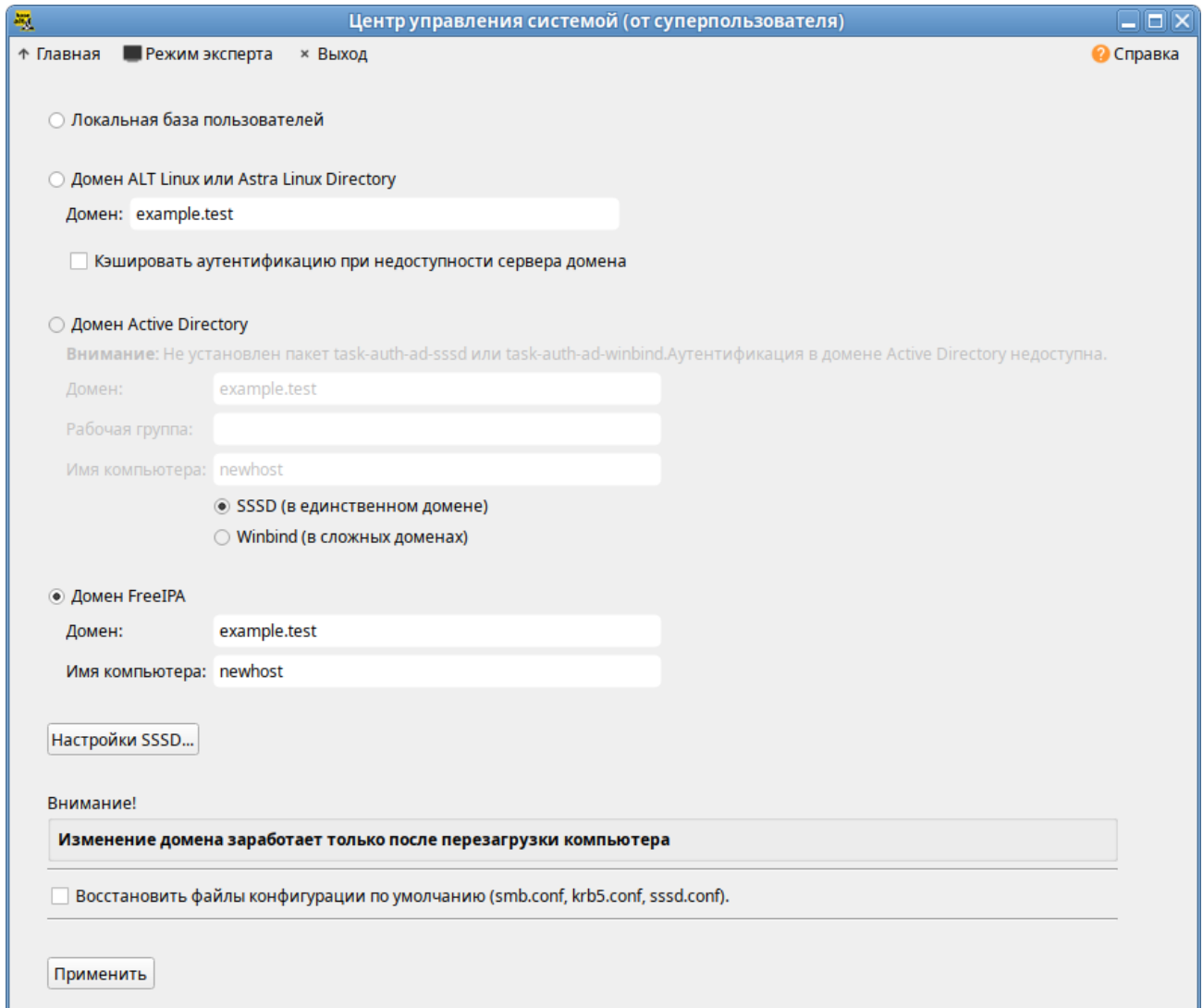


Рис. 517 – Ввод в домен в «Центре управления системой»

В открывшемся окне нужно ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать на кнопку «ОК» (рис. 518).

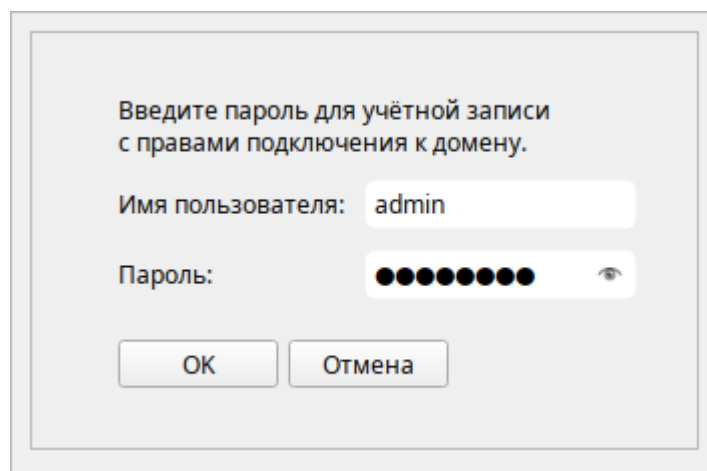


Рис. 518 – Параметры учётной записи с правами подключения к домену

В случае успешного подключения, будет выведено соответствующее сообщение (рис. 519).

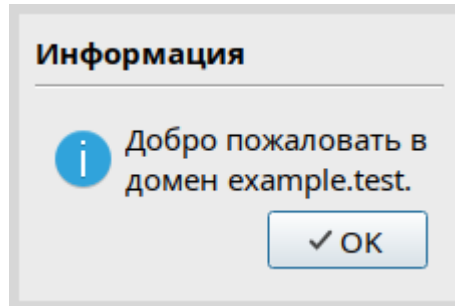


Рис. 519 – Успешное подключение к домену

Перезагрузить рабочую станцию.

12.4.4. Подключение к серверу в консоли

Запустить скрипт настройки клиента в пакетном режиме:

```
# ipa-client-install -U -p admin -w 12345678
```

или интерактивно:

```
# ipa-client-install
```

Если все настроено, верно, скрипт должен выдать такое сообщение:

```
'''Discovery was successful!'''
```

```
Client hostname: comp01.example.test
```

```
Realm: EXAMPLE.TEST
```

```
DNS Domain: example.test
```

```
IPA Server: ipa.example.test
```

```
BaseDN: dc=example,dc=test
```

```
Continue to configure the system with these values? [no]:
```

Нужно ответить `yes`, ввести имя пользователя, имеющего право вводить машины в домен, и его пароль.

ВНИМАНИЕ!

Если при входе в домен возникает такая ошибка:

```
Hostname (comp01.example.test) does not have A/AAAA record.
```

```
Failed to update DNS records.
```

Нужно проверить IP-адрес доменного DNS-сервера в файле `/etc/resolv.conf`.

В случае возникновения ошибки, нужно перед повторной установкой запустить процедуру удаления:

```
# ipa-client-install -U --uninstall
```

Для работы sudo-политик для доменных пользователей на клиентской машине нужно разрешить доступ к sudo:

```
# control sudo public
```

12.4.5. Вход пользователя

В окне входа в систему (рис. 520) необходимо ввести логин учетной записи пользователя FreeIPA и нажать кнопку «Войти», в открывшемся окне ввести пароль, соответствующий этой учетной записи и нажать кнопку «Войти».

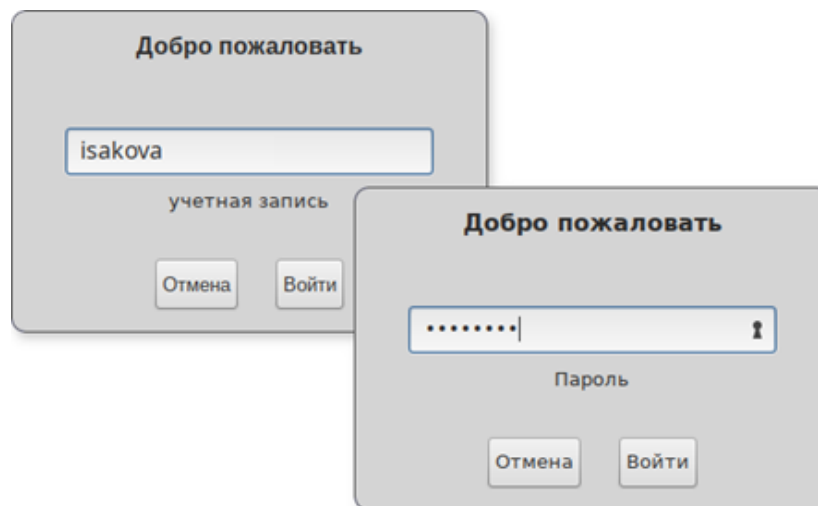


Рис. 520 – Вход пользователя

При первом входе пользователя будет запрошен текущий (установленный администратором) пароль и затем у пользователя запрашивается новый пароль (рис. 521) и его подтверждение.

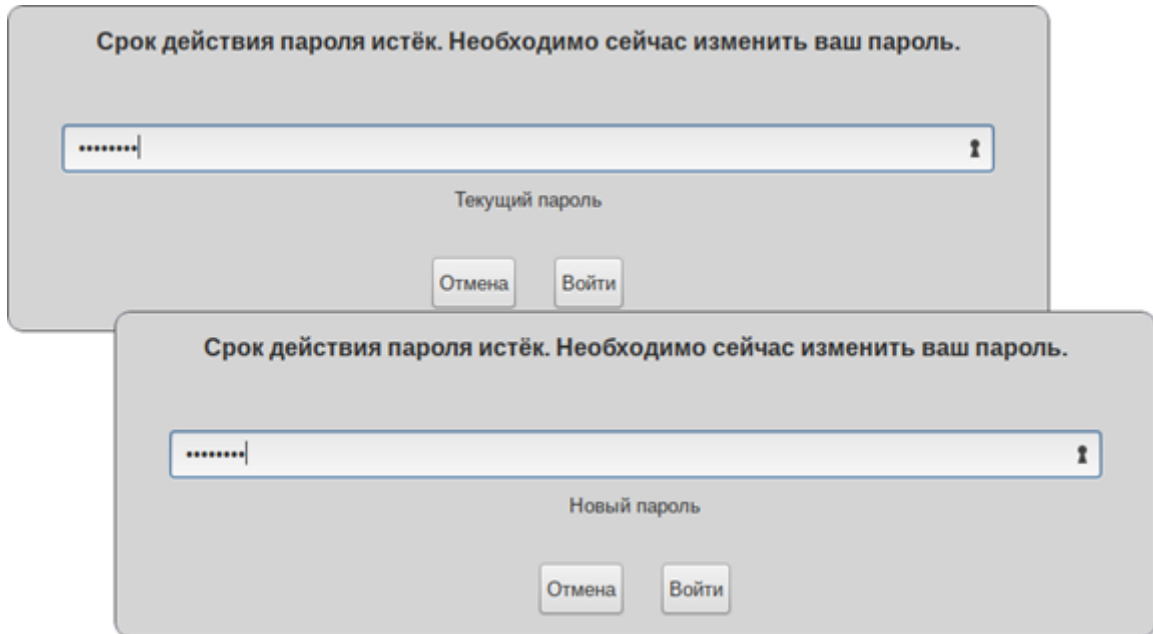


Рис. 521 – Запрос текущего пароля и нового пароля

⚠ Если машина до этого была в других доменах или есть проблемы со входом пользователей рекомендуется очистить кэш sssd:

```
# systemctl stop sssd
# rm -f /var/lib/sss/db/*
# rm -f /var/lib/sss/mc/*
# systemctl start sssd
```

12.4.6. Удаление клиента FreeIPA

При удалении, клиент удаляется из домена FreeIPA вместе с конфигурацией системных служб FreeIPA.

Для удаления клиента FreeIPA необходимо:

- на клиенте ввести команду:

```
# ipa-client-install --uninstall
...
Client uninstall complete.
The original nsswitch.conf configuration has been restored.
You may need to restart services or reboot the machine.
Do you want to reboot the machine? [no]: yes
The ipa-client-install command was successful
```

- на клиенте удалить, если они есть, старые принципалы Kerberos (кроме /etc/krb5.keytab):

```
# ipa-rmkeytab -k /path/to/keytab -r EXAMPLE.TEST
```


- на сервере FreeIPA удалить все записи DNS для клиентского узла:

```
# ipa dnsrecord-del
Имя записи: comp01
Имя зоны: example.test
Возможность удаления определенной записи не предусмотрена.
Удалить все? Yes/No (default No): yes
-----
Удалена запись "comp01"
-----
```

- на сервере FreeIPA удалить запись узла с сервера LDAP FreeIPA (при этом будут удалены все службы и отозваны все сертификаты, выданные для этого узла):

```
# ipa host-del comp01.example.test
-----
Удален узел "comp01.example.test"
-----
```

12.5. Настройка репликации

Для установки реплики используется утилита `ipa-replica-install`. Реплики необходимо устанавливать по одной. Установка нескольких реплик одновременно не поддерживается.

Новую реплику можно установить:

- на существующем клиенте FreeIPA путем преобразования клиента в реплику;
- на машине, которая еще не зарегистрирована в домене FreeIPA.

В обеих этих ситуациях можно настроить реплику, добавив нужные параметры в команду `ipa-replica-install`.

Для возможности установки реплики должны быть установлены те же пакеты, что и при установке сервера:

```
# apt-get install freeipa-client freeipa-server-dns
Задать имя сервера:
# hostnamectl set-hostname replica.example.test
```

Перед настройкой репликации необходимо настроить систему на использование DNS-сервера, который был сконфигурирован на сервере FreeIPA во время его установки см. п. 12.4.2.

12.5.1. Настройка реплики на существующем клиенте

Развернуть и настроить клиент:

```
# ipa-client-install -d --domain=example.test --server=ipa.example.test  
--realm=EXAMPLE.TEST --principal=admin --password=12345678 --enable-dns-  
updates -U
```

После выполнения этой операции узел `replica.example.test` должен появиться в веб-интерфейсе FreeIPA.

Перед разворачиванием реплики необходимо убедиться, что при настройке DNS в процессе инициализации FreeIPA была создана обратная зона DNS («Сетевые службы»→«DNS»→«Зоны DNS») и в обратной зоне создана реверсивная запись для основного сервера 192.168.0.113.

Создать обратный адрес для реплики на DNS-сервере основного сервера. Для этого в веб-интерфейсе FreeIPA необходимо перейти в «Сетевые службы»→«DNS»→«Зоны DNS», выбрать в таблице запись домена (например, `example.test.`), в открывшемся списке открыть запись реплики (например, `replica`), нажать на IP-адрес в поле A записи и в открывшемся окне на ссылку «Создать запись DNS» (рис. 522) или выполнить команду:

```
# ipa dnsrecord-add 0.168.192.in-addr.arpa 145 --ptr-rec  
'replica.example.test.'
```

При необходимости повторить данную процедуру для записи AAAA.

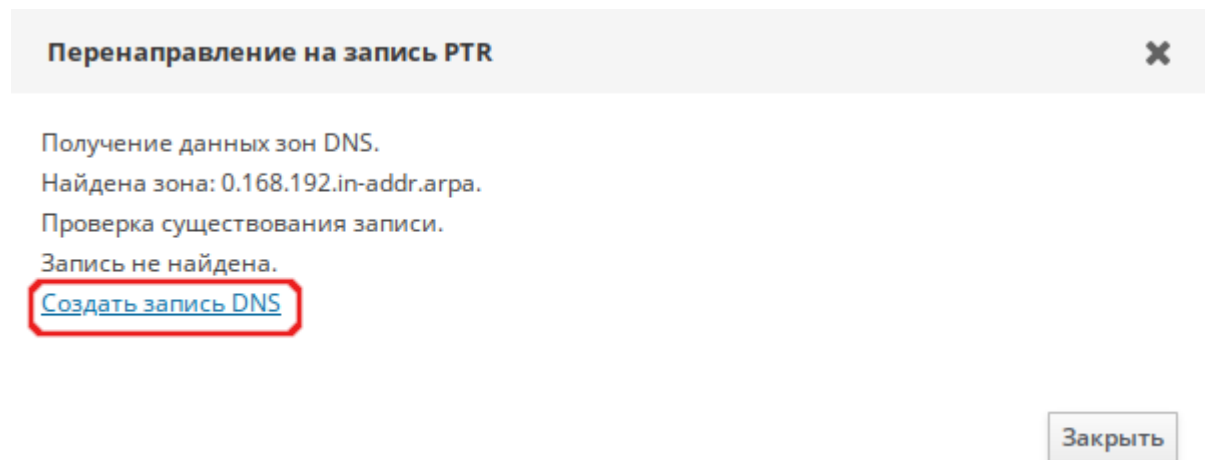


Рис. 522 – Создать запись обратной зоны DNS

Примечание. Перед настройкой репликации необходимо убедиться, что серверы видят друг друга и правильно разрешают доменные имена.

Проверить возможность подключения можно, выполнив следующую команду на машине, где будет установлена реплика:

```
# ipa-replica-conncheck --master ipa.example.test
Check connection from replica to remote master
'ipa2.example.test':
  Directory Service: Unsecure port (389): OK
  Directory Service: Secure port (636): OK
  Kerberos KDC: TCP (88): OK
  Kerberos Kpasswd: TCP (464): OK
  HTTP Server: Unsecure port (80): OK
  HTTP Server: Secure port (443): OK
```

The following list of ports use UDP protocol and would need to be checked manually:

```
  Kerberos KDC: UDP (88): SKIPPED
  Kerberos Kpasswd: UDP (464): SKIPPED
```

Connection from replica to master is OK.
Start listening on required ports for remote master check
Listeners are started. Use CTRL+C to terminate the listening part after the test.

Please run the following command on remote master:
/usr/sbin/ipa-replica-conncheck --replica replica.example.test

И на машине FreeIPA сервере:

```
# /usr/sbin/ipa-replica-conncheck --replica replica.example.test
Check connection from master to remote replica
'replica.example.test':
  Directory Service: Unsecure port (389): OK
  Directory Service: Secure port (636): OK
  Kerberos KDC: TCP (88): OK
  Kerberos KDC: UDP (88): OK
  Kerberos Kpasswd: TCP (464): OK
  Kerberos Kpasswd: UDP (464): OK
  HTTP Server: Unsecure port (80): OK
  HTTP Server: Secure port (443): OK
```

Connection from master to replica is OK.

При установке реплики на существующем клиенте FreeIPA можно выбрать один из двух способов, чтобы авторизовать установку:

- использовать учетные данные привилегированного пользователя;
- включить узел в группу ipaservers.

В примере, описанном ниже, для авторизации регистрации используется пароль привилегированного пользователя.

Настроить репликацию LDAP-каталога:

```
# ipa-replica-install
Password for admin@EXAMPLE.TEST:
```

Примечание. dbus может мешать проверке соединений при установке реплики, при появлении ошибок может помочь перезапуск сервиса:

```
# systemctl reload dbus
```

Добавить в DNS второй NTP-сервер:

```
# kinit admin
# ipa dnsrecord-add example.test _ntp_udp --srv-priority=0 --srv-weight=100 --srv-port=123 --srv-target=replica.example.test
Имя записи: _ntp_udp
SRV record: 0 100 123 ipa.example.test., 0 100 123
replica.example.test
```

Настроить репликацию DNS-зон:

```
# ipa-dns-install
```

Настроить репликацию СА:

```
# ipa-ca-install
```

12.5.2. Установка реплики на машине, которая еще не зарегистрирована в домене FreeIPA

При установке реплики в системе, которая еще не зарегистрирована в домене FreeIPA, утилита ipa-replica-install сначала регистрирует систему в качестве клиента, а затем устанавливает компоненты реплики.

Перед разворачиванием реплики необходимо убедиться, что при настройке DNS в процессе инициализации FreeIPA была создана обратная зона DNS («Сетевые службы»→«DNS»→«Зоны DNS») и в обратной зоне создана реверсивная запись для основного сервера 192.168.0.113.

Примечание. Если реплика находится в другой IP-сети, необходимо вручную добавить запись для обратной зоны реплики на сервере FreeIPA.

В примере, описанном ниже, для авторизации регистрации используется случайный пароль, действительный только для одной регистрации этого клиента.

Установка реплики с использованием случайного пароля:

- на сервере FreeIPA получить билет Kerberos:

```
$ kinit admin
```

- на сервере FreeIPA добавить внешнюю систему в качестве узла FreeIPA:

```
$ ipa host-add replica.example.test --random --ip-address=192.168.0.145
```

```
-----
Добавлен узел "replica.example.test"
-----
```

```
Имя узла: replica.example.test
Случайный пароль: 2AaT0Ix8itDsYugdDGoRtBt
Пароль: True
Таблица ключей: False
Managed by: replica.example.test
```

- на сервере FreeIPA добавить систему replica.example.test в группу узлов ipaservers:

```
$ ipa hostgroup-add-member ipaservers --hosts replica.example.test
```

```
Группа узлов: ipaservers
Описание: IPA server hosts
Узлы-участники: ipa.example.test, replica.example.test
```

```
-----
Количество добавленных участников 1
-----
```

- на машине, где будет установлена реплика, установить необходимые пакеты:

```
# apt-get install freeipa-server freeipa-server-dns
```

- на машине, где будет установлена реплика, запустить утилиту ipa-replica-install, указав сгенерированный пароль в параметре --password (т.к. пароль часто содержит специальные символы, следует заключить его в одинарные кавычки):

```
# ipa-replica-install --password='2AaT0Ix8itDsYugdDGoRtBt' \
--setup-ca --setup-dns --forwarder 192.168.0.113 --forwarder
8.8.8.8
```

```
Configuring client side components
This program will set up IPA client.
Version 4.9.14
```

```
Discovery was successful!
Client hostname: replica.example.test
Realm: EXAMPLE.TEST
DNS Domain: example.test
IPA Server: ipa.example.test
BaseDN: dc=example,dc=test
```

```
...
The ipa-client-install command was successful
...
The ipa-replica-install command was successful
```

Примечание. dbus может мешать проверке соединений при установке реплики, при появлении ошибок может помочь перезапуск сервиса:

```
# systemctl reload dbus
```

12.5.3. Проверка репликации

После создания реплики можно проверить, реплицирует ли реплика данные должным образом:

- создать пользователя на новой реплике:

```
$ kinit admin
$ ipa user-add test_user
```

- убедиться, что пользователь виден на другой реплике:

```
$ kinit admin
$ ipa user-show test_user
```

После настройки и репликации контроллеров посмотреть топологию можно в веб-интерфейсе FreeIPA (рис. 523) («IPA-сервер» → «Топология» → «Topology Graph»).

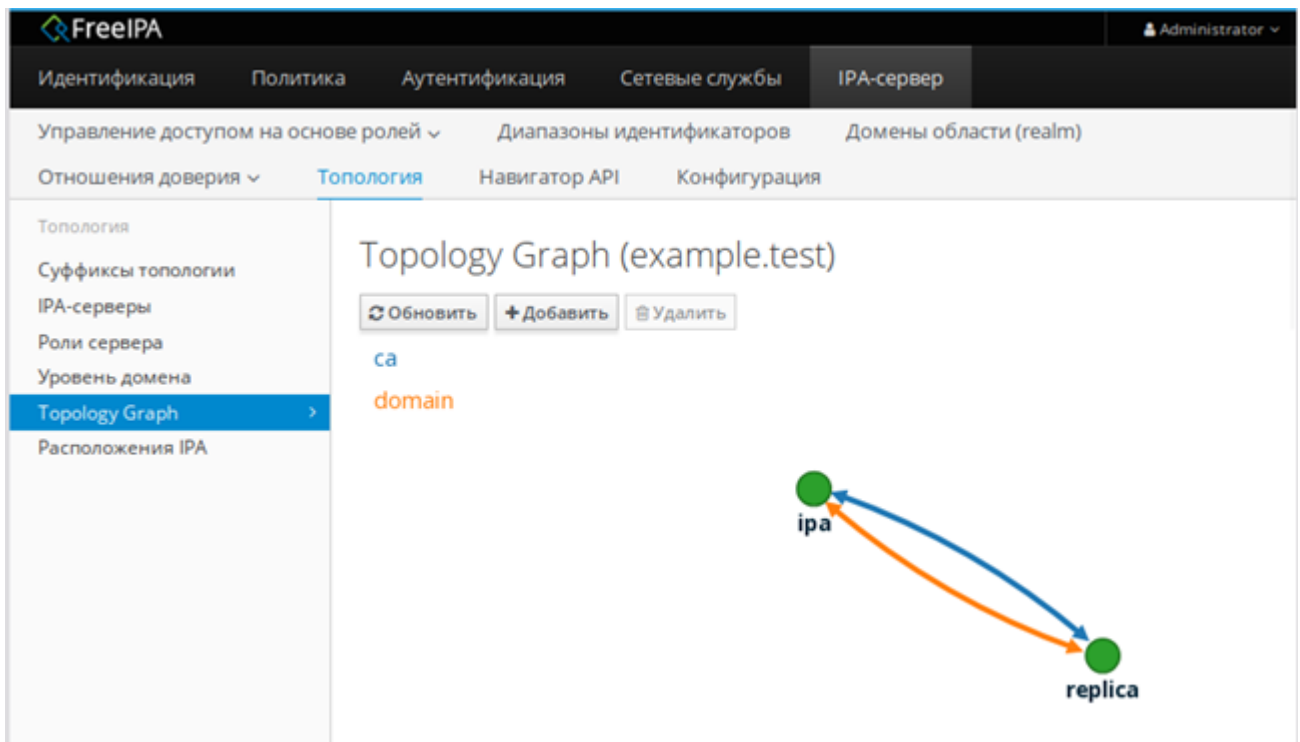


Рис. 523 – Топология FreeIPA

12.6. Настройка доверительных отношений с Active Directory

FreeIPA использует Samba для интеграции в AD. Для работы Samba нужен работающий стек IPv6.

Начальные данные:

- IP-адрес IPA-сервера: 192.168.135.130;
- Имя IPA-сервера: dcf;
- Имя IPA-домена: domf.testf;
- NetBIOS имя IPA домена: DOMF;
- IP-адрес AD DC: 192.168.135.150;
- Имя AD DC: dcc;
- Имя AD домена: domc.testc;
- NetBIOS имя AD домена: DOMC.

Установить пакет:

```
# apt-get install freeipa-server-trust-ad
```

12.6.1. Настройка DNS

Перед подключением FreeIPA и AD к доверию необходимо убедиться, что серверы видят друг друга и правильно разрешают доменные имена.

Для настройки DNS необходимо:

- настроить зоны DNS на сервере FreeIPA;
- настроить условную переадресацию DNS в AD;
- проверить правильность конфигурации DNS.

12.6.1.1. Настройка зоны перенаправления DNS на сервере FreeIPA

Создание зоны переадресации DNS для домена AD в командной строке (следует указать IP-адрес удаленного DNS-сервера с параметром `--forwarder`):

```
# kinit admin
```

```
Password for admin@EXAMPLE.TEST:
```

```
# ipa dnsforwardzone-add test.alt --forwarder=192.168.0.132 \  
--forward-policy=first
```

Сервер проверит DNS-перенаправитель (перенаправители).

Это может занять некоторое время; пожалуйста, подождите...

Имя зоны: test.alt.

```
Активная зона: True
Перенаправители зон: 192.168.0.132
Политика перенаправления: first
```

Примечание. Если при добавлении зоны перенаправления появляется предупреждение об ошибке проверки DNSSEC, это означает, что удаленный DNS-сервер не использует DNSSEC. Рекомендуется включить DNSSEC на удаленном DNS-сервере.

Если включить проверку DNSSEC на удаленном DNS-сервере нельзя, можно отключить DNSSEC на сервере FreeIPA.

Для этого в файле `/etc/bind/ipa-options-ext.conf` следует установить для параметра `dnssec-validation` значение `no`:

```
dnssec-validation no;
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

Проверка настройки:

```
# dig dc1.test.alt +noall +answer
```

```
dc1.test.alt.      886 IN  A    192.168.0.132
```

12.6.1.2. Настройка переадресации DNS в AD

На сервере AD необходимо создать сервер условной пересылки для зоны IPA-домена.

Настройка «Альт Домен»:

1) добавить в файл `/etc/bind/options.conf` строки (если используется

`dns_backend BIND9_DLZ`):

```
zone "example.test" {
    type forward;
    forwarders { 192.168.0.113; };
};
```

2) перезапустить службу DNS:

```
# systemctl restart bind.service
```

Настройка Windows Server с AD:

```
C:\> dnscmd 127.0.0.1 /ZoneAdd example.test /Forwarder
192.168.0.113
```

```
DNS Server 127.0.0.1 created zone example.test:
```

```
Command completed successfully
```


12.6.2. Предварительная настройка IPA-сервера

Выполнить предварительную настройку IPA-сервера для работы с доверием:

```
# ipa-adtrust-install
```

Записи DNS создаются автоматически, если FreeIPA был установлен с интегрированным DNS-сервером. Если FreeIPA установлен без встроенного DNS-сервера, `ipa-adtrust-install` выведет список служебных записей, которые нужно вручную добавить в DNS.

Далее скрипт сообщит, что файл `/etc/samba/smb.conf` уже существует и будет переписан:

```
WARNING: The smb.conf already exists. Running ipa-adtrust-install
will break your existing samba configuration.
```

```
Do you wish to continue? [no]: yes
```

Скрипт спросит, нужно ли конфигурировать `slapi-nis` плагин для поддержки работы старых клиентов (SSSD < 1.9) с пользователем из доверенного домена:

```
Enable trusted domains support in slapi-nis? [no]:
```

Результат выполнения команды:

```
Done configuring CIFS.
```

```
=====
Setup complete
```

```
You must make sure these network ports are open:
```

```
TCP Ports:
```

- * 135: epmap
- * 138: netbios-dgm
- * 139: netbios-ssn
- * 445: microsoft-ds
- * 1024..1300: epmap listener range
- * 3268: msft-gc

```
UDP Ports:
```

- * 138: netbios-dgm
- * 139: netbios-ssn
- * 389: (C)LDAP
- * 445: microsoft-ds

```
See the ipa-adtrust-install(1) man page for more details
```

IPA-сервер в своей работе использует следующие порты:

- TCP ports: 80, 88, 443, 389, 636, 88, 464, 53, 135, 138, 139, 445, 1024 – 1300;
- UDP ports: 88, 464, 53, 123, 138, 139, 389, 445.

Они должны быть открыты и доступны.

Перезапустить ipa:

```
# systemctl restart ipa
```

Проверить, проходит ли Samba аутентификацию Kerberos со стороны IPA-сервера:

```
# smbclient -L ipa.example.test
lpcfg_do_global_parameter: WARNING: The "domain logons" option is
deprecated
Password for [admin@EXAMPLE.TEST]:
      Sharename      Type            Comment
      -
      IPC$           IPC             IPC Service (Samba 4.19.7-alt4)
SMB1 disabled -- no workgroup available
```

12.6.3. Проверка конфигурации DNS

Перед настройкой доверия необходимо убедиться, что серверы FreeIPA и AD могут разрешать себя и друг друга.

12.6.3.1. На IPA-сервере

Проверить наличие записей для работы сервисов IPA на DNS-сервере IPA.

1) запись, отвечающая за работу сервисов Kerberos через UDP и LDAP через TCP:

```
$ dig +short -t SRV _kerberos._udp.example.test
0 100 88 ipa.example.test.
0 100 88 replica.example.test.

$ dig +short -t SRV _ldap._tcp.example.test
0 100 389 replica.example.test.
0 100 389 ipa.example.test.
```

В выводе команд должен быть отображен список всех серверов IPA.

2) запись, отвечающая за имя Kerberos realm IPA домена:

```
$ dig +short -t TXT _kerberos.example.test
"EXAMPLE.TEST"
```

3) записи для работы сервисов AD на DNS-сервере IPA:

```
$ dig +short -t SRV _kerberos._tcp.dc._msdcs.test.alt
0 100 88 dc1.test.alt.
[user@ipa ~]$ dig +short -t SRV _ldap._tcp.dc._msdcs.test.alt
0 100 389 dc1.test.alt.
```

12.6.3.2. На Windows сервере с AD

Проверить наличие записей для работы сервисов IPA на DNS-сервере AD.

1) запустить утилиту nslookup.exe для поиска служебных записей:

```
C:\> nslookup.exe
> set type=SRV
```

2) записи, отвечающие за работу сервисов Kerberos через UDP и LDAP через

TCP:

```
> _kerberos._udp.example.test
_kerberos._udp.example.test      SRV service location:
  priority                        = 0
  weight                          = 100
  port                            = 88
  svr hostname                    = ipa.example.test
ipa.example.test internet address = 192.168.0.113
> _ldap._tcp.example.test
_ldap._tcp.example.test          SRV service location:
  priority                        = 0
  weight                          = 100
  port                            = 389
  svr hostname                    = ipa.example.test
ipa.example.test internet address = 192.168.0.113
```

3) запись, отвечающая за имя Kerberos realm IPA домена:

```
C:\> nslookup.exe
> set type=TXT
> _kerberos.example.test
_kerberos.example.test          text =

        "EXAMPLE.TEST"
```

12.6.4. Настройка доверия

Добавление двунаправленных доверительных отношений леса (Forest Trust) с AD (нужно ввести пароль Administrator AD, имя доменного администратора Windows – должно быть на латинице):

```
# kinit admin
# ipa trust-add --type=ad domc.testc --admin Administrator --password -
-two-way=true
Пароль администратора домена Active Directory:
-----
Добавлено отношение доверия Active Directory для области (realm)
"test.alt"
-----
Имя области (realm): test.alt
Имя домена NetBIOS: TEST
Идентификатор безопасности домена: S-1-5-21-1716172980-2818422221-
1777127716
Направление отношения доверия: Двустороннее отношение доверия
Тип отношения доверия: Домен Active Directory
Состояние отношения доверия: Установлено и проверено
```

При появлении запроса следует ввести пароль администратора домена Active Directory.

Примечание. Учетная запись пользователя, используемая при создании доверия (аргумент опции `--admin`), должна быть членом группы Domain Admins. Имя учетной записи должно быть на английском языке.

Получить список доверенных доменов леса со стороны AD:

```
# ipa trust-fetch-domains test.alt
```

При этом IPA создаст нужные id-диапазоны для доверенных доменов.

Чтобы увидеть список всех доверенных доменов из леса можно выполнить следующую команду:

```
# ipa trustdomain-find test.alt
Имя домена: test.alt
Имя домена NetBIOS: TEST
Идентификатор безопасности домена: S-1-5-21-1716172980-
2818422221-1777127716
Домен включен: True
```

```
-----
Количество возвращенных записей 1
-----
```

Просмотреть доверенные домены можно и в веб-интерфейсе (рис. 524) («IPA-Server» → «Отношения доверия» → «Отношения доверия»).

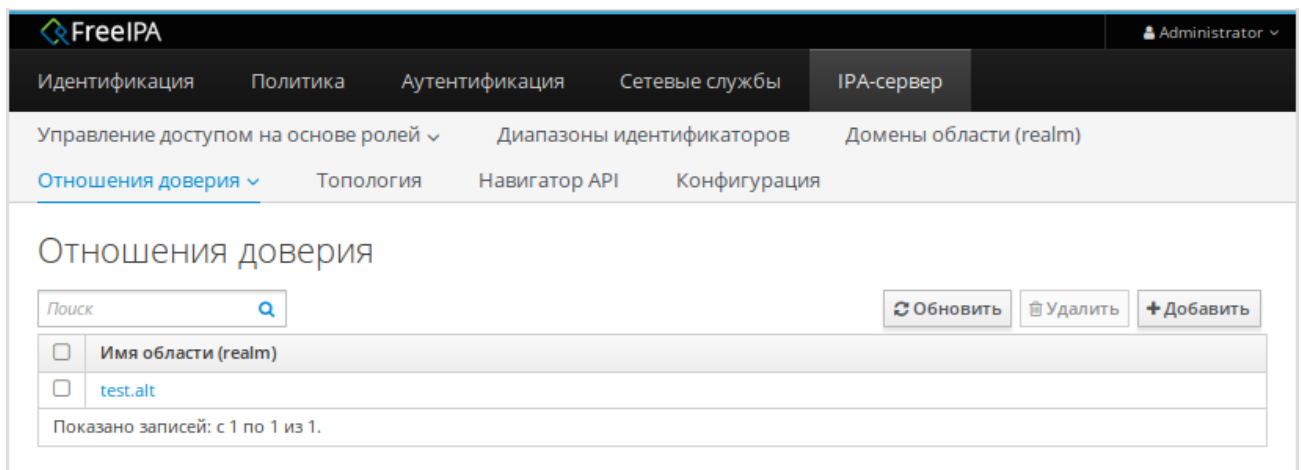


Рис. 524

12.6.5. Проверка конфигурации Kerberos

Для проверки конфигурации Kerberos, следует проверить, возможно ли получить билет для пользователя AD и может ли пользователь AD запрашивать служебные билеты.

Проверка конфигурации:

1) запросить билет для пользователя AD:

```
# kinit ivanov@test.alt
Password for ivanov@test.alt:
```

2) запросить service ticket для сервиса из IPA домена:

```
# kvno -S host $(hostname)
host/ipa.example.test@EXAMPLE.TEST: kvno = 2
```

3) запросить service ticket сервиса из AD домена:

```
# kvno -S cifs dc1.test.alt
cifs/dc1.test.alt@: kvno = 1
```

Если билет службы AD предоставлен, в списке билетов будет отображаться билет на предоставление билетов между областями (TGT) – krbtgt/IPA.DOMAIN@AD.DOMAIN (в примере: krbtgt/EXAMPLE.TEST@TEST.ALT):

```
# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_EhXu7Rx
Default principal: ivanov@TEST.ALT

Valid starting      Expires            Service principal
21.11.2024 10:25:51  21.11.2024 20:24:56  cifs/dc1.test.alt@
    renew until 22.11.2024 10:24:53
    Ticket server: cifs/dc1.test.alt@TEST.ALT
21.11.2024 10:25:33  21.11.2024 20:24:56
host/ipa.example.test@EXAMPLE.TEST
    renew until 22.11.2024 10:24:53
21.11.2024 10:25:33  21.11.2024 20:24:56
krbtgt/EXAMPLE.TEST@TEST.ALT
    renew until 22.11.2024 10:24:53
21.11.2024 10:24:56  21.11.2024 20:24:56
krbtgt/TEST.ALT@TEST.ALT
    renew until 22.11.2024 10:24:53
```

12.6.6. Проверка пользователей доверенного домена

Необходимо проверить, имеют ли рабочие станции FreeIPA доступ к пользователям из доверенного домена.

На рабочей станции IPA выполнить команду:

```
# getent passwd ivanov@test.alt
ivanov@test.alt:*:386401105:386401105:ivanov:/home/test.alt/ivanov:
```

где `ivanov` – пользователь из AD домена.

Следует обратить внимание, что у пользователя не указана оболочка входа.

Назначить оболочку входа для пользователей из доверенного домена можно добавив на сервере IPA в файл `/etc/sssds/sssds.conf` строку:

```
[domain/example.test]
...
default_shell = /bin/bash
...
```

И перезапустить службу `sssds`:

```
# systemctl restart sssds
```

Вывод команды должен стать таким:

```
# getent passwd ivanov@test.alt
ivanov@test.alt:*:386401105:386401105:ivanov:/home/test.alt/ivanov:/bin/bash
```

ВНИМАНИЕ!

1) Для корректной работы сервера IPA с пользователями доверенного домена AD нужно обеспечить доступ сервиса `sssds` к `/etc/krb5.keytab`.

2) Для входа AD пользователя на рабочую станцию в домене под управлением FreeIPA, идентификатор пользователя должен быть указан в формате `<ИМЯ_ДОМЕНА>\<идентификатор_пользователя_AD>` или `<идентификатор_пользователя_AD>@<имя_домена>` (например, `TEST\ivanov`, `TEST.ALT\ivanov`, `ivanov@test`, `ivanov@test.alt`).

3) Для входа IPA пользователя в Windows рабочую станцию из AD имя пользователя вводится в формате `<ИМЯ_ДОМЕНА>\<идентификатор_пользователя_IPA>`.

13. НАСТРОЙКА СЛУЖБ DNS (BIND)

13.1. Общие сведения

Службы DNS (Bind) в ОС Альт СП отвечают за преобразование доменного имени в IP-адрес и за обратную операцию.

Если локальная сеть не подключена к сети Интернет, вполне возможно, что внутренний DNS-сервер в ней не нужен. За преобразование доменного имени в IP-адрес и обратно в различные механизмы, лишь один из которых базируется на службе доменных имен. В самом простом случае имена всех компьютеров вместе с их адресами можно записать в файл `/etc/hosts`. Порядок просмотра различных пространств имен указывается в файле `/etc/nsswitch.conf`. Строка `hosts: files dns` этого файла предписывает приложениям, пользующимся стандартной функцией `gethostbyname()` сначала обратиться в `/etc/hosts`, а затем отправить запрос к DNS-серверу.

Если задачу преобразования имен в адреса взял на себя провайдер, собственный DNS-сервер также не требуется. В этом случае на всех компьютерах в качестве сервера имен указывается сервер провайдера (поле «`nameserver`» в файле `/etc/resolv.conf`), к которому и идут все запросы. Даже если внутренняя сеть организована согласно RFC1918 (т. н. интранет) и адреса компьютеров в ней недоступны из внешней сети, DNS-запросы во внешнюю сеть будут выполняться. Между собой компьютерам предлагается общаться с помощью `/etc/hosts` или IP-адресов.

Некоторые службы и системные утилиты, работающие с доменными именами, запускаются в ОС Альт СП с использованием `chroot` (в каталоге `/var/resolv`), поэтому после изменения упомянутых файлов рекомендуется выполнить команду:

```
update_chrooted conf
```

Собственную службу доменных имен рекомендуется настраивать для решения задач, описанных ниже.

13.2. Уменьшение времени ответа на DNS-запрос абонентов внутренней сети

Если канал подключения к сети Интернет обладает большим временем задержки, то работа с данными, включающими в себя много доменных имен (например, с www-страницами) может замедлиться. Общий объем трафика при этом не вырастет, поскольку система доменных имен – распределенная база данных, поддерживающая механизм кеширования запросов. Первое обращение к кеширующему DNS-серверу приводит к выполнению рекурсивного запроса: опрашивается сервер более высокого уровня, который, если не знает ответа, передаст запрос дальше. Результат запроса сохраняется в кэше, таким образом все последующие обращения именно к этой записи дальше кеширующего сервера не уйдут. Время жизни (Time To Live, TTL) записи в кэше определяется хозяином запрошенного доменного имени. По истечении TTL запись из кэша удаляется.

13.3. Именованние компьютеров в интранет-сети

Решение этой задачи может потребоваться, если среди компьютеров внутренней сети есть свои серверы (например, корпоративный www-сервер), к которым другие компьютеры обращаются по доменному имени.

Поскольку адреса такой сети не пойдут дальше межсетевого экрана, допускается использовать имя какого угодно – в том числе несуществующего – домена и сделать соответствующие записи `/etc/hosts`. Поддержание в актуальном состоянии файла `/etc/hosts` на всех компьютерах – нелегкая задача, и лучше все-таки воспользоваться DNS-сервером.

13.4. Примеры использования DNS-сервера Bind

Решение обеих поставленных задач предоставляется настройкой DNS-сервера Bind.

В ОС Альт СП сервер Bind запускается с использованием `chroot`. В `/etc` от Bind остается символьная ссылка на главный файл настроек `named.conf`. Корневым каталогом является `/var/lib/bind`, где у Bind есть собственный каталог `/etc` содержащий набор включаемых друг в друга конфигурационных файлов, каталоги `/var` и `/dev`.

Примечание. Все пути к файлам и каталогам в настройках Bind начинаются именно из этого каталога, и /zone соответствует /var/lib/bind/zone.

Чтобы запустить named в кеширующем режиме, достаточно раскомментировать и заполнить раздел настройки forwarders (вышестоящие серверы) в файле /var/lib/bind/etc/options.conf.

В связи с возможными ограничениями на право обращаться к серверу с обычными и рекурсивными запросами (настройки allow-query и allow-recursion), допускается раскомментировать установки по умолчанию. Эти настройки открывают доступ только абонентам локальных сетей, к которым компьютер подключен непосредственно:

```
# grep allow- /var/lib/bind/etc/options.conf
// allow-query { localnets; };
// allow-recursion { localnets; };
```

Использование Bind для полноценного именования компьютеров в локальной сети требует создания двух зон (прямой и обратной), содержащих в виде записей определенного формата информацию о доменных именах компьютеров и об их роли в этих доменах.

Каждая зона должна включать запись типа SOA (StateOfAuthority, сведения об ответственности). В этой записи определяются основные временные и административные параметры домена, в том числе электронный адрес лица, ответственного за домен (администратора) и серийный номер зоны.

Серийный номер – число в диапазоне от 0 до 4294967295 (232); каждое изменение, вносимое в зону, должно сопровождаться увеличением этого номера. Обнаружив увеличение серийного номера, кеширующие и вторичные серверы признают все закешированные записи из этой зоны устаревшими. Удобно использовать формат «годмесяцчисловерсия», где все числа, кроме года, двузначные, а версия может обнуляться раз в день, соответствовать времени (например, по формуле $100 * (\text{часы} * 60 + \text{минуты}) / (60 * 24)$) или иметь сквозную нумерацию (в этом случае появляется сложность с переходом от версии 99 к версии 100, то есть 0).

Даже если серийный номер генерируется автоматически, рекомендуется пользоваться этим форматом, наглядно отражающим время создания зоны.

Пример зоны, не содержащей ничего, кроме записи SOA и обязательной записи типа NS (NameServer), находится в файле `/var/lib/bind/zone/empty`.

Кроме записи типа SOA, в каждой зоне должна быть хотя бы одна запись типа NS, указывающая адрес DNS-сервера, авторитативного в этом домене (как минимум – адрес сервера, на котором запущен `named`).

Несколько зон включаются в настройку Bind автоматически (файл `/var/lib/bind/etc/rfc1912.conf`). Они нужны для обслуживания сети, привязанной к сетевой заглушке (127.0.0.1/8). Имя домена, который обслуживается зоной, задается в файле настроек, а в самом файле зоны можно использовать относительную адресацию (без «.» в конце имени), благодаря чему операция переименования домена выполняется редактированием одной строки.

В ОС Альт СП рекомендуется добавлять описания зон в конфигурационный файл `/var/lib/bind/etc/local.conf`.

Прямая зона нужна для преобразования доменного имени в IP-адрес – операции, нужной многим программам постоянно. Большинство записей в прямой зоне – типа A (Address) – предназначены именно для этого. Другие часто встречающиеся типы записей – это CNAME (CanonicalName, настоящее имя), позволяющий привязать несколько дополнительных имен к одному, и MX (MailExchange, обмен почтой), указывающий, куда пересылать почтовые сообщения, в поле адресат которых встречается определенное доменное имя.

Пример прямой зоны для домена `internal.domain.net` (незначащие поля соответствующих файлов заменены на «. . .»):

```
# cat /var/lib/bind/etc/local.conf
. . .
zone "internal.domain.net" {
type master;
file "internal.domain.net";
};
. . .
# cat /var/lib/bind/zone/internal.domain.net
$TTL 1D
@ IN SOA server root.server (
2013082202 ; serial
```

```
    12H ; refresh
    1H ; retry
    1W ; expire
    1H ; ncache
)
    IN NS server
    MX 10 server
server A 10.10.10.1
www CNAME server
mail CNAME server
jack A 10.10.10.100
jill A 10.10.10.101
```

В этом примере используются правила по умолчанию: если в записи некоторое поле опущено, оно наследуется от предыдущей. Так, вместо А допускается написать IN А, а вместо MX – @ IN MX, где @ означает имя домена, указанное в конфигурационном файле.

Как видно из примера, всю работу в сети делает компьютер с адресом 10.10.10.1, он же server.internal.domain.net, он же www.internal.domain.net и mail.internal.domain.net. Несмотря на наличие среди CNAME этого сервера имени «mail», MX-запись указывает на действительный адрес – так рекомендовано RFC (Request for Comments, документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты, широко применяемые во всемирной сети).

Для того чтобы преобразовывать IP-адреса в доменные имена, у каждой сети должна быть обратная зона. Если такой зоны нет, и в файле /etc/hosts тоже ничего не написано, операция не выполнится. Такое преобразование нужно гораздо реже и в основном по соображениям административным: для того, чтобы выяснить принадлежность компьютера (с которого, допустим, пытаются атаковать сервер) по его IP-адресу. Некоторые почтовые серверы проверяют, содержится ли IP-адрес машины, передающей сообщение, в обратной зоне и похоже ли полученное доменное имя на то, что указано в сообщении, и при несовпадении отказываются принимать письмо.

Обратная зона состоит почти целиком из записей типа PTR (Pointer, указатель). Чтобы не умножать сущностей, решено было не вводить новый способ работы сервера имен и представить обратное преобразование IP-адреса как прямое преобразование доменного имени специального вида.

Например, чтобы выяснить доменное имя компьютера с адресом «1.2.3.4», нужно запросить информацию о доменном имени 4.3.2.1.in-addr.arpa. Таким образом, каждой подсети класса C (или выше) соответствует определенный домен, в котором можно найти ответ.

Обратная зона для домена, приведенного выше:

```
# cat /var/lib/bind/etc/local.conf

. . .
zone "12.11.10.in-addr.arpa" {
type master;
file "12.11.10.in-addr.arpa";
};
. . .
# cat /var/lib/bind/zone/12.11.10.in-addr.arpa
$TTL 1D
@ IN SOA server.internal.domain.net. root.server.internal.domain.net (
    2013082201 ; serial
    12H ; refresh
    1H ; retry
    1W ; expire
    1H ; ncache
)
    IN NS server.internal.domain.net.
0 PTR internal.domain.net.
1 PTR server.internal.domain.net.
100 PTR jack.internal.domain.net.
101 PTR jill.internal.domain.net.
```

Относительные адреса, использованные в левой части записей PTR, раскрываются в полные следующего вида: адрес.12.11.10.in-addr.arpa, а в правой части используются полные, которые могут указывать на имена в разных доменах.

Проверить синтаксическую правильность конфигурационного файла и файла зоны можно с помощью утилит `named-checkconf` и `named-checkzone`, входящих в пакет `bind`. Они же используются при запуске службы командой `service bind start`.

Стоит иметь в виду, что, в отличие от прямых зон, обратные описывают административную принадлежность компьютеров, но сами принадлежат хозяину сети (как правило, провайдеру).

Существует особого рода затруднение, связанное с работой DNS-сервера уже не во внутренней сети, а в сети Интернет. Связано это с тем, что подсети класса С (сети /24, в которых сетевая маска занимает 24 бита, а адрес компьютера – 8) выдаются только организациям, способным такую подсеть освоить (в сети класса С 254 абонентских IP-адреса, один адрес сети и один широковещательный адрес). Чаще всего выдаются совсем маленькие подсети – от /30 (на два абонентских адреса) до /27 (на 30 адресов) – или другие диапазоны, сетевая маска которых не выровнена по границе байта. Таких подсетей в обратной зоне получится несколько, а возможности просто разделить ее, отдав часть адресов в администрирование хостам, нет. Провайдер в таких случаях пользуется RFC2317, предписывающем в обратной зоне заводить не записи вида PTR, а ссылки CNAME на адреса в «классифицированных» обратных зонах специального вида. Обратное преобразование становится двухступенчатым, зато администрирование каждой классифицированной зоны можно отдать хосту.

DNS-сервер, отвечающий на запросы из глобальной сети, должен быть зарегистрирован в родительском домене. Правила требуют, чтобы при регистрации домена было указано не менее двух DNS-серверов, которые будут его обслуживать.

Из всех зарегистрированных серверов (записей типа NS в родительской зоне) только одна соответствует первичному (master) серверу, а остальные – вторичным (slave). Для внешнего пользователя вторичный сервер не отличается от первичного, отличия состоят только в способе администрирования: все изменения вносятся в зоны первичного сервера, а вторичный только кеширует эти зоны, целиком получая их по специальному межсерверному протоколу. Полученная зона складывается в файл, редактировать который бессмысленно: первичный сервер при изменении зоны рассылает всем своим вторичным указание скачать ее заново. Право на скачивание зоны можно ограничить настройкой allow-transfer (как правило, в ней перечисляются адреса вторичных серверов).

Пример задания вторичного сервера в файле настроек:

```
// We are a slave server for eng.example.com
zone "eng.example.com" {
type slave;
file "slave/eng.example.com";
// IP address of eng.example.com master server
masters { 192.168.4.12; };
};
```

Вторичный сервер рекомендуется размещать в сети, отличной от той, в которой помещается первичный, – так повышается надежность обработки запроса (если один сервер недоступен, возможно, ответит второй) и возрастает скорость распространения записей по кэшам промежуточных серверов.

Проверку работоспособности, доступности и вообще самочувствия DNS-сервера рекомендуется выполнять утилитой `dig` из пакета `bind-utils`, которая выдает максимум информации о том, что происходило с запросом (для информации об обратном преобразовании нужно добавить ключ `-x`):

```
dig basealt.ru
; <<>> DiG 9.10.4-P5 <<>> basealt.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32751
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;basealt.ru. IN A
;; ANSWER SECTION:
basealt.ru. 86400 IN A 194.107.17.41
;; Query time: 1177 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Mar 01 10:07:17 MSK 2017
;; MSG SIZE rcvd: 55
```

Можно также использовать утилиту `host` из того же пакета, например:

```
host basealt.ru
basealt.ru has address 194.107.17.41
```

Для выяснения административной принадлежности тех или иных доменов и сетей можно воспользоваться утилитой `whois` из одноименного пакета, которая обращается к специальной сетевой базе данных (не имеющей отношения к DNS).

14. СИСТЕМА МОНИТОРИНГА ZABBIX

Zabbix – система мониторинга и отслеживания статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования.

Для управления системой мониторинга и чтения данных используется веб-интерфейс.

14.1. Установка сервера PostgreSQL

Перед установкой Zabbix должен быть установлен и запущен сервер PostgreSQL, с созданным пользователем zabbix и созданной базой zabbix.

Установить PostgreSQL, Zabbix-сервер и дополнительную утилиту fping:

```
# apt-get install postgresql16-server zabbix-server-pgsql
```

Подготовить к запуску и настроить службы PostgreSQL, для этого нужно выполнить следующие действия:

- создать системные базы данных (пароль пользователя PostgreSQL необходимо запомнить):

```
# /etc/init.d/postgresql initdb
```

Введите новый пароль суперпользователя:

Повторите его:

Это пункт нужно пропустить, если системные базы уже инициировались.

- включить по умолчанию и запустить службу:

```
# systemctl enable --now postgresql
```

- создать пользователя zabbix и базу данных zabbix (при запросе «Пароль» следует ввести пароль пользователя postgresql, созданный при создании системных баз данных):

```
# su - postgres -s /bin/sh -c 'createuser --no-superuser --no-createdb --no-createrole --encrypted --pwprompt zabbix'
```

Введите пароль для новой роли:

Повторите его:

Пароль:

```
# su - postgres -s /bin/sh -c 'createdb -O zabbix zabbix'
```

Пароль:

```
# systemctl restart postgresql
```

- добавить в базу данные для веб-интерфейса (последовательность команд важна):

```
# su - postgres -s /bin/sh -c 'psql -U zabbix -f
/usr/share/doc/zabbix-common-database-pgsql-*/schema.sql zabbix'
# su - postgres -s /bin/sh -c 'psql -U zabbix -f
/usr/share/doc/zabbix-common-database-pgsql-*/images.sql zabbix'
# su - postgres -s /bin/sh -c 'psql -U zabbix -f
/usr/share/doc/zabbix-common-database-pgsql-*/data.sql zabbix'
```

14.2. Установка Apache2

Установить пакеты:

```
# apt-get install apache2 apache2-mod_php8.3
```

Добавить в автозапуск и запустить apache2:

```
# systemctl enable --now httpd2
```

14.3. Установка PHP

Установить пакеты:

```
# apt-get install php8.3 php8.3-mbstring php8.3-sockets php8.3-gd
php8.3-xmlreader php8.3-pgsql php8.3-ldap php8.3-openssl
```

В файле `/etc/php/8.3/apache2-mod_php/php.ini` изменить некоторые опции `php`:

```
memory_limit = 256M
post_max_size = 32M
max_execution_time = 600
max_input_time = 600
date.timezone = Europe/Moscow
always_populate_raw_post_data = -1
```

Примечание. Актуальная версия PHP может быть другой.

Перезапустить apache2:

```
# systemctl restart httpd2
```

14.4. Настройка и запуск Zabbix-сервера

Внести изменения в конфигурационный файл

`/etc/zabbix/zabbix_server.conf`:

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=Пароль от базы
```


Добавить Zabbix-сервер в автозапуск и запустить его:

```
# systemctl enable --now zabbix_pgsql
```

14.5. Установка веб-интерфейса Zabbix

Установить метапакеты:

```
# apt-get install zabbix-phpfrontend-apache2-mod_php8.3 zabbix-  
phpfrontend-engine
```

Включить аддоны в apache2:

```
# ln -s /etc/httpd2/conf/addon.d/A.zabbix.conf /etc/httpd2/conf/extra-  
enabled/
```

Перезапустить apache2:

```
# systemctl restart httpd2
```

Изменить права доступа к конфигурационному каталогу веб-интерфейса, чтобы веб-установщик мог записать конфигурационный файл:

```
# chown apache2:apache2 /var/www/webapps/zabbix/ui/conf
```

В веб-браузере перейти на страницу установки Zabbix-сервера:

```
http://<IP-сервера>/zabbix
```

При первом заходе на страницу запустится мастер, который шаг за шагом проверит возможности веб-сервера, интерпретатора PHP и сконфигурирует подключение к базе данных.

Для начала установки нужно выбрать язык установки и нажать на кнопку «Далее» (рис. 525), что осуществит переход на страницу проверки предварительных условий (рис. 526).

Нужно доустановить то, что требуется и перейти на следующую страницу.

На следующей странице (рис. 527) следует ввести параметры подключения к базе данных (параметры подключения нужно указывать такие же, как у Zabbix-сервера). По умолчанию в качестве «Схемы базы данных» («Database schema») нужно указать «public».

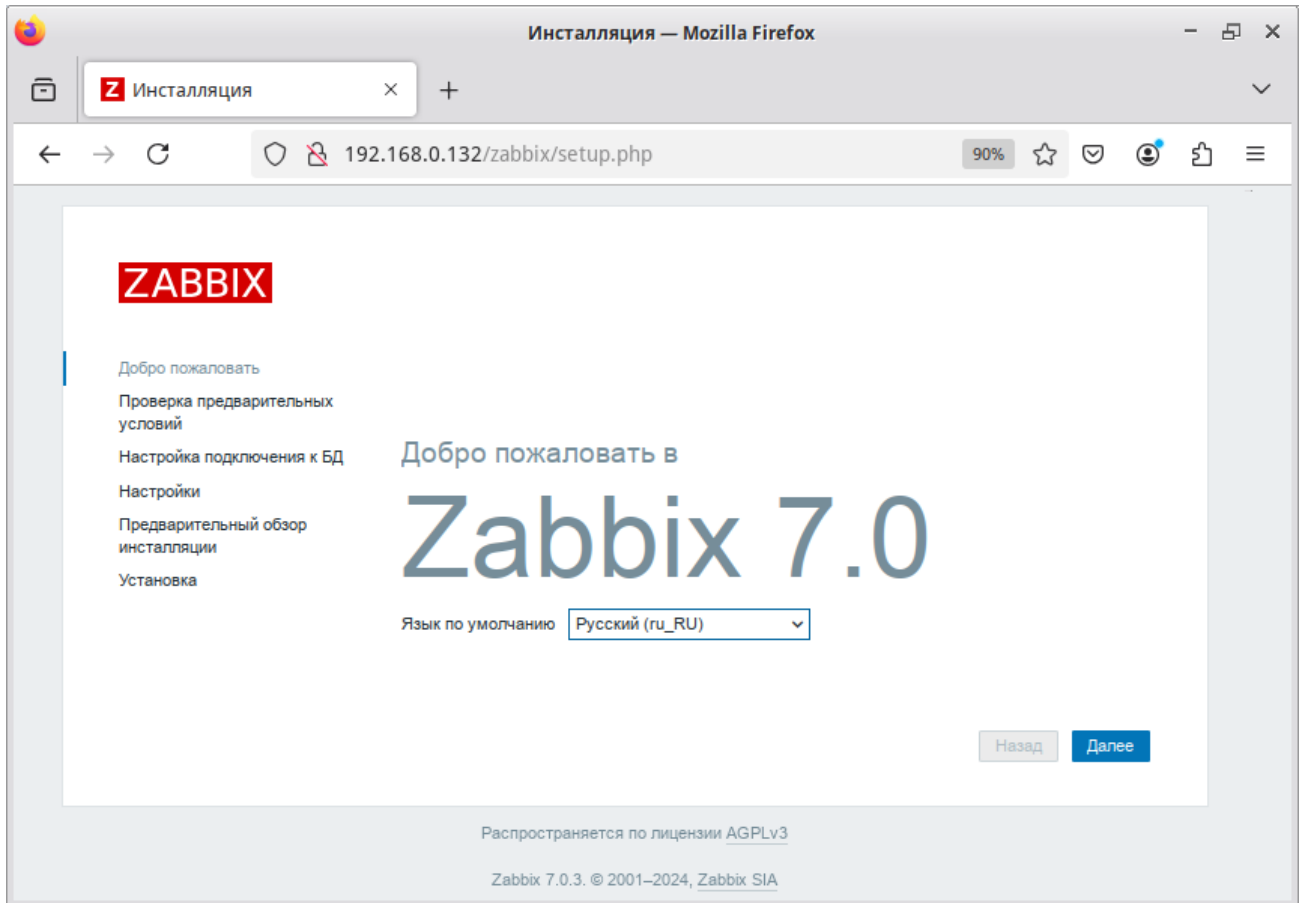


Рис. 525 – Страница установки Zabbix сервера

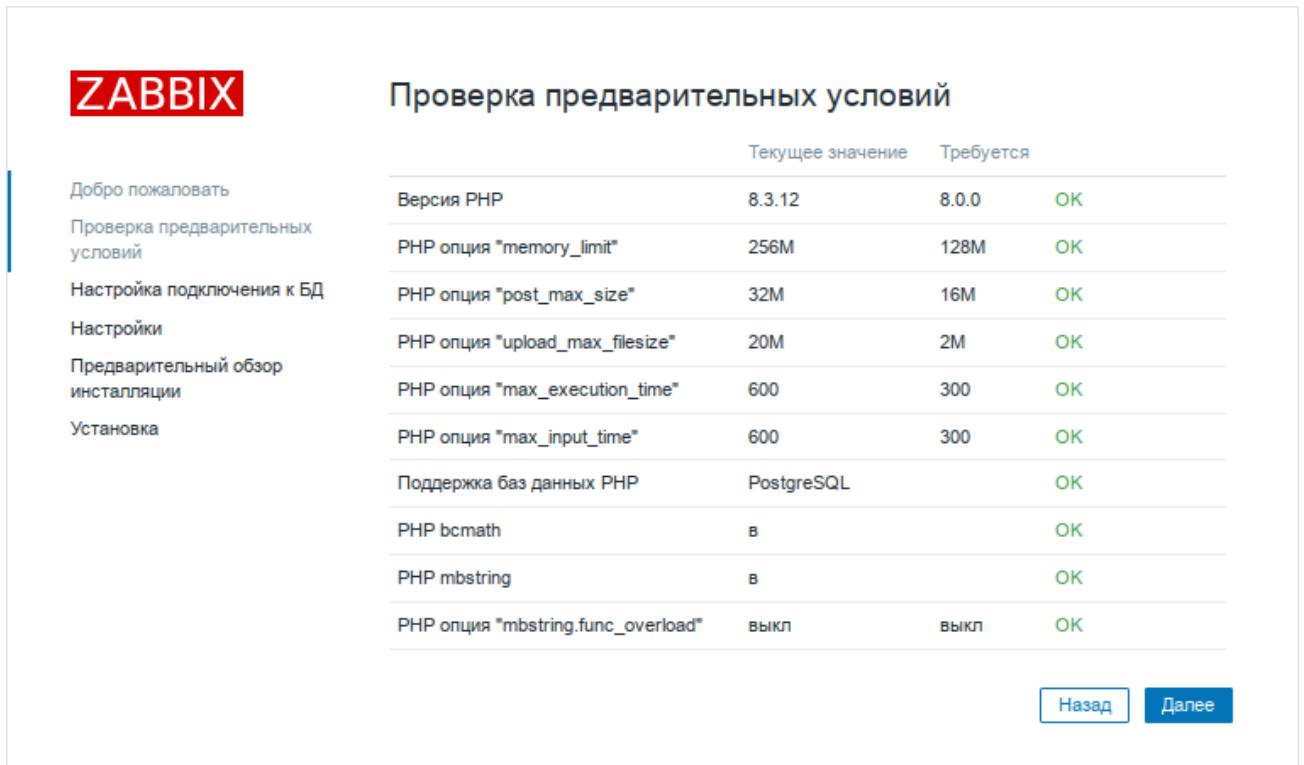


Рис. 526 – Страница проверки предварительных условий

The screenshot shows the Zabbix installation wizard's 'Настройка подключения к БД' (Database Connection Configuration) screen. The Zabbix logo is in the top left. A sidebar on the left contains navigation links: 'Добро пожаловать', 'Проверка предварительных условий', 'Настройка подключения к БД' (highlighted), 'Настройки', 'Предварительный обзор установки', and 'Установка'. The main content area has a title 'Настройка подключения к БД' and a subtitle: 'Пожалуйста, создайте базу данных вручную и укажите параметры конфигурации для соединения с этой базой. Нажмите кнопку "Далее" при завершении.' Below this are several configuration fields: 'Тип базы данных' (PostgreSQL), 'Хост базы данных' (localhost), 'Порт базы данных' (0), 'Имя базы данных' (zabbix), 'Схема базы данных' (public), 'Хранение учётных данных в' (with tabs for 'Простой текст', 'HashiCorp Vault', and 'Хранилище CyberArk'), 'Пользователь' (zabbix), 'Пароль' (masked with dots), and a 'TLS шифрование базы данных' checkbox. At the bottom right are 'Назад' and 'Далее' buttons.

Рис. 527 – Параметры подключения к базе данных

Примечание. Если выбрана опция «TLS шифрование базы данных», то в форме появятся дополнительные поля для настройки TLS-соединения с базой данных.

На следующих страницах необходимо выбрать настройки веб-интерфейса и задать имя сервера (рис. 528), и завершить установку.

The screenshot shows the Zabbix installation wizard's 'Настройки' (Settings) screen. The Zabbix logo is in the top left. A sidebar on the left contains navigation links: 'Добро пожаловать', 'Проверка предварительных условий', 'Настройка подключения к БД', 'Настройки' (highlighted), 'Предварительный обзор установки', and 'Установка'. The main content area has a title 'Настройки' and three configuration fields: 'Имя сервера Zabbix' (zabbix_server), 'Часовой пояс по умолчанию' (Системный: (UTC+03:00) Europe/Moscow), and 'Тема по умолчанию' (Голубая). At the bottom right are 'Назад' and 'Далее' buttons.

Рис. 528 – Настройки сервера Zabbix

После окончания установки на экране будет отображаться форма входа в веб-интерфейс управления системой мониторинга (рис. 529). Параметры доступа по умолчанию:

Логин: Admin

Пароль: zabbix

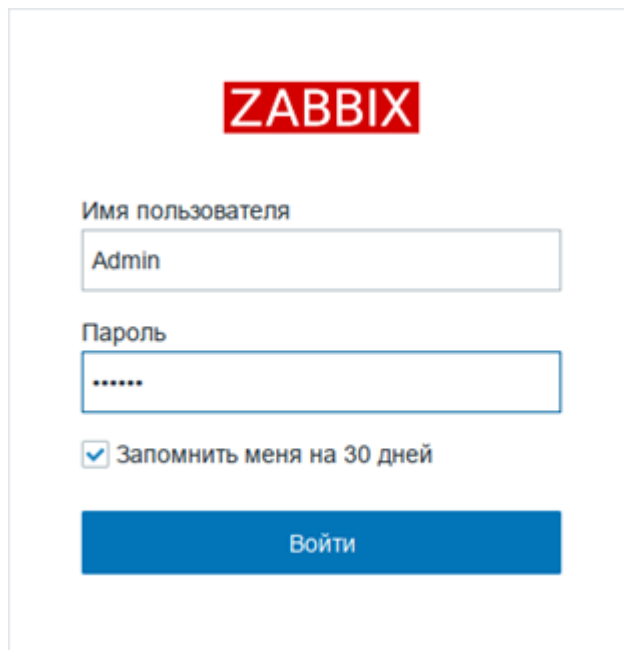


Рис. 529 – Форма входа в веб-интерфейс управления системой мониторинга

Войдя в систему, нужно сменить пароль администратора, завести других пользователей и затем можно переходить к настройкам Zabbix.

Примечание. В профиле пользователя можно настроить некоторые функции веб-интерфейса Zabbix, такие как язык интерфейса, цветовая тема, количество отображаемых строк в списках и т. п. Сделанные в профиле изменения будут применены только к пользователю, в профиле которого были сделаны эти изменения.

Чтобы собирать информацию с узлов, Zabbix-сервер использует информацию, получаемую от агентов. Чтобы добавить новый узел, следует установить на узел, который нужно мониторить, Zabbix-агент (п. 14.6) и добавить новый хост на Zabbix-сервере (п. 14.7, п. 14.8).

14.6. Установка Zabbix-агента (клиента)

Для установки Zabbix-агента нужно выполнить команду:

```
# apt-get install zabbix-agent
```

Если Zabbix-агент устанавливается не на сам сервер мониторинга, то в файле конфигурации агента `/etc/zabbix/zabbix_agentd.conf` нужно задать параметры сервера:

```
Server=<IP-сервера>
ServerActive=<IP-сервера>
Hostname=HostK.example.test
```

Где `HostK.example.test` – имя узла мониторинга, которое будет указано на Zabbix-сервере.

Примечание. Если параметр `Hostname` будет пустой или закомментирован, то узел добавится под системным именем.

Добавить Zabbix-агент в автозапуск и запустить его:

```
# systemctl enable --now zabbix_agentd.service
```

14.7. Добавление нового хоста на Zabbix-сервере

Каждый хост нужно зарегистрировать на Zabbix-сервере, сделать это можно, используя веб-интерфейс.

Информация о настроенных узлах сети в Zabbix доступна в разделе меню «Сбор данных» → «Узлы сети». Для добавления нового узла сети следует нажать кнопку «Создать узел сети» (рис. 530).

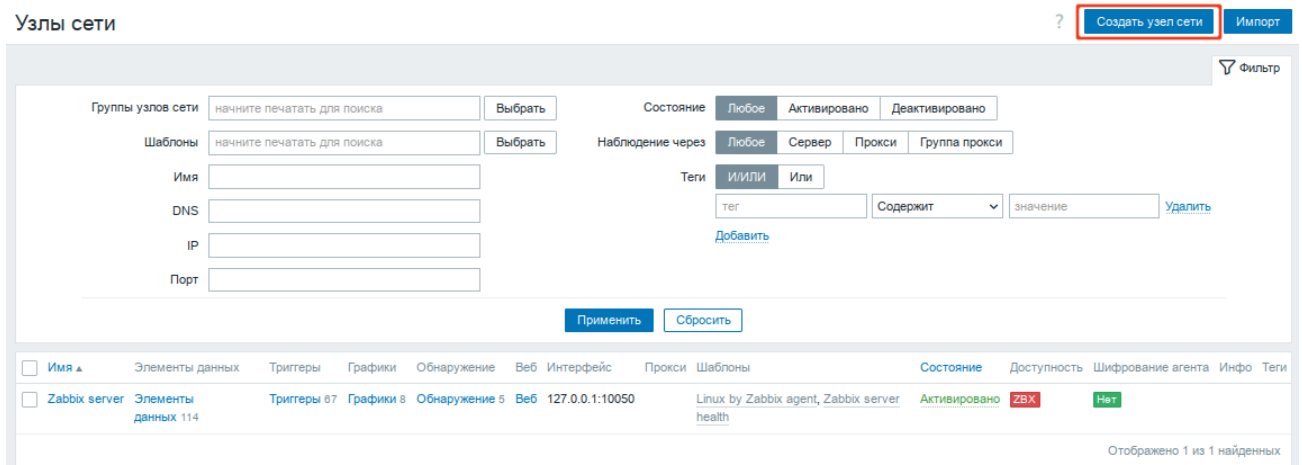


Рис. 530

В открывшемся окне нужно заполнить поля «Имя узла сети» и «IP адрес» согласно данным добавляемого хоста. Затем следует выбрать шаблон «Linux by Zabbix agent», добавить хост в определенную группу (выбрав одну из них из списка, либо создав новую группу) и нажать кнопку «Добавить» (рис. 531).

Примечание. В поле «Имя узла сети» ставится значение, которое указано в настройках агента (/etc/zabbix/zabbix_agentd.conf) в поле Hostname.

Примечание. Все права доступа назначаются на группы узлов сети, а не индивидуально узлам сети. Поэтому узел сети должен принадлежать хотя бы одной группе.

Новый узел сети

Узел сети IPMI Теги Макросы Инвентаризация Шифрование Преобразование значений

* Имя узла сети HostK.example.test

Видимое имя HostK

Шаблоны Linux by Zabbix agent × Выбрать
начните печатать для поиска

* Группы узлов сети Discovered hosts × Выбрать
начните печатать для поиска

Интерфейсы	Тип	IP адрес	DNS имя	Подключаться через	Порт	По умолчанию
Агент		192.168.0.113		IP DNS	10050	<input checked="" type="radio"/> Удалить

[Добавить](#)

Описание

Наблюдение через Сервер Прокси Группа прокси

Активировано

Добавить Отмена

Рис. 531 – Создание нового узла сети

Получение первых данных может занять до 60 секунд. Для того чтобы просмотреть собранные данные нужно перейти в раздел «Мониторинг» → «Последние данные», выбрать в фильтре нужный узел сети и нажать кнопку «Применить» (рис. 532).

Последние данные

Группы узлов сети:

Узлы сети:

Имя:

Теги:

Отображать теги: Имя тега:

Приоритет отображения тегов:

Состояние:

Подробная информация:

Подфильтр влияет только на отфильтрованные данные

УЗЛЫ СЕТИ
HostK 77

ТЕГИ
component 77 disk 16 filesystem 7 fstype 7 interface 9

ЗНАЧЕНИЯ ТЕГОВ
component: application 1 cpu 17 environment 1 memory 7 network 9 os 3 raw 4 security 1 storage 26 system 12
disk: ram 8 sda 8
filesystem: / 7
fstype: ext4 7
interface: enp0s3 9

СОСТОЯНИЕ
Не поддерживается 11 Нормальный 66

ДАННЫЕ
[Без данных](#) [С данными](#)

<input type="checkbox"/>	Узел сети	Имя ▲	Последняя проверка	Последнее значение	Изменение	Теги	Инфо
<input type="checkbox"/>	HostK	Available memory 📊	24с	784.89 MB		component: memory	График
<input type="checkbox"/>	HostK	Available memory in % 📊	23с	40.2246 %		component: memory	График
<input type="checkbox"/>	HostK	Checksum of /etc/passwd	25с	822fb73a4ea82d...		component: security	История
<input type="checkbox"/>	HostK	Context switches per second 📊	8с	226.912		component: cpu	График

Рис. 532 – Собранные данные

14.8. Авторегистрация узлов

В Zabbix существует механизм, который позволяет Zabbix-серверу начинать мониторинг нового оборудования автоматически, если на этом оборудовании имеется установленный Zabbix-агент. Такой подход позволяет добавлять новые узлы сети на мониторинг без какой-либо настройки Zabbix-сервера вручную по каждому отдельному узлу сети.

Для настройки авторегистрации необходимо перейти в раздел «Оповещения» → «Действия» → «Действия авторегистрации» и нажать на кнопку «Создать действие» (рис. 533).

На открывшейся странице на вкладке «Действия» заполнить поле «Имя». В поле «Условия» следует задать правила, по которым будут идентифицироваться регистрируемые hosts (рис. 534).

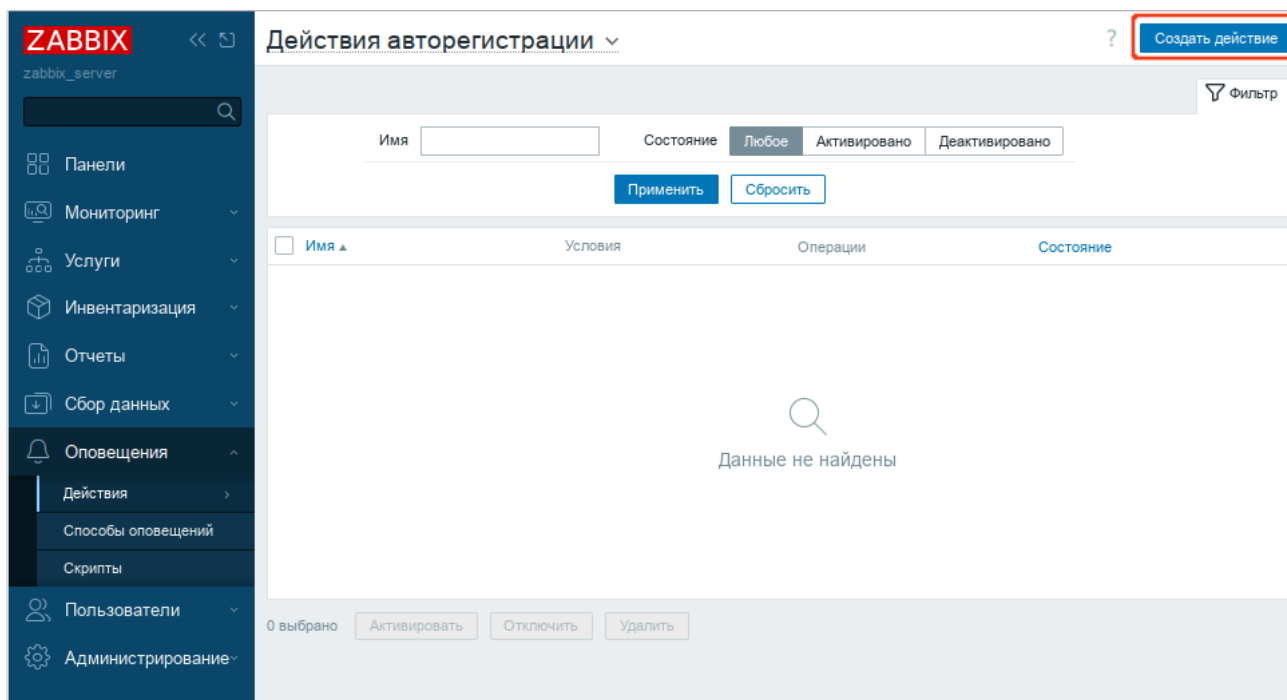


Рис. 533 – Авторегистрация узлов

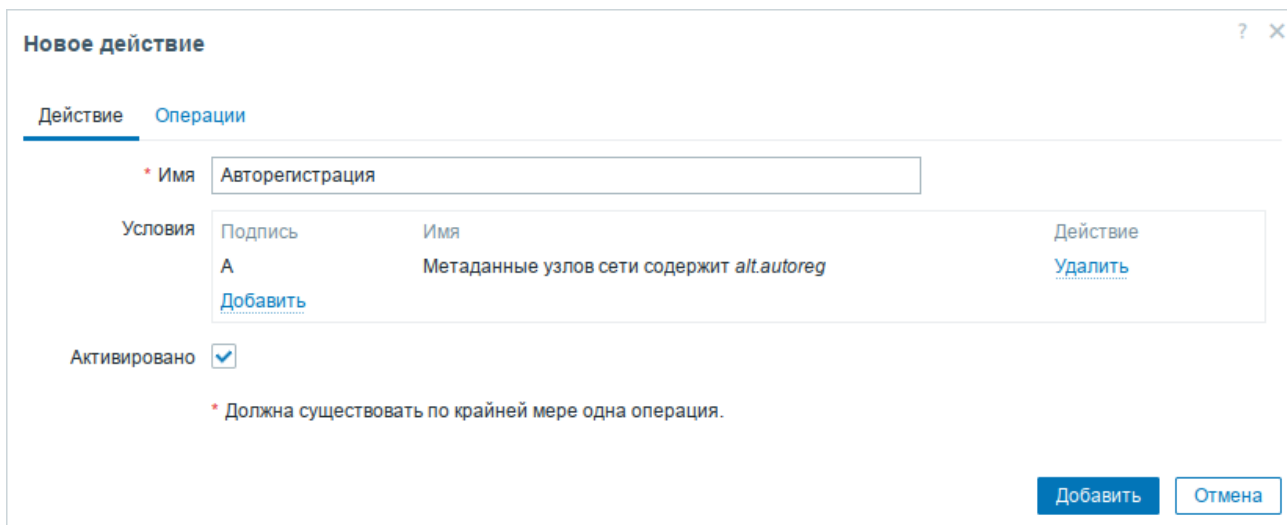


Рис. 534 – Условия идентификации узла

На вкладке «Операции» в поле «Операции» следует добавить правила, которые нужно применить при регистрации хоста. Например, для добавления узла, добавления его к группе «Discovered hosts» с присоединением к шаблону «Linux generic by Zabbix agent» (рис. 535).

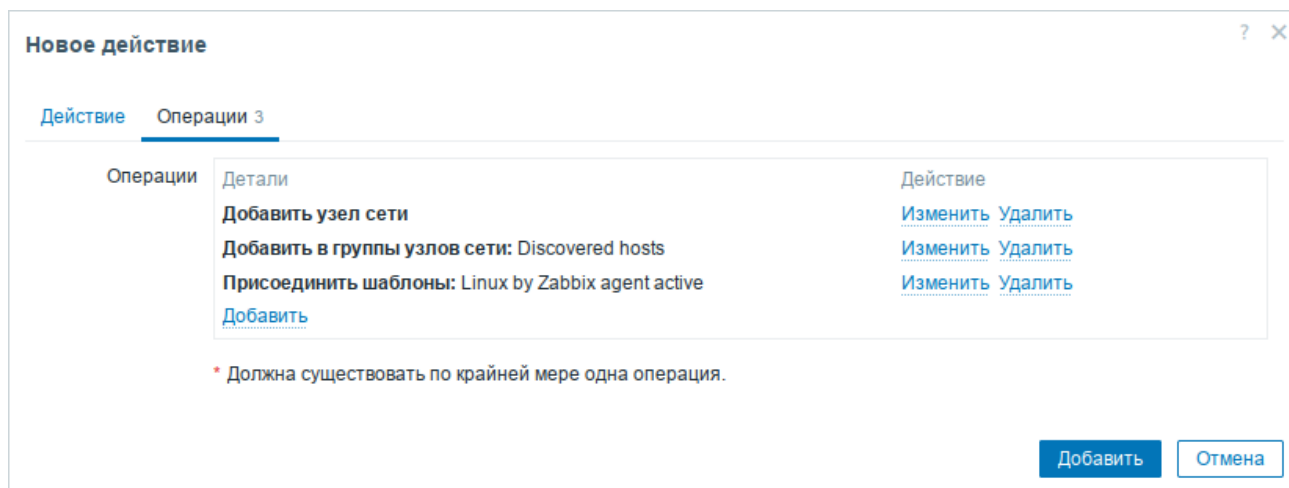


Рис. 535 – Правила, применяемые при регистрации узла

В конфигурационном файле агента `/etc/zabbix/zabbix_agentd.conf` следует указать следующие значения:

- в параметре `Hostname` – уникальное имя;
- в параметре `ServerActive` – IP-адрес сервера;
- в параметре `HostMetadata` – значение, которое было указано в настройках сервера (`HostMetadata=alt.autoreg`).

Перезапустить агент:

```
# systemctl restart zabbix_agentd.service
```

15. ОТКАЗОУСТОЙЧИВЫЙ КЛАСТЕР (HIGH AVAILABILITY) НА ОСНОВЕ RACEMAKER

Racemaker – менеджер ресурсов кластера (Cluster Resource Manager), задачей которого является достижение максимальной доступности управляемых им ресурсов и защита их от сбоев, как на уровне самих ресурсов, так и на уровне целых узлов кластера.

Ключевые особенности Racemaker:

- обнаружение и восстановление сбоев на уровне узлов и сервисов;
- возможность гарантировать целостность данных путем ограждения неисправных узлов;
- поддержка одного или нескольких узлов на кластер;
- поддержка нескольких стандартов интерфейса ресурсов (все, что может быть написано сценарием, может быть кластеризовано);
- независимость от подсистемы хранения – общий диск не требуется;
- поддержка кворумных и ресурсозависимых кластеров;
- автоматически реплицируемая конфигурация, которую можно обновлять с любого узла;
- возможность задания порядка запуска ресурсов, а также их совместимости на одном узле;
- поддерживает расширенные типы ресурсов: клоны (когда ресурс запущен на множестве узлов) и дополнительные состояния (master/slave и подобное);
- единые инструменты управления кластером с поддержкой сценариев.

Архитектура Racemaker представляет собой три уровня:

- кластеронезависимый уровень – на этом уровне располагаются ресурсы и их скрипты, которыми они управляются и локальный демон, который скрывает от других уровней различия в стандартах, использованных в скриптах;
- менеджер ресурсов (Racemaker) – реагирует на события, происходящие в кластере: отказ или присоединение узлов, ресурсов, переход узлов в сервисный режим и другие административные действия. Racemaker исходя из

сложившейся ситуации делает расчет наиболее оптимального состояния кластера и дает команды на выполнения действий для достижения этого состояния (остановка/перенос ресурсов или узлов);

- информационный уровень (Corgosync) – на этом уровне осуществляется сетевое взаимодействие узлов, т. е. передача сервисных команд (запуск/остановка ресурсов, узлов и т. д.), обмен информацией о полноте состава кластера (quorum) и т. д.

Узел (node) кластера представляет собой физический сервер или виртуальную машину с установленным Pacemaker. Узлы, предназначенные для предоставления одинаковых сервисов, должны иметь одинаковую конфигурацию.

Ресурсы, с точки зрения кластера, это все используемые сущности – сервисы, службы, точки монтирования, тома и разделы. При создании ресурса потребуется задать его класс, тип, провайдера и собственно имя с дополнительными параметрами. Ресурсы поддерживают множество дополнительных параметров: привязку к узлу (resource-stickiness), роли по умолчанию (started, stoped, master) и т. д. Есть возможности по созданию групп ресурсов, клонов (работающих на нескольких узлах) и т. п.

Связи определяют привязку ресурсов к узлу (location), порядок запуска ресурсов (ordering) и совместное их проживание на узле (colocation).

Ниже приведена инструкция по установке и настройке кластера в ОС Альт СП Сервер (64 бит (x86_64), AArch64 (ARMv8)).

15.1. Настройка узлов кластера

Рекомендации:

- дата и время между узлами в кластере должны быть синхронизированы;
- должно быть обеспечено разрешение имен узлов в кластере;
- сетевые подключения должны быть стабильными;
- у узлов кластера для организации изоляции (fencing) узла должны присутствовать функции управления питанием/перезагрузкой с помощью IPMI(ILO);

- следующие порты могут использоваться различными компонентами кластеризации: TCP-порты 2224, 3121 и 21064 и UDP-порт 5405 и должны быть открыты/доступны.

Примечание. В примере используется следующая конфигурация:

- node01 – первый узел кластера (IP 192.168.0.193/24);
- node02 – второй узел кластера (IP 192.168.0.189/24);
- node03 – третий узел кластера (IP 192.168.0.188/24);
- 192.168.0.251 – виртуальный IP-адрес, по которому будет отвечать один из узлов.

Дальнейшие действия следует выполнить на всех узлах кластера.

Примечание. Для изменения имени хоста без перезагрузки, можно воспользоваться утилитой `hostnamectl`:

```
# hostnamectl set-hostname ipa
```

Следует обеспечить взаимно однозначное прямое и обратное преобразование имен для всех узлов кластера. Желательно использовать DNS, в крайнем случае, можно обойтись соответствующими записями в локальных файлах `/etc/hosts` на каждом узле:

```
# echo "192.168.0.193 node01" >> /etc/hosts
# echo "192.168.0.189 node02" >> /etc/hosts
# echo "192.168.0.188 node03" >> /etc/hosts
```

Проверка правильности разрешения имен:

```
# ping node01
PING node01 (192.168.0.193) 56(84) bytes of data.
64 bytes from node01 (192.168.0.193): icmp_seq=1 ttl=64 time=0.635 ms
# ping node02
PING ipa2 (192.168.0.188) 56(84) bytes of data.
64 bytes from node02 (192.168.0.188): icmp_seq=1 ttl=64 time=0.352 ms
```

При настройке SSH-подключения для `root` по ключу нужно убрать комментарии в файле `/etc/openssh/sshd_config` для строк:

```
PermitRootLogin without-password
PubkeyAuthentication yes
AuthorizedKeysFile /etc/openssh/authorized_keys/%u
/etc/openssh/authorized_keys2/%u .ssh/authorized_keys .ssh/authorized_k
eys2
PasswordAuthentication yes
```

Кроме того, полезно добавить в `/etc/openssh/sshd_config` директиву:

```
AllowGroups sshusers
```

создать группу `sshusers`:

```
# groupadd sshusers
```

и добавить туда пользователей, которым разрешено подключаться по `ssh`:

```
# gpasswd -a <username> sshusers
```

Примечание. После редактирования файла `/etc/openssh/sshd_config` следует перезапустить службу `sshd`:

```
# systemctl restart sshd
```

Создать и активировать новый ключ SSH без пароля:

```
# ssh-keygen -t ecdsa -f ~/.ssh/id_ecdsa -N ""
```

ВАЖНО

Незащищенные ключи SSH (без пароля) не рекомендуются для серверов, открытых для внешнего мира.

Скопировать публичную часть SSH-ключа на другие узлы кластера:

```
# ssh-copy-id -i ~/.ssh/id_ecdsa.pub user@node02
```

```
# ssh-copy-id -i ~/.ssh/id_ecdsa.pub user@node03
```

В результате получаем возможность работы с домашними каталогами пользователя `user` удаленного узла – копировать к себе и от себя, удалять, редактировать и т. д.

Скопировать публичную часть SSH-ключа на все узлы кластера для администратора. Для этого подключиться к каждому узлу и под `root` скопировать публичную часть ключа:

```
# ssh user@node02
user@node02 $ su -
node02      #      cat      /home/user/.ssh/authorized_keys      >>
/root/.ssh/authorized_keys
node02 # exit
user@node02 $ exit
```

Примечание. Каталог `/root/.ssh` при этом должен существовать.

Убедиться, что теперь можно запускать команды удаленно, без пароля:

```
# ssh node02 -- uname -n
node02
```

15.2. Установка кластерного ПО и создание кластера

Для управления кластером Pacemaker можно использовать утилиту pcs.

Установить на всех узлах пакеты:

```
# apt-get install corosync resource-agents pacemaker pcs
```

Примечание. Пакет resource-agent содержит агенты ресурсов (набор скриптов) кластера, соответствующие спецификации Open Cluster Framework (OCF), используемые для взаимодействия с различными службами в среде высокой доступности, управляемой менеджером ресурсов Pacemaker. Если есть необходимость управлять дополнительными ресурсами, следует установить недостающий пакет resource-agents-*:

```
apt-cache search resource-agents*
```

Пакет pcs (pacemaker/corosync configuration system) – утилита для управления, настройки и мониторинга кластера. Управляется через командную строку.

При установке Pacemaker автоматически будет создан пользователь hacluster. Для использования pcs нужно задать пароль пользователю hacluster (одинаковый на всех узлах):

```
# passwd hacluster
```

Запустить и добавить в автозагрузку службу pcsd:

```
# systemctl enable --now pcsd
```

Настроить аутентификацию (на одном узле):

```
# pcs host auth node01 node02 node03 -u hacluster
```

```
Password:
```

```
node02: Authorized
```

```
node01: Authorized
```

```
node03: Authorized
```

После этого кластером можно управлять с одного узла.

Создать кластер:

```
# pcs cluster setup newcluster node01 node02 node03
```

```
Destroying cluster on hosts: 'node01', 'node02', 'node03'...
```

```
node03: Successfully destroyed cluster
```

```
node01: Successfully destroyed cluster
```

```
node02: Successfully destroyed cluster
```

```
Requesting remove 'pcsd settings' from 'node01', 'node02', 'node03'
```

```
node01: successful removal of the file 'pcsd settings'
```

```
node03: successful removal of the file 'pcsd settings'
```

```
node02: successful removal of the file 'pcsd settings'
```

```
Sending 'corosync authkey', 'pacemaker authkey' to 'node01', 'node02', 'node03'
```

ЛКНВ.11100-01 90 03

```
node01: successful distribution of the file 'corosync authkey'  
node01: successful distribution of the file 'pacemaker authkey'  
node03: successful distribution of the file 'corosync authkey'  
node03: successful distribution of the file 'pacemaker authkey'  
node02: successful distribution of the file 'corosync authkey'  
node02: successful distribution of the file 'pacemaker authkey'  
Sending 'corosync.conf' to 'node01', 'node02', 'node03'  
node01: successful distribution of the file 'corosync.conf'  
node02: successful distribution of the file 'corosync.conf'  
node03: successful distribution of the file 'corosync.conf'  
Cluster has been successfully set up.
```

Запустить кластер:

```
# pcs cluster start --all  
  
node02: Starting Cluster...  
node03: Starting Cluster...  
node01: Starting Cluster...
```

Настройка автоматического включения кластера при загрузке:

```
# pcs cluster enable --all  
  
node01: Cluster Enabled  
node02: Cluster Enabled  
node03: Cluster Enabled
```

Проверка состояния кластера:

```
# pcs status cluster  
  
Cluster Status:  
  Cluster Summary:  
    * Stack: corosync (Pacemaker is running)  
    * Current DC: node01 (version 2.1.7-alt1-2.1.7) - partition with  
quorum  
    * Last updated: Thu Nov 21 17:03:58 2024 on node03  
    * Last change: Thu Nov 21 17:03:39 2024 by hacluster via hacluster  
on node01  
    * 3 nodes configured  
    * 0 resource instances configured  
  Node List:  
    * Online: [ node01 node02 node03 ]  
  
PCSD Status:  
  node03: Online  
  node01: Online  
  node02: Online
```

Проверка синхронизации узлов кластера:

```
# corosync-cmapctl | grep members  
  
runtime.members.1.config_version (u64) = 0  
runtime.members.1.ip (str) = r(0) ip(192.168.0.193)  
runtime.members.1.join_count (u32) = 1  
runtime.members.1.status (str) = joined  
runtime.members.2.config_version (u64) = 0  
runtime.members.2.ip (str) = r(0) ip(192.168.0.189)
```

```
runtime.members.2.join_count (u32) = 1
runtime.members.2.status (str) = joined
runtime.members.3.config_version (u64) = 0
runtime.members.3.ip (str) = r(0) ip(192.168.0.188)
runtime.members.3.join_count (u32) = 1
runtime.members.3.status (str) = joined
```

15.3. Настройка основных параметров кластера

Настройки кластера можно просмотреть, выполнив команду:

```
# pcs property
Cluster Properties: cib-bootstrap-options
  cluster-infrastructure=corosync
  cluster-name=newcluster
  dc-version=2.1.7-alt1-2.1.7
  have-watchdog=false
```

15.3.1. Кворум

Кворум определяет минимальное число работающих узлов в кластере, при котором кластер считается работоспособным. По умолчанию, кворум считается неработоспособным, если число работающих узлов меньше половины от общего числа узлов.

Кластер, состоящий из двух узлов, будет иметь кворум только тогда, когда оба узла работают. По умолчанию, если нет кворума, Pacemaker останавливает ресурсы. Чтобы этого избежать, можно при настройке Pacemaker указать, что наличие или отсутствие кворума не должно учитываться:

```
# pcs property set no-quorum-policy=ignore
```

15.3.2. Настройка STONITH

Для корректной работы узлов с общим хранилищем, нужно настроить механизм STONITH. Этот механизм позволяет кластеру физически отключить не отвечающий на запросы узел, чтобы не повредить данные на общем хранилище. Отключить STONITH, пока он не настроен можно, выполнив команду:

```
# pcs property set stonith-enabled=false
```

ВАЖНО

В реальной системе нельзя использовать конфигурацию с отключенным STONITH. Отключенный параметр на самом деле не отключает функцию, а только лишь эмулирует ее срабатывание при определенных обстоятельствах.

15.3.3. Настройка ресурсов

В данном разделе рассмотрена настройка ресурса, который будет управлять виртуальным IP-адресом. Этот адрес будет мигрировать между узлами, предоставляя одну точку входа к ресурсам, заставляя работать несколько узлов как одно целое устройство для сервисов.

Команда создания ресурса виртуального IP-адреса с именем ClusterIP с использованием алгоритма ресурсов ocf (каждые 20 минут производить мониторинг работы, в случае выхода из строя узла нужно виртуальный IP переключить на другой узел):

```
# pcs resource create ClusterIP ocf:heartbeat:IPaddr2
ip=192.168.0.251 cidr_netmask=24 op monitor interval=20s
```

Список доступных стандартов ресурсов:

```
# pcs resource standards
lsb
ocf
service
systemd
```

Список доступных поставщиков сценариев ресурсов OCF:

```
# pcs resource providers
heartbeat
pacemaker
redhat
```

Получить список всех агентов ресурсов, доступных для определенного поставщика OCF можно, выполнив команду:

```
# pcs resource agents ocf:heartbeat
aliyun-vpc-move-ip
anything
AoEtarget
...
Xinetd
zabbixserver
ZFS
```

Статус кластера, с добавленным ресурсом:

```
# pcs status
Cluster name: newcluster
Cluster Summary:
* Stack: corosync (Pacemaker is running)
```

ЛКНВ.11100-01 90 03

```
* Current DC: node01 (version 2.1.7-alt1-2.1.7) - partition with
quorum
* Last updated: Thu Nov 21 17:16:45 2024 on node03
* Last change: Thu Nov 21 17:15:07 2024 by root via root on node03
* 3 nodes configured
* 1 resource instance configured
```

Node List:

```
* Online: [ node01 node02 node03 ]
```

Full List of Resources:

```
* ClusterIP (ocf:heartbeat:IPaddr2): Started node01
```

Daemon Status:

```
corosync: active/enabled
pacemaker: active/enabled
pcsd: active/enabled
```

Если остановить кластер на узле node01:

```
# pcs cluster stop node01
```

```
node01: Stopping Cluster (pacemaker)...
```

```
node01: Stopping Cluster (corosync)...
```

ClusterIP начнет работать на узле node02 (переключение произойдет автоматически). Проверка статуса на узле node02:

```
# pcs status
```

```
Cluster name: newcluster
```

Cluster Summary:

```
* Stack: corosync (Pacemaker is running)
* Current DC: node03 (version 2.1.7-alt1-2.1.7) - partition with
quorum
* Last updated: Thu Nov 21 17:17:58 2024 on node03
* Last change: Thu Nov 21 17:15:07 2024 by root via root on node03
* 3 nodes configured
* 1 resource instance configured
```

Node List:

```
* Online: [ node02 node03 ]
```

```
* OFFLINE: [ node01 ]
```

Full List of Resources:

```
* ClusterIP (ocf:heartbeat:IPaddr2): Started node02
```

Daemon Status:

```
corosync: active/enabled
pacemaker: active/enabled
pcsd: active/enabled
```

16. POSTGRESQL

В качестве СУБД в составе ОС Альт СП используется PostgreSQL.

СУБД PostgreSQL предназначена для создания и управления реляционными БД и предоставляет многопользовательский доступ к расположенным в них данным. Данные в реляционной БД хранятся в отношениях (таблицах), состоящих из строк и столбцов. При этом единицей хранения и доступа к данным является строка, состоящая из полей, идентифицируемых именами столбцов. Кроме таблиц, существуют другие объекты БД (виды, процедуры), которые предоставляют доступ к данным, хранящимся в таблицах.

Для работы СУБД на НЖМД выделяется область для хранения БД, называемая «кластером БД». Кластер БД является набором БД, управляемых одним экземпляром сервера СУБД. Настройка работы отдельного экземпляра сервера СУБД так же определяется в рамках кластера соответствующими конфигурационными файлами.

16.1. Состав

СУБД PostgreSQL состоит из нескольких компонентов:

- postgresql – сервисная служба, реализующая непосредственно сервер БД;
- libpq – клиентская библиотека, предоставляющая доступ к серверу СУБД;
- набор серверных утилит для управления работой сервера и создания кластеров БД;
- набор клиентских утилит для создания и управления БД.

16.2. Настройка

Настройка сервера СУБД осуществляется установкой параметров в конфигурационном файле `postgresql.conf`. В дополнение к файлу `postgresql.conf` в PostgreSQL используется еще два конфигурационных файла, которые контролируют аутентификацию клиента.

По умолчанию все эти три файла находятся в каталоге данных кластера БД или в соответствующем кластеру конфигурационном каталоге, например, `/etc/postgresql/x.x/main`.

За расположение указанных файлов отвечают конфигурационные параметры, описанные ниже:

- `data_directory` – определяет каталог для хранения данных;
- `config_file` – определяет основной конфигурационный файл сервера (`postgresql.conf`), значение этого параметра может быть задано только в командной строке `postgres`;
- `hba_file` – определяет конфигурационный файл для аутентификации по узлам (`pg_hba.conf`);
- `ident_file` – определяет конфигурационный файл для аутентификации по методу `ident` (`pg_ident.conf`);
- `external_pid_file` – определяет имя дополнительного файла с идентификатором процесса, который сервер создает для использования программами администрирования сервера.

16.3. Использование postgresql

16.3.1. Конфигурирование сервера

Установить пакет `postgresql-deploy-cert` (если при установке ОС Альт СП релиз 10 Сервер не была отмечена группа пакетов «Сервер Postgresql»):

```
# apt-get install postgresql-deploy-cert
```

Разворачивание системы управления базами данных (СУБД) `postgresql` выполняется командой:

```
# deploy postgresql-cert
```

ввести и записать пароль для `postgres`.

Раскомментировать строку `default_realm` в `/etc/krb5.conf` и изменить значение на `POSTGRESQL`:

```
default_realm = POSTGRESQL
```

Выполнить создание базы данных (БД) ключей для `realm POSTGRESQL`. Во время выполнения команды будет запрошен пароль от `master key`, необходимо

указать пароль, который был указан при разворачивании postgresql через команду deploy:

```
# kdb5_util create -s -r POSTGRESQL
```

16.3.2. Конфигурирование ролей

16.3.2.1. Конфигурирование администратора СУБД

Отредактировать файл `/etc/hosts` и привести его к виду:

```
localhost 127.0.0.1
```

Выполнить создание принципала `pgadmin` и `postgres`:

```
# kadmin.local ank pgadmin/admin
```

```
# kadmin.local ank postgres/admin
```

Выполнить перезапуск сервиса `postgresql` и запуск сервиса `krb5kdc.service`:

```
# systemctl restart postgresql
```

```
# systemctl start krb5kdc.service
```

Выполнить создание пользователя СУБД `pgadmin`:

```
# createuser -U postgres --superuser pgadmin
```

ввести пароль, который был задан при создании базы при помощи `deploy` (см. п. 16.3.1).

Выполнить перезапуск сервиса `postgresql`:

```
# systemctl restart postgresql
```

Создать парольную политику для `kerberos`:

```
# kadmin.local add_policy -minlength 8 -minclasses 4 -maxfailure 4 \  
-failurecountinterval 180 -lockoutduration 3600 lockout_policy
```

Где:

- `--minlength` – минимальная длина пароля. В примере – 8 символов;
- `--minclasses` – минимальное количество классов символов, разрешенных в пароле. В примере пароль должен содержать символы не менее четырех различных классов (например, строчные буквы, заглавные буквы, цифры, специальные символы);
- `--maxfailure` – максимальное количество неудачных попыток ввода пароля перед блокировкой учетной записи. В данном случае – 4;

- `--failurecountinterval` – интервал времени в секундах, в течение которого учитываются неудачные попытки ввода пароля. Если неудачная попытка аутентификации происходит после того, как с момента предыдущей неудачи прошло `failurertime`, количество неудачных попыток аутентификации сбрасывается до 1. Интервал подсчета неудач, равный 0, означает «всегда». В данном случае – 180 секунд (3 минуты);
- `--lockoutduration 3600` – длительность блокировки учетной записи в секундах. Длительность 0 означает, что учетная запись будет заблокирована навсегда. В данном случае – 3600 секунд (1 час).

Добавить сервисы в автозапуск:

```
# systemctl enable postgresql --now
# systemctl enable krb5kdc --now
# systemctl enable kadmin --now
```

Создать пользователей `pgadmin`, `admindb1`, `userdb1` и задать им пароли:

```
# useradd pgadmin
# useradd admindb1
# useradd userdb1
# passwd pgadmin
# passwd admindb1
# passwd userdb1
```

16.3.3. Создание администратора БД и БД

От имени учетной записи `pgadmin` (администратор СУБД) выполнить создание принципа `admindb1`:

```
$ kadmin ank +requires_preauth -policy lockout_policy admindb1/admin
```

ввести пароль принципа `pgadmin` и новый пароль для `admindb1`. Пароль для `admindb1` должен удовлетворять парольной политике для `kerberos`.

Создать пользователя `admindb1` в СУБД:

```
$ createuser admindb1 --createrole
```

при запросе пароля следует ввести пароль принципа `pgadmin`.

Выполнить создание БД:

```
$ createdb -O admindb1 db1
```

при запросе пароля следует ввести пароль принципа `pgadmin`.

16.3.4. Работа роли администратора БД

Выполнить авторизацию в ОС от имени учетной записи admindb1.

Создать принципал для пользователя userdb1:

```
$ kadmin ank +requires_preauth -policy lockout_policy userdb1/user
```

при запросе пароля следует ввести пароль принципала admindb1 и новый пароль userdb1. Пароль для userdb1 должен удовлетворять парольной политике для kerberos.

```
$ createuser userdb1
```

при запросе пароля следует ввести пароль принципала admindb1.

Подключиться к БД и назначить пользователю userdb1 права на БД (при запросе пароля следует ввести пароль принципала admindb1):

```
$ psql db1
```

```
db1=> grant all on database db1 to userdb1;
db1=> grant all on schema public to userdb1;
db1=> \q
```

16.4. Настройка кластера postgresql

В качестве кластера выступают три ноды (узла) с установленной группой пакетов «Сервер Postgresql». В качестве сервера аутентификации Kerberos в примере далее выступает arm3(node3).

Следующие действия следует выполнить на всех трех нодах:

1) прописать соответствие имени хостов их IP-адресам в файл /etc/hosts:

```
192.168.10.1   arm1.POSTGRESQL arm1
192.168.10.2   arm2.POSTGRESQL arm2
192.168.10.3   arm3.POSTGRESQL arm3
```

2) создать каталог:

```
# mkdir /srv/pgsql
```

3) развернуть postgresql:

```
# deploy postgresql-cert
```

4) создать символические ссылки и изменить права для PGDATA:

```
# mv /var/lib/pgsql/data /srv/pgsql
# ln -s /srv/pgsql/data /var/lib/pgsql/data
# chown postgres:postgres -R /var/log/postgres
# chown postgres:postgres -R /srv/pgsql
```

- 5) переключить `sudo` в режим работы `public`, изменить оболочку для пользователя `postgres` и сгенерировать ключи SSH:

```
# control sudo public
# usermod -s /bin/bash postgres
# su - postgres -c 'ssh-keygen -t ed25519'
```

- 6) записать открытый ключ с каждой ноды в файл `/var/lib/pgsql/.ssh/authorized_keys`.

Файл должен иметь следующий вид, на каждой из нод:

```
# cat /var/lib/pgsql/.ssh/authorized_keys
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIJQaH2TiiTJUkPRqhXgUMkjnLBsWrkxw2Vzyu2ThW7Bw postgres@arm1.POSTGRESQL
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIJih4kd9QL8Iam6pkDuJgvaXu88gnNJ9PSO7Ds30XLFn postgres@arm2.POSTGRESQL
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIAtPE8584kT5JHVrs4F86NRDARTfM1F4ohvtP3bASEd3 postgres@arm3.POSTGRESQL
```

- 7) выполнить SSH-подключение с каждой на каждую ноду для появления записей в `known_hosts`. Для этого выполнить команды:

```
# su - postgres
$ ssh postgres@arm1
$ ssh postgres@arm2
$ ssh postgres@arm3
```

На ноде `arm1` в файле `/var/lib/pgsql/data/pg_hba.conf` добавить правила для сетевого подключения:

```
host      all             all    192.168.10.0/24    pam pamservice=postgres
host      replication   all    192.168.10.0/24    pam pamservice=postgres
```

На ноде `arm1` в файле `/var/lib/pgsql/data/postgresql.conf` изменить параметр `listen_addresses` на:

```
listen_addresses = '*'
```

Выполнить перезапуск службы:

```
# systemctl restart postgresql
```

Далее в руководстве нода будет `arm1` определена как `primary` СУБД, ноды `arm2` и `arm3` – `standby`.

На всех нодах раскомментировать строчку `default_realm` в `/etc/krb5.conf` и изменить значение на `POSTGRESQL`:

```
default_realm = POSTGRESQL
```

На всех нодах в файле `/etc/krb5.conf.d/postgresql_krb5.conf` параметры `kdc` и `admin_server` заменить на `arm3`.

Пример файла:

```
# cat /etc/krb5.conf.d/postgresql_krb5.conf
[libdefaults]
default_realm=POSTGRESQL
[realms]
  POSTGRESQL = {
    kdc = arm3
    admin_server = arm3:749
  }
```

На ноде `arm3` в файле `/var/lib/kerberos/krb5kdc/kdc.conf` заменить `EXAMPLE.COM` на `POSTGRESQL`.

На ноде `arm3`, выступающей в роли сервера аутентификации Kerberos, выполнить настройки из п. 16.3 и выполнить создание принципала для роли СУБД `repmgr`, которая будет выполнять репликацию нод:

```
# kadmin.local ank +requires_preauth -policy lockout_policy
repmgr/admin
```

На всех нодах создать файл с правами `600` и владельцем `postgres:postgres` `/var/lib/pgsql/.pgpass`:

```
# su - postgres -c 'touch /var/lib/pgsql/.pgpass'
# chmod 600 /var/lib/pgsql/.pgpass
```

Со следующим содержимым файла:

```
*:5432:repmgrdb:repmgr:ПАРОЛЬ_ЧТО_НАЗНАЧЕН_В_Kerberos
*:5432:replication:repmgr:ПАРОЛЬ_ЧТО_НАЗНАЧЕН_В_Kerberos
```

На ноде `arm1` (`primary`) выполнить создание пользователей СУБД (при запросе пароля следует ввести пароль принципала `repmgr`):

```
# createuser -U postgres --superuser pgadmin
# createuser -U pgadmin --superuser repmgr
# createdb -U repmgr repmgrdb
```


Убедиться, что arm1 является primary node:

```
# su - postgres -c 'repmgr -f /etc/repmgr/repmgr.conf cluster show'
```

```
ID | Name   | Role      | Status      | Upstream | Location | Priority
---+-----+-----+-----+-----+-----+-----
 1 | arm1   | primary   | * running   |          | default  | 100
```

Добавить ноды arm2 и arm3 в кластер как standby ноды:

```
# systemctl stop postgresql
# rm -rf /var/lib/pgsql/data/*
# su - postgres -c 'repmgr -f /etc/repmgr/repmgr.conf -h arm1 -U
repmgr -d repmgrdb standby clone'
```

Вся иерархия файлов СУБД будет скопирована на ведомую ноду утилитой pg_basebackup.

Выполнить запуск сервиса postgresql:

```
# systemctl start postgresql
```

Выполнить на каждой standby ноде регистрацию нод в кластере:

```
# su - postgres -c 'repmgr -f /etc/repmgr/repmgr.conf standby
register'
# systemctl enable repmgr.service --now
```

17. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ОС

17.1. Управление системными сервисами, основные команды

17.1.1. Сервисы

Сервисы – это программы, которые запускаются и останавливаются через инициализированные скрипты, расположенные в каталоге `/etc/init.d`. Многие из этих сервисов запускаются на этапе старта ОС Альт СП.

Каталог `/sbin/service` обеспечивает интерфейс (взаимодействие) пользователя с инициализированными скриптами. В свою очередь, скрипты обеспечивают интерфейс для управления сервисами, предоставляя пользователю опции для запуска, остановки, перезапуска, запроса состояния сервиса и выполнения других воздействий на сервис.

Инициализированный скрипт сервиса `openssh` имеет следующие опции:

```
/etc/init.d/sshd
Usage: sshd
{start|stop|reload|restart|condstop|condrestart|condreload|check|
status}
```

Текущее состояние всех системных служб в ОС Альт СП можно просмотреть с помощью команды `systemctl`:

```
systemctl
...
sshd.service
loaded active running   OpenSSH server daemon
  systemd-binfmt.service
loaded active exited   Set Up Additional Binary F
  systemd-fsck-root.service
loaded active exited   File System Check on Roo
...
```

Информация о запущенности и включенности сервисов может быть получена или изменена с помощью команды `systemctl`. Например, для службы удаленного доступа `ssh` установки по умолчанию выглядят следующим образом:

```
/sbin/systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/lib/systemd/system/sshd.service; enabled;
 vendor preset: ena
```

```
Active: active (running) since Mon 2019-04-01 09:48:34 MSK; 4h
0min ago
```

```
Process: 921 ExecStartPre=/usr/sbin/sshd -t (code=exited,
status=0/SUCCESS)
```

```
Process: 904 ExecStartPre=/usr/bin/ssh-keygen -A (code=exited,
status=0/SUCCESS)
```

```
Main PID: 942 (sshd)
```

```
CGroup: /system.slice/sshd.service
```

```
└─942 /usr/sbin/sshd -D
```

Сервис sshd запускается автоматически. Для того чтобы отключить его автоматический запуск сервиса, можно воспользоваться следующей опцией команды systemctl:

```
/sbin/systemctl disable sshd
```

Запуск, остановка, перезапуск и перезагрузка настроек служб выполняются соответственно командами:

```
/sbin/systemctl start <служба>
/sbin/systemctl stop <служба>
/sbin/systemctl restart <служба>
/sbin/systemctl reload <служба>
```

17.1.2. Команды

Далее приведены основные команды, используемые в ОС Альт СП:

- ar – создание и работа с библиотечными архивами;
- at – формирование или удаление отложенного задания (см. п. 17.8.2);
- awk – язык обработки строковых шаблонов;
- batch – планирование команд в очереди загрузки (см. п. 17.8.3);
- bc – строковый калькулятор;
- chfn – управление информацией учетной записи (имя, описание);
- chsh – управление выбором командного интерпретатора (по умолчанию – для учетной записи);
- cut – разбивка файла на секции, задаваемые контекстными разделителями;
- df – вывод отчета об использовании дискового пространства;
- dmesg – вывод содержимого системного буфера сообщений;
- du – вычисление количества использованного пространства элементов ФС;

- `echo` – вывод содержимого аргументов на стандартный вывод;
- `egrep` – поиск в файлах содержимого согласно регулярным выражениям;
- `fgrep` – поиск в файлах содержимого согласно фиксированным шаблонам;
- `file` – определение типа файла;
- `find` – поиск файла по различным признакам в иерархии каталогов (см. п. 17.5.1);
- `gettext` – получение строки интернационализации из каталогов перевода;
- `grep` – вывод строки, содержащей шаблон поиска (см. п. 17.4.4);
- `groupadd` – создание новой учетной записи группы;
- `groupdel` – удаление учетной записи группы;
- `groupmod` – изменение учетной записи группы;
- `groups` – вывод списка групп;
- `gunzip` – распаковка файла;
- `gzip` – упаковка файла;
- `hostname` – вывод и задание имени хоста;
- `install` – копирование файла с установкой атрибутов;
- `ipcrm` – удаление ресурса IPC;
- `ipcs` – вывод характеристик ресурса IPC;
- `kill` – прекращение выполнения процесса (см. п. 17.2.6);
- `killall` – удаление процессов по имени (см. п. 17.2.6);
- `lpr` – система печати;
- `ls` – вывод содержимого каталога (см. п. 17.3.1);
- `lsb_release` – вывод информации о дистрибутиве;
- `m4` – запуск макропроцессора;
- `md5sum` – генерация и проверка MD5-сообщения;
- `mknod` – создание файла специального типа (см. п. 17.4.6);
- `mktemp` – генерация уникального имени файла;
- `more` – постраничный вывод содержимого файла;
- `mount` – монтирование ФС (см. п. 17.3.12);

- `msgfmt` – создание объектного файла сообщений из файла сообщений;
- `newgrp` – смена идентификатора группы;
- `nice` – изменение приоритета процесса перед его запуском (см. п. 17.2.4);
- `nohup` – работа процесса после выхода из системы (см. п. 17.2.3);
- `od` – вывод содержимого файла в восьмеричном и других видах;
- `passwd` – смена пароля учетной записи (см. п. 21.3);
- `patch` – применение файла описания изменений к оригинальному файлу;
- `pidof` – вывод идентификатора процесса по его имени;
- `ps` – вывод информации о процессах (см. п. 17.2.2);
- `renice` – изменение уровня приоритета процесса (см. п. 17.2.5);
- `rm` – удаление файлов или каталогов;
- `sed` – строковый редактор;
- `sendmail` – транспорт системы электронных сообщений;
- `sh` – командный интерпретатор;
- `shutdown` – команда останова системы;
- `srm` – безопасная перезапись/переименование/удаление целевого файла;
- `su` – изменение идентификатора запускаемого процесса (см. п. 21.2.4);
- `sync` – сброс системных буферов на носители;
- `tar` – файловый архиватор (см. п. 17.6.1);
- `umount` – размонтирование ФС;
- `useradd` – создание новой учетной записи или обновление существующей (см. п. 21.3);
- `userdel` – удаление учетной записи и соответствующих файлов окружения (см. п. 21.3);
- `usermod` – модификация информации об учетной записи (см. п. 21.3);
- `w` – список пользователей, кто в настоящий момент работает в системе и с какими файлами;
- `who` – вывод списка пользователей системы (см. п. 17.2.1).

Узнать об опциях команд можно с помощью команды `man`.

17.2. Администрирование многопользовательской и многозадачной среды

17.2.1. Команда `who`

Для получения списка пользователей, работающих в ОС, используется команда `who`, которая позволяет вывести в консоль идентификаторы активных пользователей, терминалы и время входа в систему.

Для получения списка пользователей, зарегистрировавшихся в системе, нужно выполнить команду `who`. Задавая различные опции, с помощью команды `who` можно получить информацию о времени начала и конца сеансов работы пользователей, перезагрузок, корректировках системных часов, а также о других процессах, порожденных процессом `init`.

Синтаксис команды `who`:

```
who [-u] [-T] [-l] [-H] [-q] [-p] [-d] [-b] [-r] [-t] [-a] [-s]
[имя файла]
```

Опции команды `who` приведены в таблице 100.

Т а б л и ц а 100 – Опции команды `who`

Опция	Описание
<code>-u</code>	Позволяет вывести информацию о пользователях, которые в настоящее время являются активными (работают в ОС).
<code>-H</code>	Опция, аналогичная опции <code>-u</code> (дополнительно в консоль выводится название столбцов).
<code>-s</code>	Позволяет вывести в консоль имена активных пользователей и терминальных линий, а также время и дату начала сессии пользователей.
<code>-t</code>	Позволяет вывести информацию о последней корректировке системных часов администратором.
<code>-r</code>	Позволяет вывести текущий уровень выполнения процесса <code>init</code> , кроме этого, будут выведены идентификатор процесса, системный код завершения и пользовательский код завершения процесса.
<code>-a</code>	Позволяет обработать файл <code>/etc/utmp</code> или файл, указанный в команде, считая, что все опции (кроме <code>THqs</code>) включены.
<code>-b</code>	Позволяет вывести время и дату последней загрузки системы.
<code>-d</code>	Позволяет вывести информацию обо всех процессах, которые прекратили существование и не были заново порождены процессом <code>init</code> .

Окончание таблицы 100

Опция	Описание
-P	Позволяет вывести список всех других процессов, активных в настоящий момент, которые были порождены процессом init.
-q	Позволяет вывести имена и количество пользователей, работающих в настоящий момент в системе.
-l	Позволяет вывести список линий, на которых система ожидает входа в нее какого-либо пользователя.
-T	Аналогична опции -s с той разницей, что дополнительно в позиции STATE выводится информация о состоянии терминальной линии.

Сообщения, выводимые после выполнения команды `who`, имеют следующий формат:

```
NAME [STATE] LINE TIME [IDLE] [PID] [COMMENT] [EXIT]
```

Информация `NAME`, `LINE` и `TIME` выводится при использовании всех опций, кроме `-q`, `STATE` — только при использовании опции `-T`, `IDLE` и `PID` — только при использовании опции `-u` и `-l`, `COMMENT` и `EXIT` — только при использовании опции `-a`.

В сообщениях, выводимых после выполнения команды `who`, фигурируют следующие параметры:

- `NAME` — имя пользователя;
- `STATE` — состояние терминальной линии (состояние — возможность передавать сообщения на терминал от кого-либо другого терминала: состояние «+» — свидетельствует о том, что терминалу может передавать сообщения любой другой терминал, состояние «-» — терминалу сообщения передаваться не могут; пользователь `root` может передавать сообщения во все линии, которым отвечает состояние «+» или «-»; при обнаружении неисправной линии выводится «?»);
- `LINE` — имя терминальной линии;
- `TIME` — время и дата начала сеанса работы пользователя в системе;
- `IDLE` — время, прошедшее со времени последней активной работы пользователя;
- `PID` — идентификатор процесса входной оболочки пользователя;

- COMMENT – комментарий, характеризующий данную линию (если таковые имеются в файле `/etc/inittab` – этот файл может содержать, например, сведения о местоположении терминала, телефонном номере комнаты или о типе физического терминала).

Чтобы получить сведения о сеансе, учетной записи и PID запущенного процесса нужно выполнить следующую команду:

```
who -uH
```

На экран монитора будет выведено сообщение следующего вида:

```
ИМЯ          ЛИНИЯ      ВРЕМЯ      IDLE      PID      КОММЕНТАРИЙ
user-name line-name mm-dd hh:mm .      10340 (:0)
```

где:

- user-name – имя пользователя;
- line-name – имя терминальной линии;
- yy-mm-dd hh:mm – дата (в формате гг – мм – дд, гг – год, мм – месяц, дд – день) и время (в формате чч:мм, чч – час, мм – минута) начала сеанса работы пользователя;
- 10340 – PID-идентификатор процесса;
- (:0) – отсутствующий комментарий.

Точка (.) в параметре IDLE свидетельствует о том, что данный терминал находился в активном состоянии не более минуты тому назад.

17.2.2. Команда ps

Для получения информации о состоянии запущенных процессов используется команда `ps`. Она выдает следующую информацию о процессах: какие из них выполнены, какие вызвали проблемы в системе, как долго выполняется тот или иной процесс, какие он затребовал системные ресурсы, идентификатор процесса (который будет нужен, например, для прекращения работы процесса с помощью команды `kill`).

Команда `ps`, запущенная без опций командной строки, выдает список процессов, которые порождены учетной записью администратора.

Наиболее распространенное применение `ps` – отслеживание работы фоновых и других процессов в системе. Поскольку в большинстве случаев фоновые процессы никак не взаимодействуют ни с экраном, ни с клавиатурой, команда `ps` остается основным средством наблюдения за ними.

Синтаксис команды `ps`:

```
ps [-e] [-d] [-a] [-f] [-l] [-n файл_с_системой] [-t список_терминалов]
[-p список_идентификаторов_процессов]
[-u список_идентификаторов_пользователей]
[-g список_идентификаторов_лидеров_групп]
```

Опции команды `ps` приведены в таблице 101.

Т а б л и ц а 101 – Опции команды `ps`

Опция	Описание
<code>-e</code>	Позволяет вывести информацию обо всех процессах
<code>-d</code>	Позволяет вывести информацию обо всех процессах, кроме лидеров групп
<code>-a</code>	Позволяет вывести информацию обо всех наиболее часто запрашиваемых процессах, то есть обо всех процессах, кроме лидеров групп и процессов, не ассоциированных с терминалом
<code>-f</code>	Позволяет сгенерировать полный листинг
<code>-l</code>	Генерировать листинг в длинном формате
<code>-n файл_с_системой</code>	Считать, что ОС загружена из файла <code>с_системой</code> , а не из файла <code>/unix</code>
<code>-t список_терминалов</code>	Позволяет вывести информацию только о процессах, ассоциированных с терминалами из заданного списка <code>терминалов</code> (терминал – это либо имя файла-устройства, например, <code>tty</code> , номер или <code>console</code> , либо просто номер, если имя файла начинается с <code>tty</code>)
<code>-p</code>	Список_идентификаторов_процессов – позволяет вывести информацию только об указанных процессах
<code>-u</code>	Список_идентификаторов_пользователей – позволяет вывести информацию только о процессах с заданными идентификаторами или входными именами пользователей (идентификатор пользователя выводится в числовом виде, а при наличии опции <code>-f</code> – в символьном)
<code>-g</code>	Список_идентификаторов_лидеров_групп – позволяет вывести информацию только о процессах, для которых указаны идентификаторы лидеров групп (лидер группы – это процесс, номер которого идентичен его идентификатору группы)

`ps` выводит четыре основных поля информации для каждого процесса:

- PID – идентификатор процесса;
- TTY – терминал, с которого был запущен процесс;
- TIME – время работы процесса;
- COMMAND – имя выполненной команды.

При указании опции `-f` команда `ps` пытается определить имя команды и аргументы, с которыми был создан процесс, исследуя пользовательский блок процесса. В случае если это не удастся, имя процесса выводится так же, как и при отсутствии опции `-f`, только заключается в квадратные скобки.

В таблице 102 приводятся заголовки колонок листинга, и поясняется смысл их содержимого. Буквы «l» или «f» в скобках означают, что эта колонка появляется соответственно при длинном или полном формате листинга, отсутствие букв означает, что данная колонка выводится всегда. При этом опции `-l` и `-f` влияют только на формат выдачи, но не на список процессов, информация о которых будет предоставлена.

Т а б л и ц а 102 – Описание заголовков колонок листинга

Заголовок	Значение	Описание
F (l)	Флаги (шестнадцатеричные), логическая сумма которых характеризует процессы следующим образом:	
	00	Процесс терминирован, элемент таблицы процессов свободен.
	01	Системный процесс: всегда в основной памяти.
	02	Процесс трассируется родительским процессом.
	04	Родительский трассировочный сигнал остановил процесс, родительский процесс находится в состоянии ожидания
	08	Процесс не может быть разбужен сигналом
	10	Процесс в основной памяти
	20	Процесс в основной памяти, заблокирован до завершения события
	40	Идет сигнал к удаленной системе
	80	Процесс в очереди на ввод/вывод
S (l)	Статус процесса:	
	O	Процесс обрабатывается процессором
	S	Процесс ожидает завершения события
	R	Процесс стоит в очереди на выполнение
	I	Процесс создается
	Z	Процесс завершен, но родительский процесс не ждет этого
	T	Процесс остановлен сигналом, так как родительский процесс трассирует его
	X	Процесс ожидает получения большего объема основной памяти

Окончание таблицы 102

Заголовок	Значение	Описание
UID (f,l)		Идентификатор владельца процесса, при указании опции -f выдается входное имя пользователя
PID		Идентификатор процесса (нужен для терминирования процесса)
PPID(f,l)		Идентификатор родительского процесса
C (f,l)		Доля выделенного планировщиком времени центрального процессора
STIME (f)		Время запуска процесса (часы:минуты:секунды). Если процесс запущен более чем 24 часа назад, выводится месяц и день запуска
PRI (l)		Приоритет процесса: большее число означает меньший приоритет
NI (l)		Поправка к приоритету
ADDR (l)		Адрес процесса в памяти
SZ (l)		Размер (в блоках по 512 байт) образа процесса в памяти
WCHAN (l)		Адрес события, которого ожидает процесс (у активного процесса эта колонка пуста)
TTY		Управляющий терминал (обычно – терминал, с которого был запущен процесс). В случае если такового нет, выводится символ «?»
TIME		Истраченное процессом время на выполнение центральным процессором
COMMAND		Имя программы: если указана опция -f, выводится полное имя команды и ее аргументы

17.2.3. Команда nohup

Команда nohup применяется для того, чтобы процесс продолжал выполняться даже после выхода из системы, поскольку выполнение стандартного дочернего процесса завершается сразу после прекращения работы родительского, и, если был запущен фоновый процесс, он также прекращает работу при выходе из системы.

При выполнении, команду nohup следует поместить в начало командной строки следующим образом:

```
nohup sort sales.dat &
```

В данном примере nohup заставляет ОС игнорировать выход из нее и продолжать выполнение до тех пор, пока процесс не закончится сам по себе. Будет запущен процесс, который продолжит свое выполнение, не требуя контроля администратора.

17.2.4. Команда `nice`

Команда `nice` позволяет запустить другую команду с предопределенным приоритетом выполнения, предоставляя администратору возможность определять приоритет при выполнении своих задач.

При обычном запуске все задачи имеют один и тот же приоритет, и ОС равномерно распределяет между ними процессорное время. С помощью команды `nice` можно понизить приоритет какой-либо задачи, предоставив другим задачам больше процессорного времени. Повысить приоритет той или иной задачи имеет право только пользователь с идентификатором `root`.

Команда `nice` обладает следующим синтаксисом:

```
nice -number command
```

Уровень приоритета определяется параметром `number`, при этом большее его значение означает меньший приоритет команды. Значение по умолчанию равно «10», и `number` представляет собой число, на которое он должен быть уменьшен.

Например, если запущен процесс сортировки:

```
sort sales.dat > sales.srt &
```

Далее, чтобы дать ему преимущество над следующим процессом, нужно запустить следующий процесс с уменьшенным приоритетом:

```
nice -5 lp mail_list &
```

Для того чтобы назначить процессу самый низкий приоритет из возможных, нужно выполнить следующую команду:

```
nice -10 lp mail_list &
```

Примечание. В случае команды `nice` тире означает знак опции.

Только пользователь с идентификатором `root` может повысить приоритет того или иного процесса, применяя для этого отрицательное значение аргумента. Максимально возможный приоритет – «20», присвоить его процессу пользователь с идентификатором `root` может с помощью команды:

```
nice --10 job &
```

Наличие символа «&» в примере достаточно условно, можно изменять приоритеты, как фоновых процессов, так и процессов переднего плана.

17.2.5. Команда `renice`

Команда `renice` позволяет изменить приоритет работающего процесса.

Формат этой команды подобен формату команды `nice`:

```
renice -n PID
```

Для изменения приоритета работающего процесса нужно знать его идентификатор, получить который можно с помощью команды `ps`, например, вызвав:

```
ps -e | grep name
```

В данной команде нужно заменить `name` именем интересующего процесса. Команда `grep` отфильтрует только те записи, в которых будет встречаться имя нужной команды. В случае, если нужно изменить приоритет всех процессов пользователя или группы пользователей, в команде `renice` используется идентификатор пользователя или группы.

Далее приводится пример использования команды `renice`, предположив, что имя пользователя – `pav`:

```
ps -ef | grep $LOGNAME
pav 11805 11804 0 Dec 22 ttysb 0:01 sort sales.dat > sales srt
pav 19955 19938 4 16:13:02 ttyo 0:00 grep pav
pav 19938 1 0 16:11:04 ttyo 0-00 bash
pav 19940 19938 42 16:13:02 ttyo 0:33 find . -name core -exec nn
{};
```

Теперь, чтобы понизить приоритет процесса `find` с идентификатором `19940`, нужно ввести:

```
renice -5 19940
```

В случае команды `renice` работают те же правила, что и в случае команды `nice`, а именно:

- ее можно использовать только со своими процессами;
- пользователь с идентификатором `root` может применить ее к любому процессу;
- только пользователь с идентификатором `root` может повысить приоритет процесса.

17.2.6. Команда `kill` и `killall`

В отдельных ситуациях нужно прекратить выполнение процесса, не дожидаясь его нормального завершения. Это может произойти в следующих случаях:

- процесс использует слишком много времени процессора и ресурсов компьютера;
- процесс работает слишком долго, не давая ожидаемых результатов;
- процесс производит слишком большой вывод информации на экран или в файл;
- процесс привел к блокировке терминала или другой сессии;
- из-за ошибки пользователя или программы используются не те файлы или параметры командной строки;
- дальнейшее выполнение процесса бесполезно.

В случае если процесс работает не в фоновом режиме, нажатие клавиш `<Ctrl>+<C>` должно прервать его выполнение, но, если процесс фоновый, то прервать его выполнение можно только с помощью команды `kill`, которая посылает процессу сигнал, требующий от процесса завершения. Для этого используются две формы:

```
kill PID(s)
kill -signal PID(s)
```

Для завершения процесса с идентификатором 127 ввести:

```
kill 127
```

Для того чтобы завершить процессы 115, 225 и 325, ввести:

```
kill 115 225 325
```

С помощью опции `-signal` можно, например, заставить процесс перечитать конфигурационные файлы без прекращения работы.

Список доступных сигналов можно получить с помощью команды:

```
kill -l
```

При успешном завершении процесса никакое сообщение не выводится.

Сообщение появится при попытке завершения процесса без наличия соответствующих прав доступа или при попытке завершить несуществующий процесс.

Завершение родительского процесса иногда приводит к завершению дочерних, однако для полной уверенности в завершении всех процессов, связанных с данным, следует указывать их в команде `kill`.

В случае, если терминал оказался заблокированным, можно войти в систему с другого терминала:

```
ps -ef | grep $LOGNAME
```

и завершить работу оболочки на заблокированном терминале.

При выполнении команда `kill` посылает процессу соответствующий сигнал. Программы ОС могут посылать и принимать более 20 сигналов, каждый из которых имеет свой номер. Например, при выходе администратора ОС посылает всем его процессам сигнал 1, который заставляет все процессы (кроме запущенных с помощью `nohup`) прекратить работу.

Программы могут быть написаны и таким образом, что будут игнорировать посылаемые им сигналы, включая сигнал 15, который возникает при запуске команды `kill` без указания конкретного сигнала.

Однако сигнал 9 не может быть проигнорирован – процесс все равно будет завершён. Таким образом, если команда `kill PID` не смогла завершить процесс (он виден при использовании команды `ps`), нужно воспользоваться следующей командой:

```
kill -9 PID
```

Команда `kill -9` прекращает процесс, не давая возможности, например, корректно закрыть файлы, что может привести к потере данных. Использовать эту возможность следует только в случае крайней необходимости.

Для завершения всех фоновых процессов нужно ввести следующую команду:

```
kill 0
```

Команда `killall` завершает все процессы с данным именем, обладает следующим синтаксисом:

```
killall [имя процесса]
```

Пример использования `killall`:

```
killall httpd
```

Преимущественное право контроля над процессом принадлежит владельцу. Права владельца могут отменяться только пользователем с идентификатором `root`.

Ядро назначает каждому процессу четыре идентификатора: реальный и эффективный `UID`, реальный и эффективный `GID`. Реальные `ID` используются для учета использования системных ресурсов, а эффективные – для определения прав доступа. Как правило, реальные и эффективные `ID` совпадают. Владелец процесса может посылать в процесс сигналы, а также понижать приоритет процесса.

Процесс, приступающий к выполнению другого программного файла, осуществляет один из системных вызовов семейства `exec`. Когда такое случается, эффективные `UID` и `GID` процесса могут быть установлены равными `UID` и `GID` файла, содержащего образ новой программы, если у этого файла установлены биты смены идентификатора пользователя и идентификатора группы.

Системный вызов `exec` – это механизм, с помощью которого такие команды, как `passwd`, временно получают права пользователя с идентификатором `root` (команде `passwd` они нужны для того, чтобы изменить `/etc/passwd`).

17.3. Основные утилиты для операций с файлами и каталогами

17.3.1. Команда `ls`

Команда `ls` предназначена для вывода информации о файлах или каталогах. Команда `ls` для каждого имени каталога распечатывает список входящих в этот каталог файлов; для файлов – повторяется имя файла и выводится дополнительная информация в соответствии с указанными флагами.

По умолчанию имена файлов выводятся в алфавитном порядке. Если имена не заданы, выдается содержимое текущего каталога.

Синтаксис:

```
ls [параметры]... [файл]...
```

Параметры:

- 1) `-a, --all` – вывести список всех файлов (обычно не выводятся файлы, имена которых начинаются с точки);
- 2) `-A, --almost-all` – не показывать подразумеваемые «.» и «..»;
- 3) `--block-size=РАЗМЕР` – выдает размеры в блоках по РАЗМЕР байт. Например, `--block-size=M` для вывода объема в единицах равных 1048576 байтов;
- 4) `-B, --ignore-backups` – не показывать файлы, заканчивающиеся на «~», если они не заданы в командной строке;
- 5) `-c, --time=ctime, --time=status` – сортировать содержимое каталога в соответствии со временем изменения состояния файла. Если с помощью опции `-l` задан этот формат, то выдавать время изменения файла вместо времени его модификации. С опцией `-t` показать время последней модификации описания файла и сортировать по имени;
- 6) `-C, --format=vertical` – вывод в несколько колонок с сортировкой по вертикали;
- 7) `--color[=КОГДА]` – использовать цвета в выводе. КОГДА по умолчанию `always`. Также можно использовать `never` и `auto`;
- 8) `-d, --directory` – если аргумент является каталогом, то выводить только его имя, а не содержимое. Часто используется с флагом `-l` для получения сведений о состоянии каталога;
- 9) `-h, --human-readable` – в сочетании с `-l` показывает размеры в удобочитаемом формате (например, 1K 234M 2G);
- 10) `-i, --inode` – показывать индекс каждого файла;
- 11) `-I, --ignore= ШАБЛОН` – не показывать записи, соответствующие ШАБЛОНУ командного интерпретатора;
- 12) `-k, --kibibytes` – использовать блоки по 1024 байта;
- 13) `-l` – вывод в длинном формате;

- 14) `-m` – показать записи в список шириной в размер терминала, имена файлов разделяются запятыми;
- 15) `-r, --reverse` – изменить порядок сортировки на обратный;
- 16) `-R, --recursive` – рекурсивно обойти встретившиеся подкаталоги;
- 17) `-s, --size` – выдавать размер файлов в блоках;
- 18) `-S` – отсортировать по размеру файлов, большие сначала;
- 19) `--sort=СЛОВО` – сортировать по СЛОВУ, а не по имени: `none` (без сортировки) `-U, extension` (расширение) `-X, size` (размер) `-S, time` (время) `-t` или `version` (версия) `-v`;
- 20) `-t` – файлы сортируются по времени последнего изменения (сначала идут самые новые файлы);
- 21) `-U` – не сортировать, отображать записи в обычном порядке;
- 22) `-v` – сортировать по номерам (версии) в текстовом представлении;
- 23) `-x` – вывод в несколько колонок с сортировкой по строкам;
- 24) `-Z, --context` – вывести контекст для каждого файла;
- 25) `-l` – отображать по одному файлу в строке.

Режим доступа к файлу при указании флага `-l` выводится в виде 10 символов.

При этом первый символ означает:

- 1) `d` – файл является каталогом;
- 2) `b` – файл является специальным блочным файлом;
- 3) `c` – файл является специальным символьным файлом;
- 4) `p` – файл является именованным каналом;
- 5) `-` – обычный файл.

Остальные 9 символов делятся на три группы по три символа: права доступа владельца, других пользователей из его группы, всех прочих пользователей. Внутри каждой группы используются три символа, обозначающие права на чтение, запись и выполнение файла соответственно.

Для каталога под правом на выполнение подразумевается право на просмотр в поисках требуемого файла.

Пример:

```
ls -l /util/by
-rwxr-xr-x 1 root sys 50 Jun 22 10:42 /util/by
```

Права обозначаются следующим образом:

- 1) *r* – право на чтение;
- 2) *w* – право на запись;
- 3) *x* – право на выполнение (поиск в каталоге);
- 4) – – данное право доступа отсутствует;
- 5) *l* – учет блокировки доступа (бит переустановки идентификатора группы равен 1, бит права на выполнение членами группы равен 0). Располагается на месте права на выполнение для членов группы;
- 6) *s* – право переустанавливать идентификатор группы или идентификатор владельца и право выполнения файла для членов группы или владельца;
- 7) *s* – неопределенная комбинация бит: право переустанавливать идентификатор владельца есть, а право выполнения файла для владельца отсутствует;
- 8) *t* – установлен бит навязчивости у файла, который могут выполнять прочие пользователи. Располагается на месте права на выполнение для прочих пользователей;
- 9) *t* – бит навязчивости установлен, а права на выполнение у прочих пользователей нет. Располагается на месте права на выполнение для прочих пользователей.

Примеры:

- 1) если файл доступен владельцу для чтения, записи и выполнения, а членам группы и прочим пользователям только для чтения, он имеет режим:

```
-rwxr--r-
```

- 2) файл доступен владельцу для чтения, записи и выполнения, а членам группы и прочим пользователям только для чтения и выполнения. Разрешена переустановка при выполнении идентификатора пользователя на идентификатор владельца файла:

```
-rwsr-xr-x
```

- 3) файл доступен для чтения и записи только владельцу и членам группы; может быть заблокирован при доступе:

```
-rw-rw1--
```

- 4) вывести имена всех файлов в текущем каталоге, включая и те, которые начинаются с точки и обычно не выдаются:

```
ls -a
```

- 5) вывести разнообразную информацию: список всех файлов, включая те, которые обычно не выводятся (a); номера описателей файлов будут выведены в левой колонке (i); размеры файлов (в блоках) выводятся во второй колонке (s); наконец, будут выданы числовые идентификаторы владельцев и групп (n):

```
ls -aisn
```

Возможные сообщения об ошибках, при использовании команды `ls`:

```
ls: невозможно открыть каталог <путь>: Отказано в доступе
```

```
ls: невозможно получить доступ к <путь>/<файл>: Нет такого файла
```

или каталога

17.3.2. Команда `cp`

Команда `cp` предназначена для копирования файлов и каталогов.

Синтаксис:

```
cp [ОПЦИЯ]... [-T] ИСТОЧНИК НАЗНАЧЕНИЕ
```

```
cp [ОПЦИЯ]... ИСТОЧНИК... КАТАЛОГ
```

```
cp [ОПЦИЯ]... -t КАТАЛОГ ИСТОЧНИК...
```

Копирует ИСТОЧНИК в НАЗНАЧЕНИЕ или несколько ИСТОЧНИКОВ в КАТАЛОГ.

Основные опции:

- 1) `--backup [=CONTROL]` – сделать резервную копию каждого целевого файла;
- 2) `-b` – тоже что и `--backup`, но не принимает аргументы;
- 3) `-f`, `--force` – если невозможно открыть существующий файл, то удалить его и попробовать еще раз (данная опция игнорируется, если используется совместно с `-n`);
- 4) `-i`, `--interactive` – спросить перед перезаписью (отменяет ранее указанный ключ `-n`);

- 5) `-H` – следовать символическим ссылкам в источнике;
- 6) `-l`, `--link` – создавать жесткие ссылки вместо копирования;
- 7) `-n`, `--no-clobber` – не перезаписывать существующие файлы (отменяет стоящую перед ней опцию `-i`);
- 8) `-R`, `-r`, `--recursive` – копировать каталоги рекурсивно;
- 9) `-s`, `--symbolic-link` – создать символическую ссылку вместо копирования;
- 10) `-u`, `--update` – копировать, только если файл источник новее, чем файл назначения или если файл назначения отсутствует;
- 11) `-v`, `--verbose` – выводить имя каждого файла перед копированием.

По умолчанию суффикс для резервных копий «~». Его можно переопределить при помощи опции `--suffix` или переменной окружения `SIMPLE_BACKUP_SUFFIX`. Способ контроля версий может быть задан через опцию `--backup` или через переменную окружения `VERSION_CONTROL`. Допустимые значения:

- 1) `none`, `off` – никогда не делать резервные копии (даже если задана опция `--backup`);
- 2) `numbered`, `t` – создать нумерованные резервные копии;
- 3) `existing`, `nil` – если существуют нумерованные резервные копии, то создавать нумерованные резервные копии, если нет, то создавать простые;
- 4) `simple`, `never` – всегда создавать простые резервные копии.

Следующий пример использования команды `cp` демонстрирует копирование файла `srcfile1` в каталог `dest_dir`: `cp srcfile1 dest_dir`

17.3.3. Команда `rsync`

Команда `rsync` выполняет синхронизацию файлов и каталогов, использует протокол удаленного обновления для ускорения передачи файлов, которые существуют в месте назначения.

Синтаксис:

```
rsync [ОПЦИИ] источник место_назначения
```

Опции:

- 1) `-v` – подробный режим;
- 2) `-r` – копировать данные рекурсивно;
- 3) `-a` – режим архивирования, позволяет копировать данные рекурсивно, с сохранением прав доступа на файлы, символических ссылок и другой информации);
- 4) `-h` – вывод данных в удобном формате;
- 5) `-z` – сжатие данных.

Примеры:

- 1) скопировать или синхронизировать все файлы из одного каталога в другой:

```
rsync -avh /tmp/firstdir /tmp/seconddir
```

- 2) копирование локальных данных на удаленный хост:

```
rsync -avzh /tmp/firstdir user@10.110.2.1:/tmp/seconddir
```

Возможные сообщения об ошибках, при использовании команды `sfill`:

```
rsync: change_dir#1 <каталог> failed: Отказано в доступе
```

```
rsync: change_dir <каталог> failed: Нет такого файла или каталога
```

17.3.4. Команда `mv`

Команда `mv` – перемещение (переименование) файлов.

Синтаксис:

```
mv [ОПЦИЯ]... [-T] ИСТОЧНИК НАЗНАЧЕНИЕ
```

```
mv [ОПЦИЯ]... ИСТОЧНИК... КАТАЛОГ
```

```
mv [ОПЦИЯ]... -t КАТАЛОГ ИСТОЧНИК...
```

Переименовать ИСТОЧНИК в НАЗНАЧЕНИЕ или переместить ИСТОЧНИК (и) в КАТАЛОГ.

Основные опции:

- 1) `-i`, `--interactive` – просит подтверждения на замену существующего файла;
- 2) `-n`, `--no-clobber` – не переписывать существующий файл. Если указано несколько опций `-i`, `-f` и `-n`, то действовать будет только последняя;

3) `-u, --update` – перемещать только, если файл ИСТОЧНИК новее, чем файл назначения или если файл назначения отсутствует;

4) `-v, --verbose` – выдавать имя каждого файла перед его переносом.

Возможные сообщения об ошибках, при использовании команды `mv`:

`mv: невозможно переместить <файл> в <файл>: Операция не позволена`

`mv: не удалось выполнить stat для <файл>: Отказано в доступе`

`mv: не удалось выполнить stat для <файл>: Нет такого файла или каталога`

17.3.5. Команда `dd`

Команда `dd` предназначена для копирования файла (по умолчанию из стандартного ввода на стандартный вывод), используя заданные размеры блоков для ввода и вывода, и в тоже время, выполняя его преобразование.

Синтаксис:

`dd [параметр]`

Основные опции:

1) `if=ФАЙЛ` – читает данные из ФАЙЛа вместо стандартного ввода;

2) `of=ФАЙЛ` – пишет данные в ФАЙЛ вместо стандартного вывода;

3) `ibs=ЧИСЛО` – читает по ЧИСЛО байт за раз. По умолчанию 512;

4) `obs=ЧИСЛО` – пишет по ЧИСЛО байт за раз. По умолчанию 512;

5) `bs=ЧИСЛО` – читает и пишет по ЧИСЛО байт за раз. По умолчанию 512.

Примеры:

1) Заполнить устройство случайными данными:

```
dd if=/dev/urandom of=/dev/sda bs=4k
```

2) Скопировать раздел в другой раздел:

```
dd if=/dev/sda3 of=/dev/sdb3 bs=4096 conv=notrunc,noerror
```

Возможные сообщения об ошибках, при использовании команды `dd`:

`dd: не удалось открыть <файл>: Отказано в доступе`

17.3.6. Команда `s_rm`

Команда `s_rm` выполняет безопасное удаление целевого файла.

Синтаксис:

`s_rm ФАЙЛ...`

Возможные сообщения об ошибках, при использовании команды `s_rm`:

Ошибка: файл <файл>: Отказано в доступе

Ошибка: файл <файл>: Нет такого файла или каталога

Примечание. Для работы команды `s_rm` и `s_fill` должен быть установлен пакет `altsp-test-scripts`.

17.3.7. Команда `s_fill`

Команда `s_fill` выполняет безопасную перезапись свободного пространства на разделе, в котором находится указанная директория и всех свободных индексных дескриптеров указанного каталога.

Синтаксис:

```
s_fill каталог...
```

Возможные сообщения об ошибках, при использовании команды `s_fill`:

Ошибка: не достаточно прав для <каталог>: Отказано в доступе

17.3.8. Команда `cd`

Команда `cd` предназначена для смены каталога. Команда работает как с абсолютными, так и с относительными путями. Если каталог не указан, используется значение переменной окружения `HOME` (домашний каталог пользователя). Если каталог задан полным маршрутным именем, он становится текущим. По отношению к новому каталогу нужно иметь право на выполнение, которое в данном случае трактуется как разрешение на поиск.

Синтаксис:

```
cd [-L|-P] [каталог]
```

Опция `-L` заставляет следовать по символическим ссылкам.

Поскольку для выполнения каждой команды создается отдельный процесс, `cd` не может быть обычной командой; она распознается и выполняется командной оболочкой.

Если в качестве аргумента задано `-`, то это эквивалентно `$OLDPWD`.

Если переход был осуществлен по переменной окружения `CDPATH` или в качестве аргумента был задан `-` и смена каталога была успешной, то абсолютный путь нового рабочего каталога будет выведен на стандартный вывод.

17.3.9. Команда `pwd`

Команда `pwd` выводит абсолютный путь текущего (рабочего) каталога.

Синтаксис: `pwd [-LP]`

Опции:

- 1) `-P` – вывод не будет содержать символических ссылок;
- 2) `-L` – вывод может содержать символические ссылки.

17.3.10. Команда `mkdir`

Команда `mkdir` предназначена для создания каталогов.

Синтаксис:

`mkdir [опция]... каталог...`

Опции:

- 1) `-m`, `--mode=РЕЖИМ` – установить права доступа для создаваемых каталогов;
- 2) `-p`, `--parents` – перед созданием нового каталога предварительно создаются все несуществующие вышележащие каталоги. В случае существования каталога не будет выведена ошибка;
- 3) `-v`, `--verbose` – выводить сообщение для каждого созданного каталога;
- 4) `-Z`, `--context [=CTX]` – задать контекст для каждого создаваемого каталога.

Если `CTX` не задан, то контекст будет равным типу по умолчанию.

Чтобы создать поддерево каталогов `tmpdir/temp/dir`, надо выполнить команду:

```
mkdir -p tmpdir/temp/dir
```

Возможные сообщения об ошибках, при использовании команды `mkdir`:

```
mkdir: невозможно создать каталог <каталог>: Отказано в доступе
```

```
mkdir: невозможно создать каталог <каталог>: Нет такого файла или каталога
```

17.3.11. Команда `rmdir`

Команда `rmdir` предназначена для удаления каталога, при условии, что он пуст.

Синтаксис:

`rmdir [опция]... каталог...`

Для команды `rmdir` доступна опция `-p` – при указании пути к каталогу (а не просто имени каталога), команда удалит каталог и его потомков:

```
rmdir -p a/b/c
```

Команда `rmdir` часто заменяется командой `rm -rf`, которая позволяет удалять каталоги, даже если они не пусты.

17.3.12. Команда `mount`

Команда `mount` используется для монтирования файловых систем.

Синтаксис:

```
mount [-lhV]
mount -a [опция]
mount [опция] [--source] <source> | [--target] <directory>
mount [опция] <source> <directory>
```

Опции:

- 1) `-t` – определение типа файловой системы раздела, предполагаемого для размещения;
- 2) `-o` – указание параметров монтирования.

Примеры:

- 1) просмотр примонтированных устройств:

```
mount -l
```

- 2) монтирование разделов жесткого диска:

```
mount -t ext3 /dev/sdb1 /home/user/test
```

Возможные сообщения об ошибках, при использовании команды `mount`:

```
mount: точка монтирования <каталог> не существует
```

17.4. Создание, просмотр и редактирование файлов

17.4.1. Команда `cat`

Команда `cat` позволяет просмотреть файл целиком, копируя файлы в стандартный поток вывода и объединяя их.

Синтаксис:

```
cat [ОПЦИЯ]... [ФАЙЛ]...
```

Опции:

- 1) `-A`, `--show-all` – тоже что и `-vET`;

- 2) `-e` – тоже что и `-vE`;
- 3) `-E`, `--show-ends` – отображать символ «\$» в конце каждой строки;
- 4) `-n`, `--number` – нумеровать выводимые строки;
- 5) `-s`, `--squeeze-blank` – скрывать повторяющиеся пустые строки в выводе;
- 6) `-t` – тоже что и `-vT`;
- 7) `-T`, `--show-tabs` – отображать символ табуляции как `^I`;
- 8) `-v`, `--show-nonprinting` – использовать `^-` и M-нотацию для всех непечатаемых символов кроме LFD (перевод строки и табуляция) и табуляции.

Если файл не задан или задан как «-», то читать из стандартного ввода.

Примеры:

- 1) вывести содержимое файла `f`, затем со стандартного ввода, затем – содержимое файла `g`:

```
cat f - g
```

- 2) скопировать стандартный ввод на стандартный вывод:

```
cat
```

Возможные сообщения об ошибках, при использовании команды `cat`:

```
cat: <файл>: Отказано в доступе
```

```
cat: <файл>: Нет такого файла или каталога
```

17.4.2. Команда `less`

Команда `less` позволяет просматривать текст постранично.

```
less [ опции ] файл
```

Опции:

- 1) `-c` – очистка экран перед тем, как отобразить следующую страницу;
- 2) `-m` – вывод информации о том, какая часть файла выведена на данный момент (в процентах);
- 3) `-N` – вывод номеров строк;
- 4) `-r` – вывод управляющих (непечатаемых) символов;
- 5) `-s` – объединение несколько пустых строк в одну;
- 6) `-S` – урезание длинных строк до длины экрана вместо переноса.

Возможные сообщения об ошибках, при использовании команды `less`:

<файл>: Отказано в доступе

<файл>: Нет такого файла или каталога

17.4.3. Команда `echo`

Команда `echo` выводит текст на стандартное устройство вывода.

`echo [опции] [строка]`

Опции:

- 1) `-n` – не выводить в конце символ новой строки;
- 2) `-e` – включить интерпретацию управляющих символов;
- 3) `-E` – отключить интерпретацию управляющих символов;

Возможные сообщения об ошибках, при использовании команды `echo`:

<файл>: Отказано в доступе

<файл>: Нет такого файла или каталога

17.4.4. Команда `grep`

Команда `grep` предназначена для поиска текста, соответствующего регулярному выражению в файлах или потоке вывода.

Синтаксис:

`grep [опции] шаблон_поиска [файл]`

Опции:

- 1) `-r` – рекурсивный поиск во всех каталогах;
- 2) `-n` – вывод номеров строк, в которых найдено совпадение;
- 3) `-l` – вывод списка файлов, содержащих шаблон;
- 4) `-v` – поиск строк, не содержащих шаблон (инверсия);
- 5) `-i` – поиск с игнорированием регистра.

17.4.5. Команда `touch`

Создание и редактирование файлов выполняется командой `touch`, которая устанавливает время последнего изменения и доступа в текущее системное время у заданного файла. Если файл не существует – он создается.

Синтаксис:

`touch [опции]... файл`

Основные опции:

- 1) `-a` – изменить только время доступа к файлу;
- 2) `-c, --no-create` – не создавать файл;
- 3) `-d, --date=СТРОКА` – проанализировать строку и использовать вместо текущего времени;
- 4) `-m` – изменить время последней модификации файла;
- 5) `-r, --reference=ФАЙЛ` – использовать соответствующий временной штамп от ФАЙЛ в качестве нового значения для изменяемого временного штампа;
- 6) `-t время` – использовать заданное время в качестве нового значения для изменяемого временного штампа.

Следующий пример использования команды `touch` создает файл `myfile.txt`:

```
touch myfile.txt
```

Возможные сообщения об ошибках, при использовании команды `touch`:

```
touch: невозможно выполнить touch для <файл>: Отказано в доступе
```

```
touch: невозможно выполнить touch для <путь>/<файл>: Нет такого  
файла или каталога
```

17.4.6. Команда `mknod`

Утилита `mknod` создает специальные блочные или символьные файлы. Специальный файл записывается в файловой системе с помощью тройки параметров: один логический и два целых. Логический параметр говорит о том, является ли специальный файл символьным или блочным. Два целых параметра задают старший и младший номера устройства. Специальный файл практически не занимает места на диске и используется только для общения с операционной системой, а не для хранения данных.

Синтаксис:

```
mknod [опции] имя {bc} старший_номер младший_номер
```

```
mknod [опции] имя p
```

Основные опции:

- 1) `-m, --mode=РЕЖИМ` – установить РЕЖИМ доступа;
- 2) `-z` – установить контекст безопасности равным типу по умолчанию.

Тип устройства может принимать следующие значения:

- 1) `b` – создать файл блочного устройства (буферизированный);
- 2) `c` – создать файл символьного устройства (небуферизированный);
- 3) `p` – создать именованный канал.

Возможные сообщения об ошибках, при использовании команды `mknod`:

`mknod: <файл>: Файл существует`

17.5. Поиск файлов

17.5.1. Команда `find`

Утилита `find` используется для поиска файлов.

Синтаксис:

```
find [-H] [-L] [-P] [-0уровень] [-D help | tree | search | stat |
rates | opt | exec] [путь...] [выражение]
find [путь] [опции] [критерии поиска] [действия над файлами]
```

В качестве пути для поиска можно использовать как абсолютные, так и относительные пути, а также список путей, разделенных пробелом. Путем по умолчанию является текущий подкаталог. Выражение по умолчанию `-print`.

Основные опции:

- 1) `-d`, `-depth` – поиск в подкаталогах перед поиском в самом каталоге;
- 2) `-L` – при поиске следовать по символическим ссылкам;
- 3) `-P` – никогда не следовать по символическим ссылкам;
- 4) `-maxdepth N` – при поиске проверять не более чем `N` вложенных уровней каталогов;
- 5) `-mindepth N` – не проверять вложенные каталоги уровня `N` и меньше;
- 6) `-mount` – не искать в каталогах других файловых систем.

У команды `find` может быть несколько критериев поиска (`tests`). Каждый критерий представляет собой определенное условие проверки, которое возвращает либо `true` либо `false`.

В процессе обработки очередного файла команда `find` по очереди проверяет каждый критерий, и, если очередной критерий возвращает `false`, тогда команда `find` переходит к следующему файлу.

Основные критерии поиска:

- 1) `-name шаблон` – имя файла (шаблон имени) без указания пути.
Рекомендуется всегда заключать шаблон в кавычки;
- 2) `-atime N` – последний доступ к файлу производился N дней назад.
`-atime +1` найдет файлы, доступ к которым осуществлялся как минимум два дня назад;
- 3) `-mtime N` – последнее изменение файла было N дней назад;
- 4) `-ctime N` – статус файла последний раз изменялся N дней назад;
- 5) `-newer другой_файл` – файл был модифицирован позднее, чем `другой_файл`;
- 6) `-size [±]N[cwbkMG]` – размер файла равен N блокам, если указано +N, тогда размер файла больше N, -N – меньше. Символ после N означает размер блока (b – 512 байт, c – байт, w – 2 байта, k – Кбайт, M – Мбайт, G – Гбайт);
- 7) `-type C` – файл имеет тип c, где c есть b (блочный специальный файл), c (символьный специальный файл), d (каталог), p (именованный канал), f (обычный файл), l (символьная ссылка) или s (сокет);
- 8) `[-perm] [-]восьмеричное_число` – режим доступа к текущему файлу в точности равен восьмеричному_числу. Если перед восьмеричным_числом указан знак -, то для сравнения из режима файла берутся только биты, соответствующие битам восьмеричного_числа, равным единице;
- 9) `-links n` – на файл имеется n ссылок;
- 10) `-user имя_пользователя` – файл принадлежит пользователю с данным именем. Разрешены цифровые идентификаторы пользователя;
- 11) `-group имя_группы` – файл принадлежит группе с данным именем. Разрешены цифровые идентификаторы группы.

Критерии можно объединять, используя операторы. Ниже приведены операторы в порядке убывания их приоритета:

- унарная операция отрицания, обозначается ! (! критерий);
- логическое И, обозначается пробелом (критерий1 критерий2);
- логическое ИЛИ, обозначается -o (критерий1-o критерий2).

Когда выполняется команда `find`, можно выполнять различные действия над найденными файлами.

Основные действия:

- 1) `-exec` команда `\;` – выполнить команду. Запись команды должна заканчиваться экранированной точкой с запятой. Строка «`{}`» заменяется текущим маршрутным именем файла;
- 2) `execdir` команда `\;` – то же самое что и `exec`, но команда вызывается из подкаталога, содержащего текущий файл;
- 3) `-ok` команда – эквивалентно `-exec` за исключением того, что перед выполнением команды запрашивается подтверждение (в виде сгенерированной командной строки со знаком вопроса в конце) и она выполняется только при ответе: `y`;
- 4) `-print` – вывод имени файла на экран.

Примеры:

- 1) найти в текущем каталоге обычные файлы (не каталоги), имя которых начинается с символа «`~`»:

```
find . -type f -name "~*" -print
```

- 2) найти в текущем каталоге файлы, измененные позже, чем файл `file.bak`:

```
find . -newer file.bak -type f -print
```

- 3) удалить все файлы с именами `a.out` или `*.o`, доступ к которым не производился в течение недели:

```
find / \( -name a.out -o -name '*.o' \) -atime +7 -exec rm {} \;
```

- 4) удалить из текущего каталога и его подкаталогов все файлы нулевого размера, запрашивая подтверждение:

```
find . -size 0c -ok rm {} \;
```

17.5.2. Команда `whereis`

Команда `whereis` сообщает путь к исполняемому файлу программы, ее исходным файлам (если есть) и соответствующим страницам справочного руководства.

Опции:

- 1) `-b` – вывод информации только об исполняемых файлах;
- 2) `-m` – вывод информации только о страницах справочного руководства;
- 3) `-s` – вывод информации только об исходных файлах.

17.6. Средства архивирования файлов

Команды `tar`, `cpio`, `gzip` представляют собой инструменты создания резервных копий и архивирования ФС.

При создании архива командами `tar` (п. 17.6.1) и `gzip` передается список файлов и каталогов, указываемых как параметры командной строки. Любой указанный каталог просматривается рекурсивно.

При создании архива с помощью команды `cpio` (п. 17.6.2) ей предоставляется список объектов (имена файлов и каталогов, символические имена любых устройств, гнезда доменов UNIX, именованные каналы).

17.6.1. Команда `tar`

Команда `tar` предназначена для преобразования файла или группы файлов в архив без сжатия (`tarfile`).

Синтаксис:

```
tar [Опции] [АРГ]
```

Опции:

- 1) `-c` – создает архив;
- 2) `-x` – восстанавливает файлы из архива на устройстве, заданном по умолчанию или определенном опцией `f`;
- 3) `-f name` – создает (или читает) архив с `name`, где `name` – имя файла или устройства, определенного в `/dev`, например, `/dev/rmt0`;
- 4) `-z` – сжимает или распаковывает архив с помощью `compress`;
- 5) `-Z` – сжимает или распаковывает архив с помощью `gzip`;
- 6) `-M` – создает многотомный архив;
- 7) `-t` – создает список сохраненных в архиве файлов и выводит его на консоль;

8) `-v` – выводит подробную информацию о процессе.

Упаковка файлов в архив чаще всего выполняется следующей командой:

```
tar -cf [имя создаваемого файла архива] [упаковываемые файлы  
и (или) директории]
```

Пример использования команды упаковки архива:

```
$ tar -cf moi_dokumenti.tar Docs project.tex
```

Распаковка содержимого архива в текущий каталог выполняется следующей командой:

```
tar -xf [имя файла архива]
```

Далее приводится пример использования команды распаковки архива:

```
$ tar -xf moi_dokumenti.tar
```

Для сжатия файлов используются специальные программы сжатия: `gzip`, `bzip2` и `7z`.

17.6.2. Команда `cpio`

Команда `cpio` предназначена для копирования файлов. Ее можно использовать с опцией `-o` для создания резервных архивов и с опцией `-i` – для восстановления файлов. Команда получает информацию от стандартного устройства ввода и посылает выводимую информацию на стандартное устройство вывода.

Команда `cpio` может архивировать любой набор файлов и специальные файлы, хранит информацию более эффективно, чем `tar`, пропускает сбойные сектора или блоки при восстановлении данных, и ее архивы могут быть восстановлены в ОС.

Недостатком команды `cpio` является то, что для обновления архива следует использовать язык программирования оболочки, чтобы создать соответствующий сценарий.

Синтаксис:

```
cpio [Опции] < список-имен [> архив]
```

Опции:

- 1) `-o` – создание архива в стандартное устройство вывода;
- 2) `-i` – восстановление файлов из архива, передаваемого на стандартное устройство ввода;

3) -t – создание списка содержимого стандартного устройства ввода.

Ниже приводятся примеры использования команды `cpio` для решения различных задач.

Копирование файлов из каталога `/home` в архив `home.cpio` выполняется следующим образом:

```
find /home/* | cpio -o > /tmp/home.cpio
```

Восстановление файлов из архива `home.cpio` с сохранением дерева каталогов и создание списка в файле `bkup.index` выполняется следующим образом:

```
cpio -id < /tmp/home.cpio > bkup.index
```

Использование команды `find` для поиска измененных за последние сутки файлов и сохранение их в архив `home.new.cpio` выполняется следующим образом:

```
find /home -mtime 1 -type f | cpio -o > /tmp/home.new.cpio
```

Восстановление файла `/home/dave/notes.txt` из архива `home.cpio` выполняется следующим образом:

```
cpio -id /home/dave/notes.txt < home.cpio
```

Для восстановления файла с помощью `cpio` следует указывать его полное имя.

Все эти команды могут выполняться автоматически путем их размещения в файле `crontab` пользователя с идентификатором `root`.

Пример записи, выполняющей резервное копирование каталога `/home` ежедневно в 01:30:

```
30 02 *** ls /home : cpio -o > /tmp/home.cpio
```

При необходимости выполнения резервного копирования более сложного уровня можно создать соответствующий сценарий оболочки. Запуск подобных сценариев также может быть осуществлен посредством `cron`.

Создание резервных копий означает определение политики создания резервных копий для снижения потерь и восстановления информации после возможной аварии системы.

17.7. Средства редактирования файлов

17.7.1. Текстовый редактор Vi

Текстовый редактор Vi – системный редактор, назначаемый ОС по умолчанию для работы с текстовыми файлами.

Текстовый редактор Vi имеет модальный интерфейс – одни и те же клавиши в разных режимах работы выполняют разные действия.

В редакторе Vi есть несколько режимов работы:

- 1) командный режим – перемещение по файлу, удаление текста и другие редактирующие функции. По умолчанию, работа начинается в командном режиме. Перейти в него из любого другого режима <ESC>, иногда два раза;
- 2) режим ввода – ввод текста (удаление и ввод текста происходит в двух разных режимах). Переход в режим ввода из командного режима осуществляется командой <i>;
- 3) режим строчного редактора ED – это специальный режим, в котором редактору даются сложные команды. При вводе этих команд они отображаются в последней строке экрана. Например, команда <wq> позволяет записать файл и покинуть редактор Vi, а команда <q!> – выйти из редактора Vi без сохранения изменений. В этом режиме обычно вводятся команды, название которых состоит из нескольких символов. Переход в него из командного режима осуществляется командой <:>.

Далее описаны операции, которые можно произвести с файлом в командном режиме.

17.7.1.1. Открыть (создать) файл

Управляющая команда открытия файла выглядит следующим образом:

```
vi <имя_файла>
```

Создание файла происходит при помощи той же команды, поскольку создание файла происходит в момент сохранения.

Для открытия или создания нового файла в командном режиме нужно набрать:

```
:e filename
```

Перед этим нужно сохранить предыдущий файл с помощью следующих команд:

- <:w> – сохраняет файл с существующим именем;
- <:sav filename> – или «Сохранить как».

17.7.1.2. Навигация по файлу

Навигация по файлу происходит с помощью управляющих клавиш на клавиатуре. Также допускается использовать клавиши быстрого перемещения:

- <^> или <0> – в начало текущей строки;
- <\$> – в конец текущей строки;
- <w> – на слово вправо;
- – на слово влево.

17.7.1.3. Редактирование файла

Для редактирования текста нужно перейти в режим ввода (нажать <i>).

Основные команды редактирования:

- <R>, <i> – переход в режим ввода, замена текста под курсором;
- <I> – переход в режим ввода с начала текущей строки;
- <o> – переход в режим ввода с новой строки под курсором;
- <O> – переход в режим ввода с новой строки над курсором;
- <a> – переход в режим ввода после курсора;
- <x> – стирание символа под курсором;
- <X> – стирание символа перед курсором;
- <dd> – стирание текущей строки;
- <d<число>d> – стирание выбранного числа строк, начиная с текущей;
- <y> – копирование текущей строки в неименованный буфер;
- <y<число>y> – копирование выбранного числа строк, начиная с текущей в неименованный буфер;
- <p> – вставка строки из неименованного буфера под курсор;
- <P> – вставка строки из неименованного буфера над курсором;
- <J> – слияние текущей строки со следующей;

- <u> – отмена последней команды;
- <.> – повтор последней команды.

Для перехода в режим строчного редактора ED нужно нажать <Shift>+<:>.

17.7.1.4. Запись в файл и выход из редактора

Запись в файл выполняется следующей командой:

```
<Esc>:w<Enter>
```

В случае, если файл заблокирован другим пользователем либо отсутствуют права на запись, нужно использовать следующую команду:

```
<Esc>:w!<Enter>
```

При попытке записи без «!» будет выдано соответствующее предупреждение.

Создать новый файл <имя_файла> и записать в него текущее содержимое:

```
<Esc>:w имя_файла <Enter>
```

В случае, если файл с таким именем уже существует, редактор выдаст предупреждение. После успешного создания файла и осуществления записи информации в него работа продолжится со старым файлом.

Для выхода из редактора нужно использовать следующую команду:

```
<Esc>:q<Enter>
```

В случае, если в файл были внесены изменения, нужно добавлять после команды «!».

Выйти из редактора не сохраняя изменения:

```
<Esc>:q!<Enter>
```

Сохранить изменения в файле и выйти:

```
<Esc>:wq<Enter> или <Esc>ZZ<Enter>.
```

17.7.1.5. Дополнительные возможности

Текстовый редактор Vi обладает рядом дополнительных возможностей, которые вызываются следующими командами:

- ^G – показать информацию о файле;
- G – перейти в конец файла;
- <number>G – перейти на конкретную строку <number>;
- :<number> – перейти на <number> строк вперед;

- `:set number` – отобразить слева нумерацию строк (`:set nonumber` – спрятать нумерацию);
- `:set wrap` – переносить длинные строки (`:set nowrap` – не переносить);
- `:colorscheme <name>` – задать цветовую тему (где `<name>` имя темы, ТАВ работает как автодополнение);
- `/мама` – поиск текста «мама» в файле;
- `n` – повторить поиск;
- `:h` или `:help` – список возможной помощи (`:viusage`, `:exusage`).

Привести концы строк в файле к виду dos или unix соответственно:

```
:set fileformat=dos
:set fileformat=unix
```

Задать размер табуляции в четыре пробела:

```
:set ts=4
```

17.7.2. Редактор Vim

Vim – свободный режимный текстовый редактор, созданный на основе Vi.

17.7.2.1. Основной режим работы

Основной режим работы Vim предназначен для просмотра файлов, ввода команд и перехода из него в другие режимы. В командный режим можно попасть по нажатию клавиши `<Esc>`.

При нажатии клавиши «:» становится доступна командная строка Vim, в которой вводятся следующие команды:

- команда выхода – `quit` либо `q`;
- команда сохранения – `write` либо `w`, параметром которой может быть имя файла;
- вызов справки – `help` либо `h`.

Для остальных клавиш (и их последовательностей) допускается задавать любые команды либо использовать значения по умолчанию.

Перечисленные ниже команды вводятся в основном режиме (если нет специального уточнения). Все они имеют команднострочные аналоги и могут быть легко переопределены.

17.7.2.2. Визуальный режим работы

Визуальный режим работы предназначен, в первую очередь, для выделения блоков текста. Переход в визуальный режим выполняется с помощью следующих сочетаний клавиш:

- <v> для посимвольного выбора;
- <Shift>+<v> для построчного выбора;
- <Ctrl>+<v> для блочного выбора.

В режиме посимвольного выделения (при переходе по клавише «v») допускается оперировать следующими сущностями:

- слово («w»);
- предложение («s»);
- параграф («p»);
- блок («b»).

Выделение при этом нужно начинать с позиции курсора («a»), или же с начала блока («i»). Например, выделение текущего блока (участка, ограниченного парными элементами) можно произвести следующим образом:

```
<Esc>vib
```

Копирование в буфер выделенного текста осуществляется по «u», вырезание по «d» а вставка, соответственно, «r».

17.7.2.3. Режим редактирования

Режим редактирования предназначен для ввода текста. Переключение на режим редактирования осуществляется нажатием клавиши <Insert>.

17.7.2.4. Переходы

Для перехода на строку с номером n используется команда G. Так для перехода к началу текста нужно набрать 1G, для сотой строки 100G, а для перехода в конец текста – \$G.

Для перехода на n символов в нужную сторону используются клавиши навигации на клавиатуре. То есть для перехода на 1000 символов вниз нужно набрать «1000» и нажать клавишу «↓».

Для перемещения по тексту допускается использовать следующие команды:

- «(», «)» – для перемещения по предложениям;
- «{», «}» – для параграфов;
- «[[«, «]]» – для функций;
- «%» – переход к парной скобке;
- «'» – к предыдущему положению;
- <Ctrl>+<O>, <Ctrl>+<I> – соответственно, назад и вперед по истории переходов.

17.7.2.5. Метки

Используются для отметки позиции (<буква>-метка, где меткой является любая буква) и быстрого к ней перехода (<'>-метка). Метки нижнего регистра действительны в пределах данного файла, метки верхнего регистра действуют во всех открытых файлах.

Список всех меток можно получить командой `marks`.

17.7.2.6. Регистры

Регистр отмечается видом <"буква>. К нему применимы все стандартные действия: копирование в него ("<метка>y), вырезание ("<метка>d), и вставка из него ("<метка>p), можете вместо p использовать [p,]p для вставки соответственно перед, или после курсора).

В режиме редактирования вставка из регистра осуществляется по <Ctrl>+R<метка>. Для добавления данных в регистр используйте заглавную метку.

Также допускается писать в регистр, воспользовавшись командой «q<метка>» и завершив запись по q. Таким образом сохраняется макрос, выполнить который можно по «@<метка>».

Регистры с метками «*» и «+» совпадают с X-Window clipboards, «%» – соответствует редактируемому файлу. Для просмотра содержимого всех регистров нужно воспользоваться командой `:registers`, либо `:reg метка1метка2...` для просмотра только выбранных регистров.

17.7.2.7. Фолды

Фолды предназначены для сокрытия строк, ненужных в данный момент.

По умолчанию фолды активированы в режиме ручной расстановки. Все команды для работы с фолдами начинаются с `z`:

- создание фолд выполняется командой `zf`;
- открытие фолд производится командой `zo` либо нажатием навигационной стрелки «←→»;
- закрытие кода в существующий фолд – по `zc`.

Для автоматического подключения фолд по отношению к табуляции нужно добавить в файл настроек следующую строку:

```
set foldmethod=indent
```

17.7.2.8. Сессии

Сессии предназначены для сохранения текущего состояния и настройки редактора таким образом, что при следующем запуске работа продолжится с того же места.

Сессии создаются следующей командой:

```
:mksession /path/to/Session.vim
```

Чтение сессий выполняется командой:

```
:so /path/to/Session.vim
```

Для сохранения текущего контекста (текст, положение курсора в коде, текущая расстановка фолдов) нужно использовать команду `:mkview`, а для чтения – `:loadview`.

Автоматическое сохранение и чтение контекста при начале и окончании редактирования файла может быть реализовано следующим кодом (применяется для всех файлов, имеющих точку в имени):

```
au BufWinLeave *.* mkview  
au BufWinEnter *.* silent loadview
```

17.7.2.9. Поиск и замена

Поиск по тексту осуществляется следующими командами:

- / – поиск по регулярному выражению вперед;
- ? – поиск по регулярному выражению в обратном направлении;
- n – продолжение поиска далее по тексту;
- N – повторение предыдущего запроса;

- # либо * – поиск слова под установленным курсором.

Для поиска с заменой рекомендуется использовать следующую команду:

```
%s/что/на что/gic
```

где % означает работу со всем текстом (а не с текущей строкой), g – глобальная замена (а не первое совпадение), i – игнорирование регистра, а c – подтверждение каждого действия.

17.7.2.10. Автодополнение, отмена, смена регистра, повтор

Автодополнение производится по содержимому данного файла, а также указанных в переменной dictionary по нажатию клавиш ``.

Для отмены предыдущих действий в режиме автодополнения используется u.

Для смены регистра выделенного участка (или буквы под курсором) используется ~. При этом команда U – принудительно устанавливает верхний регистр, а u – нижний.

Для повтора прошлой команды используется символ «.».

17.7.2.11. Конфигурация

Файл конфигурации используется для настройки различных аспектов поведения и внешнего вида Vim. Комментарии в этом файле начинаются с символа «"» (двойная кавычка) и продолжаются до конца строки. Основным конфигурационным файлом является ~/.vimrc.

Активация русского шрифта в GUI-режиме, плюс выбор темы для обоих режимов осуществляется, например, следующим кодом:

```
if has("gui_running")
  colorscheme ron
  set guifont=-cronyx-courier-medium-r-normal-*-*120-*-*m-*-koi8-r
endif
if !has("gui_running")
  colorscheme elflord
endif
```

В файл конфигурации можно добавить привычное поведение и привычные сочетания клавиш:

```
"Выход по F10
nmap <F10> :q<CR>
imap <F10> <ESC>:q<CR>
"Сохранение по F2
nmap <F2> :w<CR>
```

```
imap <F2> <ESC>:w<CR>i<Right>  
"Компиляция по F9  
nmap <F9> :make<CR>  
imap <F9> <ESC>:make<CR>
```

В Vim присутствует подробная документация по настройкам – `:options`.

17.8. Средства настройки отложенного исполнения команд

17.8.1. Служба `crond`

Для регулярного запуска команд в ОС Альт СП используется служба `crond`.

Служба `crond` запускается при загрузке системы и проверяет очередь заданий `at` и заданий пользователей в файлах `crontab`. При запуске, служба `crond` сначала проверяет каталог `/var/spool/cron` на наличие файлов `crontab`, файлы `crontab` имеют имена пользователей, соответствующие именам пользователей из `/etc/passwd`. Каждый пользователь может иметь только один файл `crontab`, записей в файле может быть несколько.

В случае, если задание не было обнаружено, `crond` переходит в режим ожидания на одну минуту и затем вновь приступает к поискам команды, которую следует запустить в этот момент. Большую часть времени служба `crond` проводит в режиме ожидания, и для ее работы используется минимум системных ресурсов.

Чтобы определить список задач для `cron`, используется команда `crontab`.

17.8.1.1. `Crontab`

Утилита `crontab` управляет доступом пользователя к службе `crond` путем копирования, создания, выдачи содержимого и удаления файлов `crontab`, таблиц заданий. При вызове без опций, `crontab` копирует указанный файл или стандартный входной поток (если файл не указан) в каталог, в котором хранятся пользовательские таблицы заданий `cron`. Каждый пользователь может иметь свои собственные файлы `crontab`, и, хотя эти файлы доступны в `/var/spool/cron`, они не предназначены для редактирования напрямую.

Синтаксис:

```
crontab [имя_файла]  
crontab [ -elr ] имя_пользователя
```

Опции:

- 1) `-e` – редактирует копию файла `crontab` текущего пользователя или создает пустой файл для редактирования, если соответствующего файла `crontab` не существует. Когда редактирование завершается, файл устанавливается в качестве пользовательского файла `crontab`. Переменная среды `EDITOR` задает редактор, вызываемый при указании опции `-e`. Все задания в файле `crontab` должны создаваться с помощью утилиты `crontab`;
- 2) `-l` – отображает текущий файл `crontab` на стандартный вывод;
- 3) `-r` – удаляет текущий файл `crontab`.

17.8.1.2. Контроль доступа к `crontab`

Доступ пользователя к `crontab` разрешен, если:

- имя пользователя указано в файле `/etc/cron.d/cron.allow`;
- файл `/etc/cron.d/cron.allow` не существует и имя пользователя не указано в файле `/etc/cron.d/cron.deny`.

Доступ пользователя к `crontab` не разрешен, если:

- файл `/etc/cron.d/cron.allow` существует и имя пользователя в нем не указано;
- файл `/etc/cron.d/cron.allow` не существует и имя пользователя указано в файле `/etc/cron.d/cron.deny`.

Правила разрешения и запрещения выполнения заданий применимы к пользователю `root`, только если существуют файлы `allow/deny`.

В файлах `allow/deny` надо задавать по одному имени пользователя в строке.

17.8.1.3. Формат записи файла `crontab`

Редактировать `crontab` пользователя можно используя команду:

```
crontab -e
```

Файл `crontab` состоит из строк, содержащие шесть полей. Поля разделяются пробелами или символами табуляции. Первые пять полей – целочисленные шаблоны, задающие:

- минуту (0 – 59);
- час (0 – 23);

- день месяца (1 – 31);
- месяц года (1 – 12);
- день недели (0 – 6, причем 0=воскресенье).

Каждый из этих шаблонов может представлять собой звездочку (которая обозначает все допустимые значения) или список элементов через запятые. Элемент – число или два числа через дефис (что обозначает закрытый интервал). Обратите внимание, что дни можно указывать в двух полях (день месяца и день недели). Оба поля учитываются, если заданы в виде списка элементов (запись: 30 4 1,15 * 5 приведет к выполнению команды в 4:30 пополуночи первого и пятнадцатого числа каждого месяца, плюс в каждую пятницу). При указании диапазона можно пропускать некоторые его значения, указав шаг в форме «/число». Например: «0-23/2» для поля час означает запуск команды через два часа. Шаг можно указывать также после звездочки: «каждые два часа» соответствует значению «*/2». Для задания полей месяц и день_недели можно использовать имена. Указывайте первые три буквы нужного дня или месяца на английском, регистр букв не имеет значения. Диапазоны или списки имен не разрешены.

Служба cronд запускает команды, когда значения полей минута, час, месяц и хотя бы одно из полей число и день_недели, совпадают с текущим временем. Служба cronд сверяет директивы с текущим временем раз в минуту.

Вместо первых пяти полей допустимо указание одного из восьми специальных триггеров:

- @reboot – выполнить команду один раз, при запуске cron;
- @yearly – выполнять команду каждое 1 января, «0 0 1 1 *»;
- @annually – эквивалентно @yearly;
- @monthly – выполнять команду в начале каждого месяца, «0 0 1 * *»;
- @weekly – выполнять команду каждое воскресенье, «0 0 * * 0»;
- @daily – выполнять команду в полночь, «0 0 * * *»;
- @midnight – эквивалентно @daily;
- @hourly – выполнять команду раз в час, «0 * * * *».

Шестое поле в строке файла `crontab` – строка, выполняемая командным интерпретатором в указанные моменты времени. Символ `%` (процент) в этом поле, если он не замаскирован `\%` (обратной косой), преобразуется в символ новой строки.

Только первая строка (до символа `%` или до конца строки) поля команды выполняется командным интерпретатором. Другие строки передаются команде как стандартный входной поток. Пустые строки, ведущие пробелы и символы табуляции игнорируются. Строки, начинающиеся с символа (`#`) считаются комментариями и игнорируются. Комментарии не допускаются в тех же строках, где расположены команды `cron`, так как они будут распознаны как части команды. По этой же причине комментарии не разрешены в строках, задающих переменные среды.

Строка-директива представляет собой либо задание переменной среды, либо команду `cron`.

Демон `crond` предоставляет каждому командному интерпретатору стандартную среду, задавая переменные `HOME`, `LOGNAME`, `SHELL(=/bin/sh)`, `TZ` и `PATH`. Стандартное значение переменной `PATH` для пользовательских заданий `cron` – `/usr/bin`, а для заданий `cron` пользователя `root` – `/usr/sbin:/usr/bin`.

Если стандартный выходной поток и стандартный поток ошибок команд не перенаправлены, любые сгенерированные результаты или сообщения об ошибках будут отправлены пользователю по электронной почте.

17.8.1.4. Примеры

Далее приведены примеры использования таблиц `crontab` в ходе администрирования ОС Альт СП.

17.8.1.4.1. Пример 1

```
$ crontab -e
#minute (0-59),
#| hour (0-23),
#| | day of the month (1-31),

#| | | month of the year (1-12),
#| | | | day of the week (0-6 with 0=Sunday).
#| | | | | commands
# Каждые 5 минут записывать результат вывода
# команды date в файл date.txt в домашнем каталоге
*/5 * * * * date > ~/date.txt
```

ЛКНВ.11100-01 90 03

```
# Выполнять задание в 18 часов 7 минут 13 числа
# каждого месяца и по пятницам
7 18 13 * 5 /home/www/myscript.pl
# Выполнять задание по воскресеньям в 10 час 30 минут
30 10 * * 0 /home/www/myscript.pl
crontab: installing new crontab
```

Вывод crontab: installing new crontab означает, что новый crontab успешно установлен.

17.8.1.4.2. Пример 2

```
# использовать для запуска команд /bin/sh
# не обращая внимание на то, что написано в /etc/passwd
SHELL=/bin/sh
# отправлять вывод выполнения команд по электронной
# почте пользователю 'paul'
# не обращая внимания на то, чей это crontab
MAILTO=paul
#
# запускать пять минут пополуночи, каждый день
5 0 * * * $HOME/bin/daily.job >> $HOME/tmp/out 2>&1
# запускать в 14:15 первого числа каждого месяца
15 14 1 * * $HOME/bin/monthly
# запускать в 22.00 каждый рабочий день
0 22 * * 1-5 mail -s "Уже 10 вечера"
23 0-23/2 * * * echo "запуск в 00:23, 2:23, 4:23 ..., каждый день"
5 4 * * sun echo "запуск в 4:05 каждое воскресенье"
```

17.8.1.5. Дополнительные возможности таблиц

Таблицы crontab обладают следующими дополнительными возможностями:

- при задании дня недели 0 и 7 соответствуют воскресенью;
- допускается указывать одновременно и списки, и диапазоны в одном и том же поле;
- допускается указывать диапазоны с пропусками – например, «1-9/2» соответствует «1,3,5,7,9»;
- допустимо указание месяцев или дней недели по имени;
- в crontab разрешено задавать переменные среды вручную;
- вывод команд отсылается почтой владельцу файла crontab, а также может отправляться кому-либо другому, либо отправка может быть отключена (функция не поддерживается в SysV);
- любая из команд с префиксом «@» может заменять первые пять полей файла.

17.8.2. Команда `at`

Для запуска одной или более команд в заранее определенное время используется команда `at`. В ней можно определить время и (или) дату запуска той или иной команды.

Команда `at` требует двух (или большего числа) параметров – как минимум, следует указать время запуска, и какая команда должна быть запущена. Параметры запуска с помощью команды `at` указываются в виде списка строк, следующих за ней. Ввод каждой строки завершается нажатием клавиши `<Enter>`. По окончании ввода всей команды нажать клавиши `<Ctrl>+<D>` для ее завершения.

Например, если нужно запустить команды в 1:23, следует ввести:

```
at 1:23
lpr /usr/sales/reports/.
echo "Files printed"
```

В указанном примере будут распечатаны все файлы каталога `/usr/sales/reports`, и пользователю будет выведено сообщение на экран монитора.

После ввода всей команды отобразится следующая запись:

```
job 756603300.a at Tues Jan 21 01:23:00 2007
```

Это означает, что указанные команды будут запущены, как и было задано, в 1:23. В сообщении также приведен идентификатор задания (756603300.a), который понадобится, если нужно отменить задание:

```
at -d 756603300.a
```

В случае, если список команд находится в файле, например, `getdone`, и нужно запустить все перечисленные в нем команды в 10:00, следует воспользоваться одной из двух форм команды `at`:

```
at 10:00 < getdone либо at 10:00 -f getdone
```

Обе приведенные команды эквивалентны. Разница заключается в том, что в первой команде используется механизм перенаправления потоков ввода-вывода, во второй команде – дисковый файл.

Кроме времени, в команде `at` может быть также определена дата:

```
at 17:00 Jan 24
lp /usr/sales/reports/
echo "Files printed"
```

Задания, определяемые администратором, помещаются в очередь, которую ОС периодически просматривает. Администратору необязательно находиться в системе для того, чтобы `at` отработала задания, команда будет работать в фоновом режиме.

Для того чтобы просмотреть очередь заданий, нужно ввести следующую команду:

```
at -l
```

В случае, если предыдущие примеры были запущены, то будет выведено:

```
job 756603300.a at Sat Dec 20 01:23:00 2007 job 756604200.a at Sat Jan 24  
17:00:00 2008
```

Администратор видит только свои задания по команде `at`.

Для удаления задания из очереди следует запустить `at` с опцией `-d` и номером удаляемого задания следующим образом:

```
at -d 756604200.a
```

Далее представлены варианты использования команды `at`.

Выполнить задание во время `hh:mm` в 24-часовом формате:

```
at hh:mm
```

Выполнить задание во время `hh:mm` в 24-часовом формате в соответствующий день:

```
at hh:mm месяц день год
```

Вывести список заданий в очереди (псевдоним команды – `atq`):

```
at -l
```

Выполнить задание через определенное время, которое задано параметром `count` в соответствующих единицах – неделях, днях, часах или минутах:

```
at now+count time-units
```

Удалить задание с идентификатором `job_ID` из очереди (псевдоним команды – `atrm`):

```
at -d job_ID
```

Администратор может применять все эти команды. Для других пользователей права доступа к команде `at` определяются файлами `/etc/at.allow` и `/etc/at.deny`. В случае, если существует файл `/etc/at.allow`, то применять команду `at` могут только перечисленные в нем пользователи. В случае, если же такого файла нет,

проверяется наличие файла `/etc/at.deny`, в котором отражено, кому запрещено пользоваться командой `at`. Также если ни одного из файлов, описывающих доступ к «alt», нет, то команда `at` доступна только пользователю с идентификатором `root`.

17.8.3. Команда `batch`

Команда `batch` позволяет ОС самой решить, когда наступает подходящий момент для запуска задачи – например, когда система находится в состоянии наименьшей загрузки, и процессы запускаются в фоновом режиме.

Формат команды `batch` представляет собой список заданий для выполнения, следующих в строках за ней, заканчивается список комбинацией клавиш `<Ctrl>+<D>`. Также допускается поместить список команд в файл и перенаправить его на стандартный ввод команды `batch`.

Например, для сортировки набора файлов, печати результатов и вывода сообщения нужно ввести следующие команды:

```
batch
sort /usr/sales/reports ; lp
echo "Files printed"
```

В ответ на это система выдаст:

```
job 7789001234.b at Fri Feb 21 11:43:09 1999
```

Примечание. Дата и время, приведенные в сообщении, соответствуют нажатию клавиш `<Ctrl>+<D>`.

17.9. Control

В дистрибутивах ОС Альт СП для управления доступом к важным службам используется подсистема `control`. `control` – механизм переключения между неким набором фиксированных состояний для задач, допускающих такой набор.

Команда `control` доступна только для суперпользователя (`root`).

Для того чтобы посмотреть, что означает та или иная политика `control` (разрешения выполнения конкретной команды, управляемой `control`), запустите команду с ключом `help`, например:

```
# control su help
public: Any user can execute /bin/su
```

wheel: Any user can execute /bin/su, but only "wheel" group members can switch to superuser

wheelonly: Only "wheel" group members can execute /bin/su

restricted: Only root can execute /bin/su

То есть для управления командой su есть такие политики:

- public – любой пользователь может выполнить команду /bin/su;
- wheel – любой пользователь может выполнить команду su, но только пользователи, входящие в группу wheel, могут получить через нее права root;
- wheelonly – только пользователи, входящие в группу wheel, могут выполнить команду su;
- restricted – только root может выполнять команду su.

Для получения текущего значения control, необходимо выполнить команду:

```
# control <команда>
```

Например:

```
# control fusermount
fuseonly
```

Для переключения состояния control, необходимо выполнить команду:

```
# control <команда> <состояние>
```

Например:

```
# control fusermount public
```

Для переключения состояния control вызывает соответствующий скрипт из /etc/control.d/facilities/.

Запустив control без параметров, можно увидеть полный список команд, управляемых командой (facilities) вместе с их текущим состоянием и набором допустимых состояний.

17.10. Защищенный интерпретатор команд SSH

Защищенный интерпретатор команд SSH – клиент-серверная система для организации защищенных туннелей для удаленного доступа к другим компьютерам.

SSH реализует соединение с удаленным компьютером, которое позволяет защититься от следующих угроз:

- прослушивание данных, передаваемых по этому соединению;

- манипулирование данными на пути от клиента к серверу;
- подмена клиента либо сервера путем манипулирования IP-адресами, DNS либо маршрутизацией.

Для создания защищенного туннеля используется программа ssh.

Инициировать соединение с сервером можно командой:

```
ssh <имя_клиента>@IP_addr
```

где IP_addr – IP-адрес компьютера с запущенной службой sshd.

При использовании идентификации по паролю на сервере должна существовать учетная запись с указанным именем клиента.

Параметры, относящиеся к способу аутентификации, а также все прочие настройки ssh (см. п. 8.10.1) указываются в конфигурационном файле /etc/ssh/ssh_config.

Конфигурационные файлы разбиты на разделы, установки которых относятся к отдельному компьютеру, группе компьютеров или ко всем компьютерам, при этом установки разных разделов могут конфликтовать друг с другом. Предпочтение в данном случае будет отдаваться тому параметру, который указан раньше.

17.11. Средство управления процессами xinetd

Средство управления процессами xinetd (далее – сервер xinetd) выполняет функции управления процессами, которые обеспечивают работу сервисов подключения к локальным и глобальным сетям.

Сервер xinetd представляет собой единственный процесс, который выполняет прослушивание всех портов на наличие запросов от других сервисов, перечисленных в файле конфигурации xinetd.conf (расположен в директории /etc): когда на порт поступает запрос, сервер xinetd запускает соответствующий сервер.

Сервисы, перечисленные в конфигурационном файле сервера xinetd, можно разделить на две группы.

Сервисы из первой группы («multi-threaded») на каждый новый запрос запускают новый серверный процесс.

Для таких сервисов сервер `xinetd` продолжает прослушивать сеть на соответствующем порту, ожидая новых запросов на порождение нового процесса.

В другую группу («`single-threaded`») включаются сервисы службы, которые в состоянии обрабатывать новые соединения. В ходе работы с ними сервер `xinetd` прекращает обработку новых запросов до тех пор, пока серверный процесс не завершит свою работу. Сервисы в этой группе также обычно относят к группе «`datagram-based`», работающих с дейтаграммными протоколами передачи данных формата UDP.

Сервер `xinetd` позволяет сохранять системные ресурсы за счет контроля запуска серверных процессов. Полностью соответствуя назначению запускать требуемые сервисы, сервер `xinetd` осуществляет также функции контроля доступа и регистрации событий. Кроме того, сервер `xinetd` не ограничен сервисами, перечисленными в файле `/etc/services`. Также допускается использовать сервер `xinetd` для запуска сервисов специального назначения.

Синтаксис:

```
xinetd [опции]
```

Опции:

- `-d` – активирует режим отладки. Указание этой опции приводит к большому количеству отладочных сообщений, которые делают возможным использование отладчика на `xinetd`;
- `--syslog syslog_facility` – разрешает протоколирование создаваемых `xinetd` сообщений через `syslog` с заданным `syslogfacility`. Поддерживаются следующие имена `facility`: `daemon`, `auth`, `user`, `local[0-7]` (назначение можно посмотреть в `syslog.conf`). Данная опция неэффективна в режиме отладки, так как все сообщения отправляются на терминал;
- `--filelog файл_журнала` – сообщения, создаваемые `xinetd` будут помещаться в указанный файл. Сообщения всегда добавляются к уже существующему файлу. Если файл не существует, то он будет создан. Данная опция неэффективна в режиме отладки, так как все сообщения отправляются на терминал;

- `-f файл_настроек` – задает файл, который `xinetd` использует для настройки.
По умолчанию это `/etc/xinetd.conf`;
- `-pidfile pid_файл` – в этот файл записывается идентификатор процесса.
Данная опция неэффективна в режиме отладки;
- `-stayalive` – `xinetd` будет оставаться запущенным, даже если не задано никаких служб;
- `-loop rate` – устанавливает верхнюю величину цикла, по которой определяется, что служба работает с ошибками и по которой она отключается. Величина цикла задается в терминах количества серверов в секунду, которое может быть запущено в обработку (`fork`). Для этой опции, корректное значение определяется скоростью вашей машины. По умолчанию равно 10;
- `-reuse` – `xinetd` будет устанавливать опцию сокета `SO_REUSEADDR` перед привязкой сокета службы к какому-либо интернет-адресу. Это позволяет привязать адрес, даже если есть программа, которая уже использует его, например, в том случае, если некоторые серверы были запущены во время предыдущего запуска `xinetd` и еще не завершили свою работу. Данная опция не оказывает влияния на службу RPC;
- `-limit proc_limit` – устанавливает ограничение на количество одновременно запущенных процессов, которые может запустить `xinetd`. Ее назначение предотвращать переполнение таблицы процессов;
- `-logprocs limit` – устанавливает ограничение на количество одновременно запущенных серверов на один идентификатор удаленного пользователя;
- `-shutdownprocs limit` – устанавливает ограничение на количество одновременно запущенных серверов для завершения работы службы;
- `-version` – вывести информацию о версии `xinetd`;
- `-cc interval` – `xinetd` будет выполнять периодические проверки своего внутреннего состояния каждые `interval` секунд.

Опции `syslog` и `filelog` являются взаимноисключающими. Если ни одна из них не задана, то по умолчанию используется `syslog` с `daemonfacility`. Не путайте сообщения `xinetd` с сообщениями, которые создаются службами. Последние протоколируются только если это задано в файле с настройками.

Сервер `xinetd` выполняет определенные действия при получении определенных сигналов. Действия, ассоциированные с соответствующими сигналами, могут быть переопределены путем редактирования `config.h` и последующей компиляции.

Сигналы:

- `SIGHUP` – заставляет выполнить жесткую перенастройку, означающую, что `xinetd` перечитает файл с настройками и завершит работу серверов для тех служб, которые больше не доступны. Управление доступом выполняется снова на уже запущенных серверах через проверку удаленных подключений, времени доступа и копий серверов. Если количество копий серверов уменьшается, то некоторые произвольно выбранные сервера будут убиты, чтобы соблюсти ограничение; это случится после завершения работы тех серверов, которые попадают под ограничение доступа с удаленных адресов или ограничение времени доступа. Также, если флаг `INTERCEPT` был сброшен и происходит его установка, то будет завершена работа любых запущенных серверов для служб с этим флагом. Цель такого поведения – убедиться, что после жесткой перенастройки не будет запущено серверов, которые могут принимать пакеты с тех адресов, которые не соответствуют критериями управления доступом;
- `SIGQUIT` – приводит к завершению работы;
- `SIGTERM` – завершает работу всех запущенных серверов перед завершением работы `xinetd`;
- `SIGUSR1` – приводит к снятию дампа внутреннего состояния (по умолчанию файл дампа это `/var/run/xinetd.dump`; чтобы изменить данное имя файла нужна правка `config.h` и перекомпиляция);

- SIGIOT – производит внутреннюю проверку того, что структуры данных, используемые программой не повреждены. Когда проверка завершится, xinetd сгенерирует сообщение о том, успешно прошла проверка или нет.

При реконфигурации файлы журналов закрываются и вновь открываются. Это позволяет удалять старые файлы журналов.

17.12. Работа со смарт-картами

Для настройки работы со смарт-картами нужно установить дополнительные пакеты:

1) синхронизировать файлы описаний пакетов с источником пакетов, выполнив команду:

```
# apt-get update
```

2) установить пакеты для поддержки программно-аппаратного комплекса электронно-цифровой подписи и хранения ключевой информации «RUTOKEN», выполнив команду:

```
# apt-get install opensc pcsc-lite pam_pkcs11 librtpkcs11ecp
pcsc-lite-ccid libp11 nss-utils
```

И для рабочей станции установить пакет lightdm-gtk-greeter.

17.12.1. Двухфакторная аутентификация

На токене должны присутствовать ключевая пара и сертификат.

Для генерирования ключевой пары на токене и создания самоподписанного сертификата, используя openssl, нужно выполнить следующие действия (путь зависит от архитектуры, в примере для x86_64):

1) запустить сервис поддержки смарт-карт, выполнив команду:

```
# systemctl start pcscd
```

2) сгенерировать ключевую пару, выполнив команду:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so --keypairgen
--key-type rsa:2048 -l --id 45
```

3) сгенерировать сертификат в формате PEM:

```
# openssl
OpenSSL> engine dynamic -pre
SO_PATH:/usr/lib64/openssl/engines-*/libpkcs11.so -pre ID:pkcs11 -
pre LIST_ADD:1 -pre LOAD -pre
MODULE_PATH:/usr/lib64/librtpkcs11ecp.so
```

```
OpenSSL> req -engine pkcs11 -new -key 45 -keyform engine -x509 -out
CA.pem -text
```

где engines-* – текущая версия модулей openssl;

4) конвертировать сертификат из формата PEM в формат CRT:

```
OpenSSL> x509 -in CA.pem -out cert.crt -outform DER
```

5) сохранить сертификат на аутентифицирующий носитель:

```
# pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -l -y cert
-w cert.crt --id 45
```

Для настройки двухфакторной аутентификации нужно выполнить следующие действия:

1) отредактировать файл /etc/security/pam_pkcs11/pam_pkcs11.conf для установки аутентификации по «RUTOKEN» следующим образом:

- закомментировать строку # use_pkcs11_module = opensc;

и добавить строку use_pkcs11_module = rutoken;:

```
# use_pkcs11_module = opensc;
use_pkcs11_module = rutoken;
```

- после строки use_pkcs11_module = rutoken; добавить модуль rutoken:

```
use_pkcs11_module = rutoken;
pkcs11_module rutoken {
ca_dir = /etc/security/pam_pkcs11/cacerts;
crl_dir = /etc/security/pam_pkcs11/crls;
module = /usr/lib64/librtpkcs11ecp.so;
cert_policy = subject;
description = "Rutoken ECP";
slot_description = "none";
}
```

Значение use_mappers привести к виду:

```
use_mappers = digest, cn, pwent, uid, mail, subject, null,
opensc;
```

2) включить сервисы поддержки смарт-карт, выполнив команды:

```
# systemctl enable pcscd
# systemctl start pcscd
```

3) включить системную аутентификацию по смарт-картам в графическом интерфейсе, выполнив команду:

```
# control system-auth pkcs11
```

- 4) добавить информацию об удостоверяющем центре на машину (файл о сертификате создан в начальных условиях):

```
cp CA.pem /etc/security/pam_pkcs11/cacerts/
certutil -A -n 'Root CA' -t 'CT,C,C' -a -d /etc/pki/nssdb/ -i
./CA.pem
```

- 5) добавить информацию о сертификате в домашний каталог пользователя:

```
mkdir /home/user/.eid/
cat CA.pem > /home/user/.eid/authorized_certificates
```

- б) для возможности аутентификации по сертификату в консоли нужно в файл

/etc/pam.d/login вначале добавить строку:

```
auth [success=done authinfo_unavail=ignore ignore=ignore
default=die] pam_pkcs11.so
```

17.13. Поддержка файловых систем

Файловая система представляет собой набор правил, определяющих то, как хранятся и извлекаются документы, хранящиеся на устройстве.

В ОС Альт СП поддерживаются следующие файловые системы:

- ext2 – нежурналируемая файловая система; относительно проста в восстановлении, но нуждается в относительно долгой проверке целостности после сбоя питания или ядра. Может использоваться для /boot или readonly-разделов;
- ext3 – журналируемая и достаточно надежная файловая система, имеет среднюю производительность;
- ext4 – журналируемая файловая система, логическое продолжение ext3, позволяет полностью отключить журналирование;
- btrfs – поддерживает снимки (копии файловой системы на определенный момент времени), сжатие и подтома;
- iso9660 – файловая система ISO 9660 для дисков с данными компакт-дисков.

Файловые системы FAT/FAT32/NTFS поддерживаются в установленной системе, но не для установки на них Linux.

Проверка поддержки файловых систем ext2, ext3, ext4, iso9660, fat16, fat32, ntfs:

1) создать раздел объемом менее 4 Гбайт на flash-накопителе (например, /dev/vdc1).

2) для создания ISO-файла установить пакет genisoimage:

```
# apt-get install genisoimage
```

3) создать каталог /mnt/filesystem, в который будет монтироваться раздел:

```
# mkdir /mnt/filesystem
```

4) отформатировать раздел в проверяемую файловую систему:

- для ext2:

```
# mkfs.ext2 /dev/vdc1
```

- для ext3:

```
# mkfs.ext3 /dev/vdc1
```

- для ext4:

```
# mkfs.ext4 /dev/vdc1
```

- для fat16:

```
# mkfs.fat -F 16 /dev/vdc1
```

- для fat32:

```
# mkfs.fat -F 32 /dev/vdc1
```

- для ntfs:

```
# mkfs.ntfs /dev/vdc1
```

- для iso9660 – создать iso-файл из каталога /etc:

```
# mkisofs -r -jcharset koi8-r -o /root/cd.iso /etc
```

5) для проверки поддержки файловых систем ext2, ext3, ext4, fat16, fat32, ntfs:

- примонтировать раздел с файловой системой в каталог /mnt/filesystem:

```
# mount /dev/vdc1 /mnt/filesystem
```

- проверить возможность записи файла на текущую файловую систему:

```
# echo test_content > /mnt/filesystem/test.fs
```

- проверить командой:

```
# ls -l /mnt/filesystem/test.fs
-rw-r--r--. 1 root root 13 май 23 20:10
/mnt/filesystem/test.fs
```

- проверить возможность чтения файла с текущей файловой системой:

```
# cat /mnt/filesystem/test.fs
```

б) для проверки поддержки файловой системы iso9660 смонтировать созданный ISO-файл в каталог /mnt/filesystem/ (файл образа диска будет примонтирован в режиме «только для чтения»):

```
# mount -o loop,ro /root/cd.iso /mnt/filesystem/
```

Примечание. Для просмотра файловых систем на физических дисках можно воспользоваться командой `df`:

```
$ df -Th | grep "^/dev"
```

или `lsblk`:

```
$ lsblk -f
```

Команда `fsck` позволяет узнать файловую систему раздела, который еще не примонтирован:

```
# fsck -N /dev/sdc1
```

`fsck` из `util-linux 2.39.2`

```
[/sbin/fsck.ext4 (1) -- /dev/sdc1] fsck.ext4 /dev/sdc1
```

17.14. Поддержка сетевых протоколов

17.14.1. SMB

Samba – пакет программ, которые позволяют обращаться к сетевым дискам и принтерам на различных ОС по протоколу SMB/CIFS. Имеет клиентскую и серверную части.

17.14.1.1. Настройка Samba

Samba настраивается с помощью конфигурационного файла `/etc/samba/smb.conf`.

Примечание. После редактирования файла `smb.conf`, следует запускать команду `testparm` для проверки файла на синтаксические ошибки.

17.14.1.1.1. Добавление пользователя

Samba использует отдельную от системной базу данных пользователей. Для возможности доступа пользователя к папке (если запрещен гостевой доступ) необходимо внести его в базу данных Samba и установить пароль для доступа к общим ресурсам (он может совпадать с основным паролем пользователя). Следует учитывать, что в базу данных Samba можно добавлять только тех пользователей, которые уже есть в системе.

Добавить пользователя в базу данных Samba можно, выполнив команду:

```
# smbpasswd -a <имя_пользователя>
```

Можно создать отдельного пользователя, которому разрешить только доступ к Samba-ресурсам и запретить полноценный вход в систему:

```
# useradd user_samba -d /dev/null -s /sbin/nologin
# smbpasswd -a user_samba
```

17.14.1.1.2. Создание ресурсов общего доступа

Создать папку sharefolder, для общих ресурсов:

```
# mkdir /mnt/sharefolder
```

Назначить нового владельца:

```
# chown -R user_samba:users /mnt/sharefolder
# chmod -R ugo+rwX /mnt/sharefolder
```

Добавить в конфигурационный файл сервера Samba /etc/samba/smb.conf строки:

```
[public]
    #путь к общей папке
    path=/mnt/sharefolder
    read only=No
    #открыть гостевой доступ
    guest ok=Yes
    comment = Public
```

Перезапустить службу:

```
# systemctl restart smb
# systemctl restart nmb
```

17.14.1.1.3. Создание ресурсов общего доступа от имени обычного пользователя

Пользователи могут добавлять, изменять и удалять собственные ресурсы общего доступа. Эта возможность называется `usershares` и предоставляется службой Samba.

Чтобы предоставить общий доступ к папке, нужно в контекстном меню папки выбрать пункт «Опции публикации», затем в открывшемся окне отметить пункт «Опубликовать эту папку», настроить параметры публикации (рис. 536) и нажать кнопку «Создать публикацию».

Примечание. Домашняя папка пользователя по умолчанию не отображается в списке доступных общих ресурсов в сетевом окружении. Обращение к домашней папке выполняется по имени пользователя. Например, для получения доступа к домашней папке пользователя user на компьютере с IP-адресом 192.168.0.190, необходимо указать в адресной строке smb://192.168.0.190/user. Для возможности получения доступа к домашней папке по сети, необходимо добавить каждого локального пользователя в список пользователей Samba.

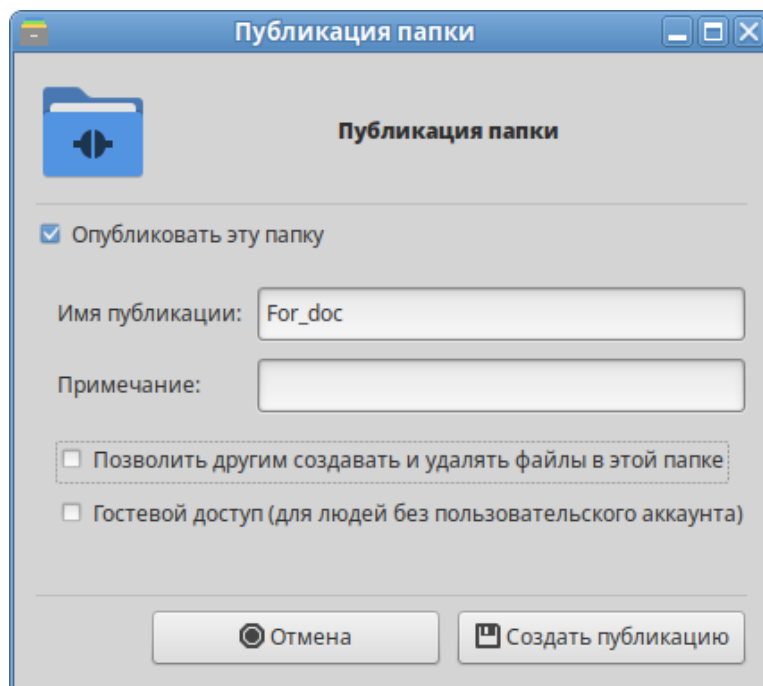


Рис. 536 – Разрешить общий доступ к папке

17.14.1.2. Настройка клиента

17.14.1.2.1. Подключение по протоколу SMB в графической среде

Для создания подключения по протоколу SMB в графической среде МАТЕ можно, запустить файловый менеджер, указать в адресной строке протокол и адрес сервера (рис. 537). Нажать клавишу <Enter>. Будут показаны ресурсы с общим доступом (рис. 538). Для доступа к папке, необходимо указать имя пользователя, пароль и нажать кнопку «Подключиться» (рис. 539).

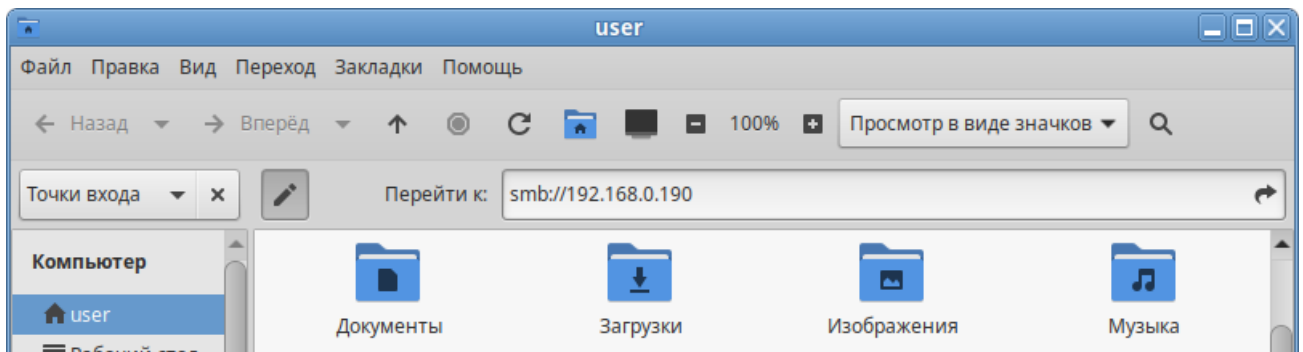


Рис. 537 – Обращение к общей папке по сети

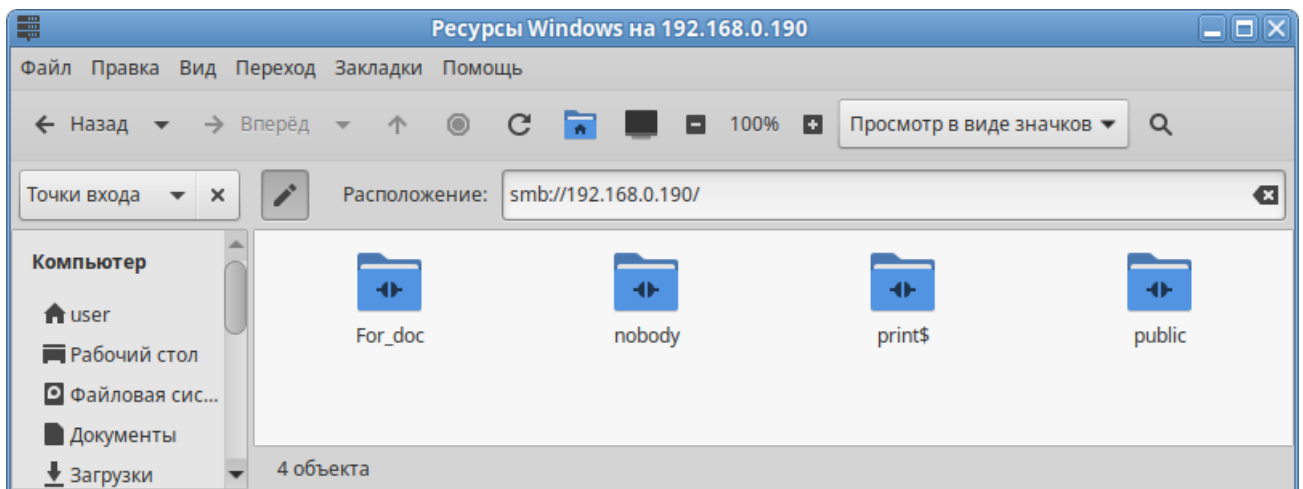


Рис. 538 – Создание подключения по протоколу SMB

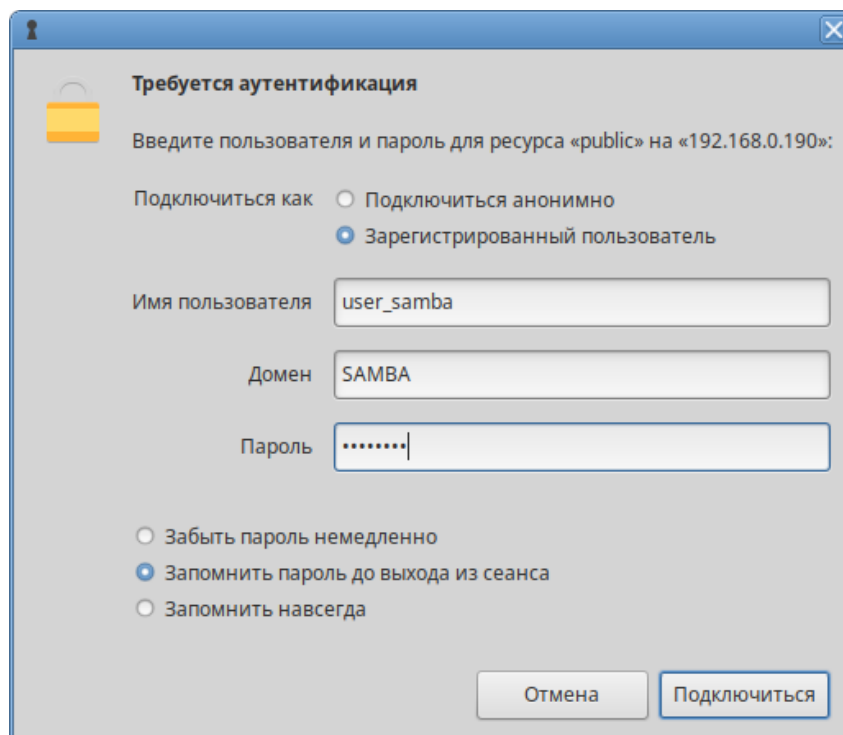


Рис. 539 – Параметры подключения к общей папке

17.14.1.2.2. Монтирование ресурса Samba через /etc/fstab

Просмотреть список общедоступных ресурсов на сервере:

```
$ smbclient -L 192.168.0.190 -U%
```

Просмотреть список ресурсов на сервере доступных пользователю user_samba:

```
$ smbclient -L 192.168.0.190 -Uuser_samba
```

```
Password for [SAMBA\user_samba]:
```

```

      Sharename      Type      Comment
      -
      print$         Disk      Printer Drivers
      public         Disk      Public
      IPC$           IPC       IPC Service (Samba 4.19.7-alt4)
      For_doc       Disk
      user_samba     Disk      Home Directories
SMB1 disabled -- no workgroup available
```

Создать файл /etc/samba/smbacreds с содержимым:

```
username=имя_пользователя
```

```
password=пароль
```

Для защиты информации, права на файл /etc/samba/smbacreds, надо установить так, чтобы файл был доступен на чтение и запись только пользователю-владельцу файла:

```
# chmod 600 /etc/samba/smbacreds
```

и принадлежать root:

```
# chown root: /etc/samba/smbacreds
```

Для монтирования ресурса Samba в /etc/fstab необходимо прописать, строку вида:

```
//СЕРВЕР/ИМЯ_РЕСУРСА          /mnt/точка_монтирования          cifs
credentials=/путь/к/полномочиям/smbacreds 0 0
```

Например:

```
//192.168.0.190/public /mnt/server_public cifs users,_netdev,x-
systemd.automount,credentials=/etc/samba/smbacreds 0 0
```

17.14.2. NFS

17.14.2.1. Настройка сервера NFS

Примечание. Должен быть установлен пакет nfs-server:

```
# apt-get install nfs-server
```

Запустить NFS-сервер и включить его по умолчанию:

```
# systemctl enable --now nfs
```

В файле `/etc/exports` следует указать экспортируемые каталоги (каталоги, которые будет разрешено монтировать с других машин):

```
/myshare dir ipaddr1(rw)
```

Например, чтобы разрешить монтировать каталог `/home` на сервере необходимо добавить в `/etc/exports` строку:

```
/home 192.168.0.0/24(no_subtree_check,rw)
```

где:

- `192.168.0.0/24` – разрешение экспорта для подсети `192.168.0.X`;
- `rw` – разрешены чтение и запись.

Подробную информацию о формате файла можно посмотреть, выполнив команду:

```
$ man exports
```

После внесения изменений в файл `/etc/exports` необходимо выполнить команду:

```
# exportfs -r
```

Проверить список экспортируемых файловых систем можно, выполнив команду:

```
# exportfs
/home          192.168.0.0/24
/srv/public   <world>
```

17.14.2.2. Использование NFS

Подключение к NFS-серверу можно производить как вручную, так и настроив автоматическое подключение при загрузке.

Для ручного монтирования:

- создать точку монтирования:

```
# mkdir /mnt/nfs
```

- примонтировать файловую систему:

```
# mount -t nfs 192.168.0.193:/home /mnt/nfs
```

где:

а) 192.168.0.193 – IP-адрес сервера NFS;

б) /mnt/nfs – локальный каталог, куда монтируется удаленный каталог;

- проверить наличие файлов в /mnt/nfs:

```
# ls -al /mnt/nfs
```

Должен отобразиться список файлов каталога /home, расположенного на сервере NFS.

Для автоматического монтирования к NFS-серверу при загрузке, необходимо добавить следующую строку в файл /etc/fstab:

```
192.168.0.193:/home /mnt/nfs nfs intr,soft,nolock,_netdev,x-systemd.automount 0 0
```

Примечание. Прежде чем изменять /etc/fstab, необходимо смонтировать каталог вручную, для того чтобы убедиться, что все работает.

17.14.3. FTP

В состав дистрибутива ОС Альт СП (Сервер) входит vsftpd (Very Secure FTP Daemon) – полнофункциональный FTP-сервер, позволяющий обслуживать как анонимные запросы, так и запросы от пользователей, зарегистрированных на сервере и имеющих полноценный доступ к его ресурсам.

Для установки vsftpd нужно выполнить следующую команду:

```
# apt-get install vsftpd
```

17.14.3.1. Организация анонимного доступа на основе vsftpd

В конфигурационном файле сервера /etc/vsftpd.conf за разрешение анонимного доступа к серверу vsftpd отвечает параметр anonymous_enable, который по умолчанию имеет значение YES, т. е. анонимный доступ к серверу разрешен.

При установке vsftpd в системе автоматически создается учетная запись псевдопользователя «novsftpd». Это регистрационное имя не должно использоваться кем-либо для входа в систему, поэтому реальный пароль для него не задается. Вместо командного интерпретатора указывается /dev/null.

При установке пакета anonftp автоматически создается каталог, который будет корневым при анонимном подключении, – /var/ftp с правами доступа. Владельцем

этого каталога является пользователь `root`. Группой-владельцем каталога является специальная группа `ftpadmin`, предназначенная для администраторов FTP-сервера.

Если требуется создать в области для анонимного доступа дерево каталогов, следует в каталоге `/var/ftp/pub` установить права доступа `2775`. При этом анонимным пользователям FTP-сервера будет предоставлен доступ на чтение к файлам, находящимся в каталоге.

Владельцем каталога следует назначить пользователя `root`. В качестве группы, которой принадлежит `/var/ftp/pub`, следует назначить группу `ftpadmin`, включив в нее пользователей, которым нужно изменять содержимое каталогов FTP-сервера.

Примечание. Не рекомендуется работать с содержимым от имени пользователя с идентификатором `root`.

Чтобы разрешить анонимным пользователям сервера доступ на запись, нужно создать каталог `/var/ftp/incoming` с правами доступа `3773` (группа-владелец – «`ftpadmin`»), тем самым предоставив анонимным пользователям право записи в этот каталог, но лишив их возможности просмотра его содержимого.

17.14.3.2. Доступ к серверу зарегистрированных пользователей

Чтобы предоставить доступ к FTP-серверу для локально зарегистрированных пользователей, нужно внести изменения в конфигурационный файл `/etc/vsftpd.conf`. Для этого достаточно удалить знак комментария перед директивой `local_enable=YES`. В такой конфигурации клиенты FTP-сервера получают доступ к любым каталогам файловой системы, для которых такой доступ разрешен, исходя из прав соответствующих локальных пользователей. Это могут быть, как домашние каталоги пользователей, так и системные каталоги. Если в настройках `vsftpd` разрешена запись, клиенты получают и все права на запись, которыми располагают эти пользователи.

Сервер `vsftpd` позволяет ограничить возможность пользователей, зарегистрированных локально, перемещаться по дереву каталогов. При этом процесс, работающий с клиентом, будет выполняться в изолированной среде (`chrooted environment`), и пользователь будет иметь доступ только к своему домашнему каталогу и его подкаталогам.

Чтобы ограничить доступ к каталогам для отдельных пользователей, нужно удалить знаки комментариев у следующих строк в конфигурационном файле:

```
chroot_list_enable=YES  
chroot_list_file=/etc/vsftpd/chroot_list
```

В файле `/etc/vsftpd/chroot_list` следует перечислить регистрационные имена пользователей, для которых должна использоваться изолированная среда выполнения. Можно использовать для этого и другой файл, указав его имя в строке `chroot_list_file` конфигурационного файла.

Чтобы ограничить доступ к дереву каталогов для всех пользователей, зарегистрированных локально, следует добавить в конфигурационный файл директиву `chroot_local_user=YES`.

В этом случае имена пользователей, перечисленные в файле `/etc/vsftpd/chroot_list` (при условии, что у строк, указанных выше, удалены знаки комментария), имеют противоположное действие.

Для них не используется изолированная среда выполнения, и перемещение по файловой иерархии не ограничивается домашним каталогом.

Чтобы запретить анонимный доступ к FTP-серверу, нужно поставить знак комментария в начале строки `anonymous_enable=YES` в конфигурационном файле.

17.14.3.3. Дополнительные сведения о настройке сервера

Сервер `vsftpd` способен осуществлять всю передачу данных в пассивном режиме, что сопряжено со значительно меньшим риском.

Чтобы разрешить использование только пассивного режима, достаточно удалить символ комментария у директивы `port_enable=NO` в конфигурационном файле.

Чтобы разрешить запись файлов на сервер, следует удалить знак комментария у директивы `write_enable=YES`. Этого достаточно для того, чтобы пользователи, зарегистрированные локально, получили возможность загружать файлы в те каталоги, для которых они располагают правами на запись.

Чтобы разрешить запись файлов анонимным пользователям, нужно, кроме этого, удалить знак комментария у строки `anon_upload_enable=YES`. Специальный

непривилегированный пользователь, используемый для работы с анонимными клиентами, должен иметь права на запись в один или несколько каталогов, доступных таким клиентам.

Параметры использования vsftpd (в том числе относящиеся к безопасности) могут быть заданы при помощи xinetd.

Этот сервер позволяет ограничить количество одновременно выполняемых процессов, как по системе в целом, так и для каждого отдельного пользователя; указать пользователя, от имени которого будет выполняться служба; задать приоритет процесса (nice); указать адреса, с которых разрешено подключение к данной службе, а также время доступа и множество других параметров.

17.14.3.4. Утилита lftp

В ОС Альт СП передача файлов обеспечивается с помощью программы lftp. Данная команда реализует протокол передачи файлов FTP. Для копирования файлов нужно знать имя и пароль пользователя, которому принадлежат файлы на сервере службы FTP.

Для запуска lftp нужно в консоли ввести команду:

```
lftp
```

После появления приглашения lftp :~> становятся доступными для использования внутренние команды lftp.

Основные внутренние команды lftp:

- open – подключение к серверу;
- user – идентификация при удаленном подключении;
- close – отключение от сервера;
- ls – просмотр списка файлов;
- lcd – смена локального каталога;
- mkdir – создание нового каталога;
- lpwd – просмотр имени каталога на локальном компьютере;
- get – копирование файла с сервера;
- put – копирование файла на сервер;
- help – просмотр списка доступных команд и справки по ним;
- exit – выход из lftp.

17.14.3.5. Пример настройки FTP-сервера

Примечание. Настроить FTP-сервер можно также в ЦУС (подробнее см. п. 8.7.11).

Настроить параметры конфигурации xinetd для vsftpd в файле /etc/xinetd.d/vsftpd:

```
# default: off
# description: The vsftpd FTP server.
service ftp
{
    disable = no # включить службу
    socket_type = stream
    protocol = tcp
    wait = no
    user = root
    nice = 10
    rlimit_as = 200M # лимит адресного пространства
    server = /usr/sbin/vsftpd # путь к исполняемому файлу
    # only_from = 192.168.0.0 # доступ из всей подсети
    # доступ с указанных адресов
    # only_from = 207.46.197.100 207.46.197.101
    only_from = 0.0.0.0 # неограниченный по адресам доступ
    access_times = 2:00-9:00 12:00-24:00 # время, доступа
}
```

Перезапустить xinetd:

```
# systemctl restart xinetd
```

Изменить настройку прав доступа в файле /etc/vsftpd/conf:

```
local_enable=YES
chroot_local_user=YES
local_root=/var/ftp/
```

Убедиться в нормальной работе FTP-сервера:

```
# netstat -ant | grep 21
tcp        0      0 0.0.0.0:21          0.0.0.0:*          LISTEN
```

FTP-сервер запущен и принимает соединения на 21 порту.

Обратитесь к серверу по протоколу FTP:

```
$ lftp user@localhost
Пароль:
lftp user@localhost:~>
```

Примечание. Пакет lftp должен быть заранее установлен. Соединение на сервере по протоколу FTP успешно установлено.

17.14.3.6. Подключение рабочей станции

Примечание. На рабочей станции должен быть установлен пакет `lftp`:

```
# apt-get install lftp
```

Для создания подключения по протоколу FTP в консоли, на рабочей станции нужно выполнить команду:

```
$ lftp user@192.168.0.193
Пароль:
lftp user@192.168.0.193:~> lpwd
/home/user
lftp user@192.168.0.193:~>
```

Для создания подключения по протоколу FTP в графической среде МАТЕ можно запустить файловый менеджер, указать в адресной строке протокол и адрес сервера (рис. 540) и нажать клавишу `<Enter>`.

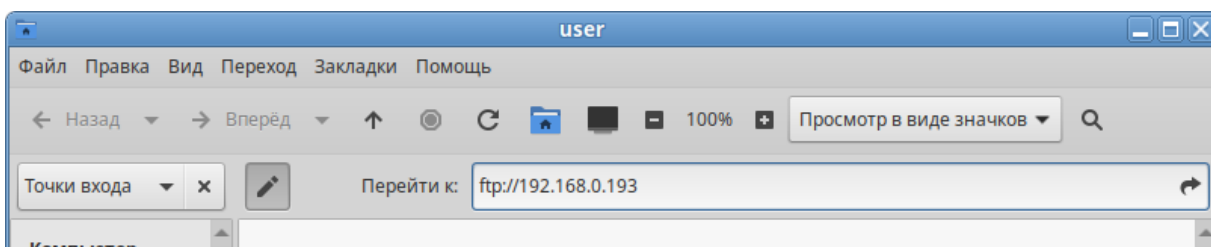


Рис. 540 – Создание подключения по протоколу FTP

В появившемся окне выбрать пункт «Зарегистрированный пользователь», указать имя пользователя, пароль и нажать кнопку «Подключиться» (рис. 541).

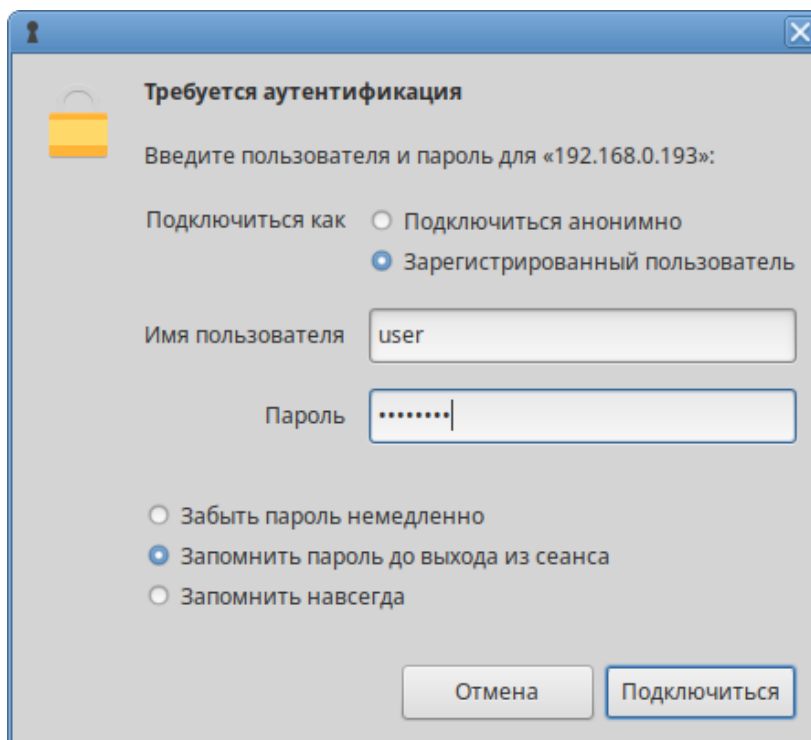


Рис. 541 – Параметры подключения к FTP-серверу

В результате должен отобразиться список файлов каталога `/var/ftp/`, расположенного на сервере FTP (рис. 542).

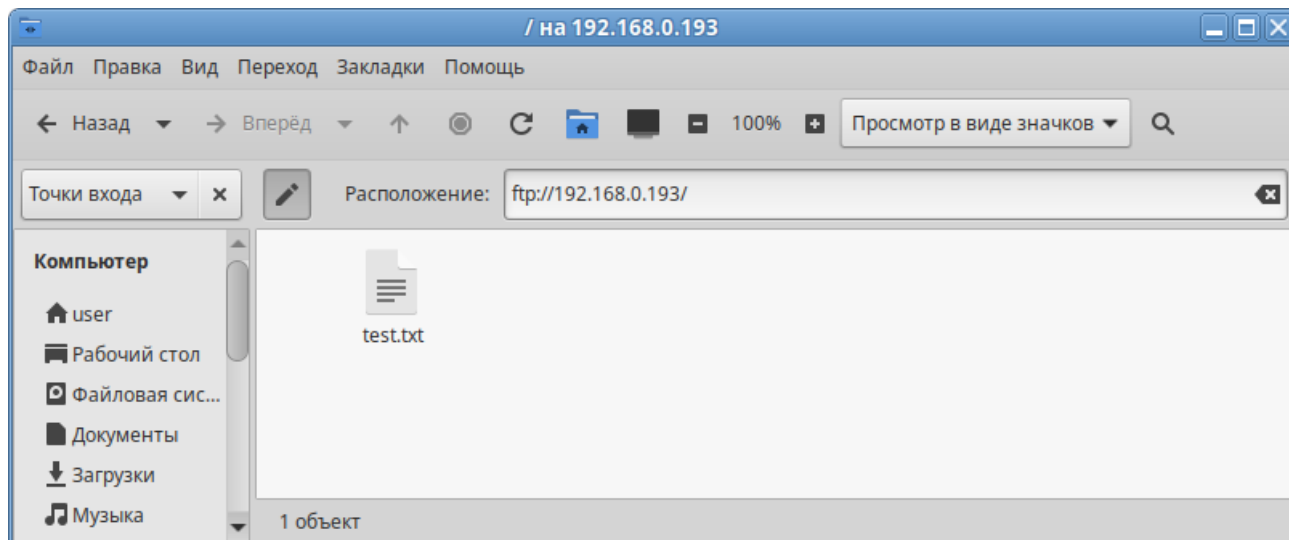


Рис. 542 – Файл на FTP-сервере

17.14.4. NTP

17.14.4.1. Настройка сервера NTP

В качестве NTP-сервера/клиента используется сервер времени chrony:

- chronyd – демон, работающий в фоновом режиме. Он получает информацию о разнице системных часов и часов внешнего сервера времени и корректирует локальное время. Демон реализует протокол NTP и может выступать в качестве клиента или сервера;
- chronyc – утилита командной строки для контроля и мониторинга программы. Утилита используется для тонкой настройки различных параметров демона, например, позволяет добавлять или удалять серверы времени.

Выполнить настройку NTP-сервера можно следующими способами:

- 1) в ЦУС настроить модуль «Дата и время» на получение точного времени с NTP-сервера (см. п. 8.7.7);
- 2) указать серверы NTP в директиве server или pool в файле конфигурации NTP /etc/chrony.conf:

```
allow all #Разрешить NTP-клиенту доступ из локальной сети
pool pool.ntp.org iburst #параметр iburst используется для
ускорения начальной синхронизации
```

- 3) и перезапустить сервис командой:

```
# systemctl restart chronyd
```

Убедиться в нормальной работе NTP-сервера, выполнив команду:

```
# systemctl status chronyd.service
```

17.14.4.2. Настройка рабочей станции

Настроить в ЦУС модуль «Дата и время» на получение точного времени с NTP-сервера (в качестве NTP-сервера указать IP-адрес сервера NTP) и нажать на кнопку «Применить» (рис. 543).

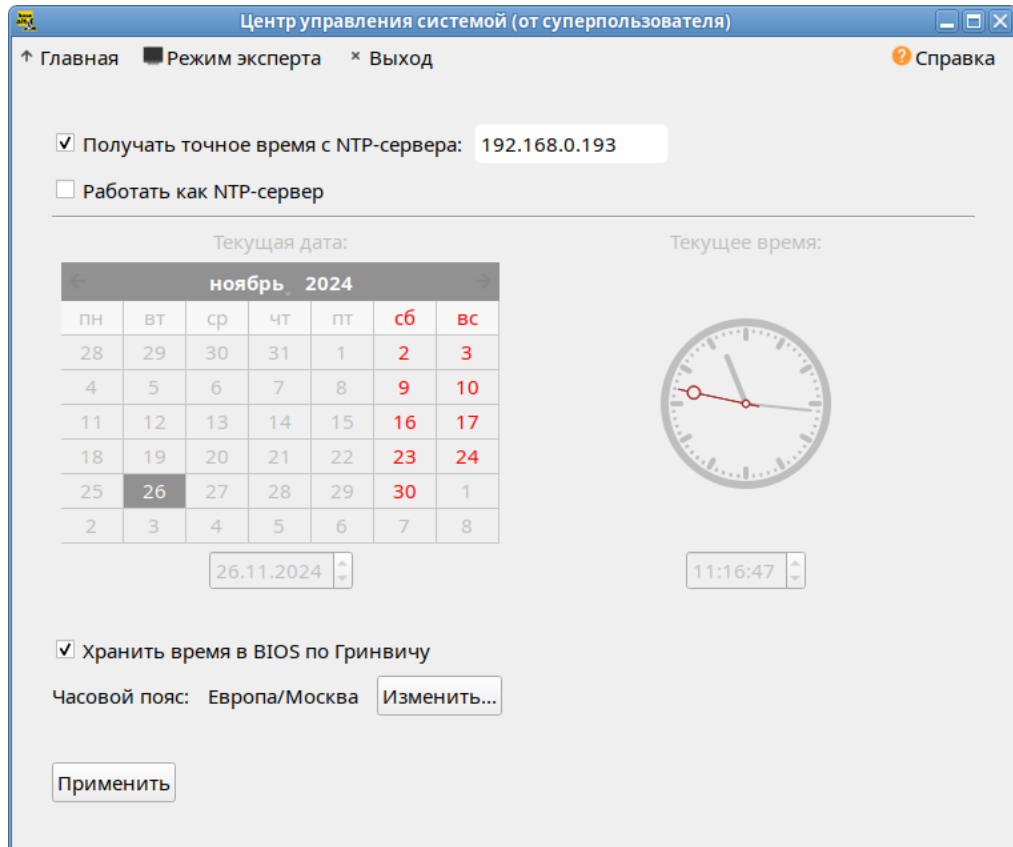


Рис. 543 – Настройка модуля «Дата и время» на рабочей станции

Проверить текущие источники времени:

```
$ chronyc sources
```

```
MS Name/IP address     Stratum Poll Reach LastRx Last sample
=====
^? 192.168.0.193         0   6     0    -      +0ns[  +0ns] +/-  0ns
```

Проверить статус источников NTP:

```
$ chronyc activity
```

```
200 OK
1 sources online
0 sources offline
0 sources doing burst (return to online)
0 sources doing burst (return to offline)
0 sources with unknown address
```

17.14.5. HTTP(S)

17.14.5.1. Настройка HTTP-сервера

Установить пакет apache2-base:

```
# apt-get install apache2-base
```

Запустить httpd2:

```
# systemctl start httpd2
```

Убедиться, что служба httpd2 запущена:

```
# systemctl status httpd2
```

Создать стартовую страницу для веб-сервера:

```
# echo "Hello, World" >/var/www/html/index.html
```

17.14.5.2. Проверка настройки на рабочей станции

Запустить веб-браузер, перейти по адресу `http://<IP-сервера>:>` (рис. 544).

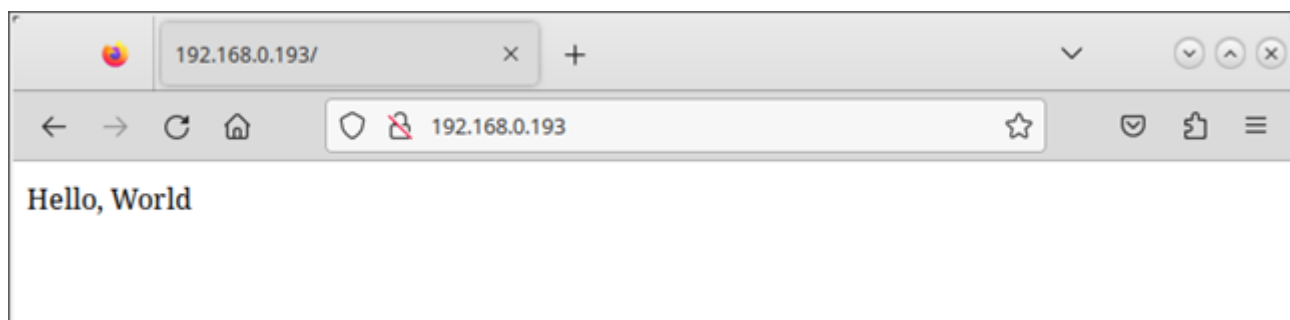


Рис. 544 – Обращение к серверу и получение данных по протоколу http

Можно также выполнить команду:

```
$ curl http://192.168.0.193  
Hello, World
```

Происходит обращение к серверу и получение данных по протоколу http.

17.15. Управление печатью

В ОС Альт СП используется система печати CUPS, которая позволяет выполнять следующие действия:

- управляет заданиями на печать;
- исполняет административные команды;
- предоставляет информацию о состоянии принтеров локальным и удаленным программам;
- информирует пользователей, если это требуется.

Система печати CUPS решает задачу монопольной постановки задания в очередь на печать. Данная функция предполагает невозможность вывода документа на печать в обход системы печати.

Существует два способа настройки принтера:

- утилита «Настройка принтера» (пакет `system-config-printer`);
- веб-интерфейс CUPS (Common UNIX Printing System) (пакет `cups`).

17.15.1. Устройство CUPS

В состав файлов конфигурации CUPS входят следующие файлы:

- файл конфигурации сервера CUPS (`/etc/cups/cupsd.conf`);
- файлы определения принтеров и классов (`/etc/cups/printers.conf`, `/etc/cups/classes.conf`);
- файлы типа MIME и файлы правил преобразования;
- файлы описания PostScript-принтеров (PPD).

17.15.1.1. Файл конфигурации сервера CUPS

Конфигурационный файл сервера очень похож на файлы конфигурации веб-сервера и определяет все свойства управления доступом. Настраивать CUPS можно либо непосредственно редактируя файл конфигурации `/etc/cups/cupsd.conf`, либо в веб-интерфейсе CUPS (рис. 545).

Веб-интерфейс CUPS можно запустить следующими способами:

- в графической среде MATE: выбрать на панели инструментов MATE «Меню» → «Приложения» → «Системные» → «Настройка печати»;
- в веб-браузере: `http://localhost:631`.

Если файл `cupsd.conf` редактируется в консоли для применения изменений, нужно перезапустить службу `cups`, выполнив команду:

```
# systemctl restart cups
```

Если файл `cupsd.conf` редактируется в веб-интерфейсе, то служба `cups` автоматически перезапускается после нажатия на кнопку «Сохранить изменения».

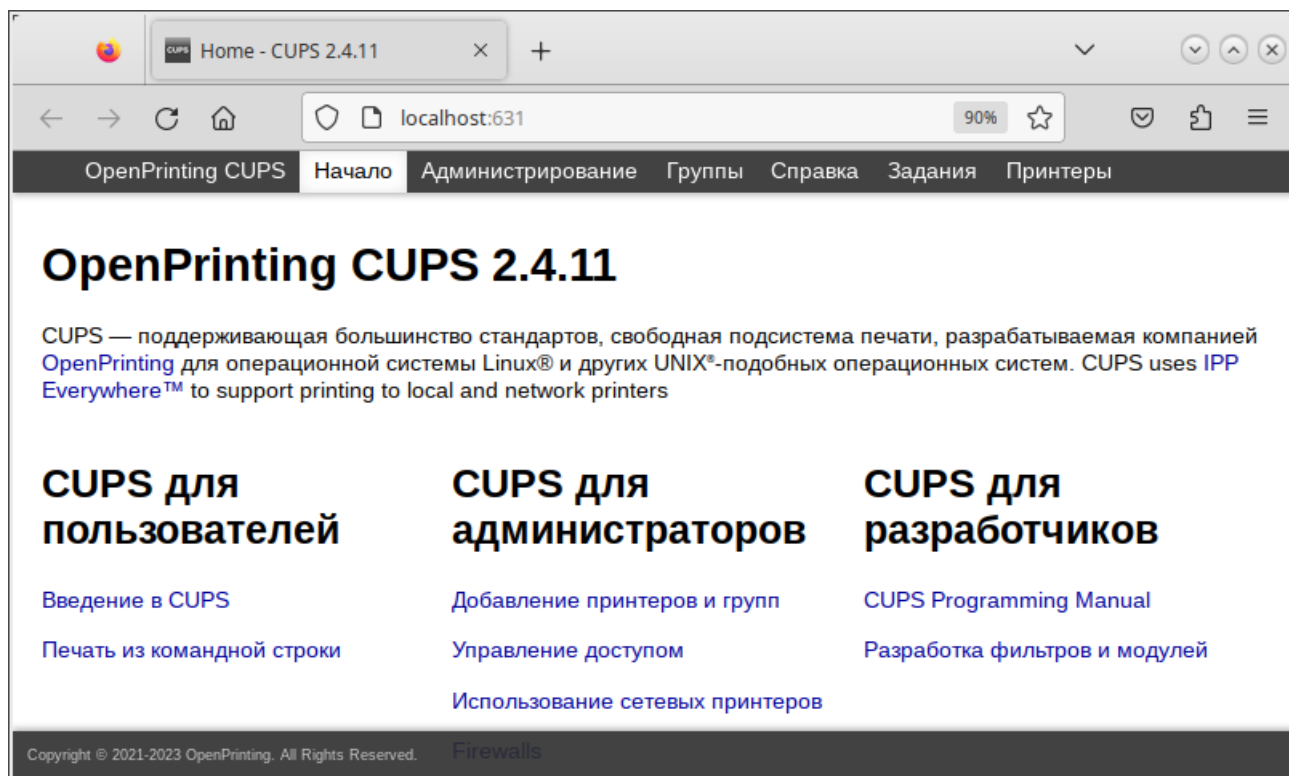


Рис. 545 – Веб-интерфейс CUPS

Файл конфигурации `cupsd.conf` начинается с ряда глобальных директив, которые оформлены в виде пар имя – значение.

`LogLevel` указывает подробность журналирования. Доступные значения: `none` (не записывать логи), `emerg`, `alert`, `crit`, `error`, `warn` (по умолчанию), `notice`, `info`, `debug`, `debug2` (подробный вывод).

`PageLogFormat` определяет формат строк журнала печати (файл `/var/log/cups/page_log`). Последовательности, начинающиеся со знака процента (%), заменяются соответствующей информацией:

- % {name} – значение указанного атрибута IPP;
- % C – количество копий для текущей страницы;
- % P – номер текущей страницы;
- % T – текущую дату и время в общий формат журнала;
- % j – идентификатор задания;
- % p – имя принтера;
- % u – имя пользователя.

По умолчанию строка `PageLogFormat` пустая (журнал печати не пишется). Для ведения журнала печати можно изменить эту строку:

```
PageLogFormat "%p %u %j %T %P %C %{job-billing}
%{job-originating-host-name} %{job-name} %{media} %{sides}"
```

`MaxLogSize` задает максимальный размер журналов до их ротации. Значение 0 отключает ротацию.

`Listen` позволяет указать, на каком IP-адресе будет доступен веб-интерфейс (по умолчанию `localhost:631`), а также прослушиваемый сокет.

Параметры `Browsing` задают настройки возможности CUPS обнаруживать принтеры в сети. Данная возможность поддерживается на уровне протокола IPP. Обнаружение происходит посредством широковещательных рассылок, что при большом количестве серверов CUPS или при частом отключении/подключении принтеров может породить дополнительную нагрузку на сеть. `Browsing` — указывает CUPS предоставлять свои серверы в общий доступ, либо нет. Значения может принимать `Yes` или `No` соответственно.

Директива `DefaultAuthType` указывает механизм аутентификации, который будет использоваться для организации доступа (по умолчанию `Basic` — использовать логины/пароли от локальной системы).

`BrowseAllow` и `BrowseDeny` — указывают CUPS на стороне клиента адреса, от которых может приниматься или отвергаться, соответственно, информация о принтерах. Формат директив соответствует директивам `Allow` и `Deny`. В качестве аргумента для данной директивы может быть, как отдельный IP, так и подсеть в формате `10.0.0.0/24` или `10.0.0.0/255.255.255.0` или `10.0.0.0-10.0.0.255`, так и значение `@LOCAL` — обозначающее локальную сеть, а также имена хостов. Возможно использование нескольких данных директив.

Директива `Order` определяет порядок предоставления доступа к CUPS по умолчанию. Значение `allow,deny` определяет что доступ запрещен, если право на доступ не указано явно. Если директива имеет значение `deny,allow`, то доступ будет разрешен, если явно не запрещен.

Далее идут параметры, сгруппированные в разделы `<Location /...>`. Такие директивы определяют доступ к определенным функциям сервера:

- `<Location />` – доступ к серверу;
- `<Location /admin>` – доступ к странице администрирования;
- `<Location /admin/conf>` – доступ к конфигурационным файлам;
- `<Location /jobs>` – доступ к заданиям;
- `<Location /printer>` – доступ к принтерам.

17.15.1.2. Управление политиками операций

Политики операций – это правила, используемые для каждой операции IPP в CUPS. Правила могут включать такие опции, как «пользователь должен предоставить пароль», «пользователь должен находиться в системной группе», «разрешать только из локальной системы» и т. д.

CUPS позволяет полностью переопределить правила для каждой операции и (или) принтера. Каждая политика имеет название и определяет правила контроля доступа для каждой операции IPP.

Политики операций используются для всех запросов IPP, отправленных в планировщик заданий, и оцениваются после правил управления доступом на основе местоположения. Таким образом, политики операций могут только добавлять дополнительные ограничения безопасности к запросу, а не ослаблять их. Для ограничений на уровне сервера нужно использовать правила управления доступом на основе местоположения, а для ограничений на отдельные принтеры, задачи или службы – политики операций.

Политики хранятся в файле `cupsd.conf` в разделах `Policy`. Каждая политика имеет название, которое используется для ее выбора. Внутри раздела политики находятся один или несколько подразделов `Limit`, в которых перечислены операции, на которые влияют правила внутри него.

Каждая политика имеет название. В названии политики можно использовать те же символы, что и в названии принтера, в частности все печатные символы, кроме пробела, слэша (/) и решетки (#).

В разделах < Limit ...> определяется, какие ограничения должна содержать политика. Директивы внутри подраздела Limit могут использовать любую из директив ограничения: Allow, AuthType, Deny, Encryption, Require и Satisfy. В таблице 103 перечислены основные примеры для разных правил контроля доступа.

Т а б л и ц а 103 – Правила контроля доступа

Уровень доступа	Директива
Разрешить всем	Order allow,deny Allow from all
Разрешить всем в локальной сети	Order allow,deny Allow from @LOCAL
Запретить всем/Отклонить операции	Order allow,deny
Требовать аутентификацию пользователя (Логин, Пароль)	AuthType Basic
Требовать CUPS аутентификацию CUPS (lppasswd) Password	AuthType BasicDigest
Требовать Kerberos	AuthType Negotiate
Только владелец	Require user @OWNER
Только администратор	Require user @SYSTEM
Члены группы foogroup	Require user @foogroup
Пользователи test или test1	Require user test test1
Требовать шифрование	Encryption Required

Пример политики, которая разрешает доступ только из подсети 10.110.1.x:

```
<Policy mypolicy>
# Операции, связанные с заданиями доступны только владельцам
# членам группы lab999 и администратору...
  <Limit Send-Document Send-URI Hold-Job Release-Job Restart-Job
Purge-Jobs      Set-Job-Attributes      Create-Job-Subscription      Renew-
Subscription    Cancel-Subscription    Get-Notifications    Reprocess-Job
Cancel-Current-Job  Suspend-Current-Job  Resume-Job      Cancel-My-Jobs
Close-Job CUPS-Move-Job>
    Require user @OWNER @lab999 @SYSTEM
    Order allow,deny
    Allow from 10.110.1.0/24
  </Limit>

# Все административные операции доступны только администратору
и членам группы lab999, также необходима процедура аутентификации...
  <Limit Pause-Printer Resume-Printer Set-Printer-Attributes
Enable-Printer      Disable-Printer      Pause-Printer-After-Current-Job
Hold-New-Jobs Release- Held-New-Jobs  Deactivate-Printer  Activate-
Printer Restart-Printer Shutdown-Printer Startup-Printer Promote-Job
Schedule-Job-After CUPS- Accept-Jobs CUPS-Reject-Jobs CUPS-Set-Default>
```

```

AuthType Default
Require user @lab999 @SYSTEM
Order allow,deny
Allow from 10.110.1.0/24
</Limit>

```

Все остальные операции доступны из подсети 10.110.1.0/24 с обязательной аутентификацией пользователей...

```

<Limit All>
AuthType Default
Order allow,deny
Allow from 10.110.1.0/24
</Limit>

```

```
</Policy>
```

После создания политики ее можно использовать двумя способами.

Первый способ – назначить ее в качестве политики по умолчанию для всей системы, используя директиву `DefaultPolicy` в файле `cupsd.conf`. Например:

```
DefaultPolicy mypolicy
```

Второй способ – связать политику с одним или несколькими принтерами. Для этого можно воспользоваться командой `lpadmin` (8) или веб-интерфейсом для изменения политики операций для каждого принтера. Например:

```
# lpadmin -p HP_LaserJet_M1536dnf_MFP -o printer-op-policy=mypolicy
```

17.15.1.3. Файлы описания принтеров и классов

Файлы описания принтеров и классов перечисляют доступные очереди печати и классы. Классы принтеров – наборы принтеров. Задания, посланные классу принтеров, направляются к первому доступному принтеру данного класса. Для редактирования файлов `/etc/cups/printers.conf` и `/etc/cups/classes.conf` можно использовать утилиту `lpadmin`.

Пример настройки для локального принтера:

```

<DefaultPrinter laserjet>
UUID urn:uuid:7efaaede-819d-3d9a-6270-3fe957597756
Info laserjet
Location host-15.localdomain
MakeModel HP LaserJet m1537dnf MFP pcl3, hpcups 3.19.1
DeviceURI
usb://HP/LaserJet%20M1536dnf%20MFP?serial=00CND9D8YC9C&interface=1
State Idle
StateTime 1553167952
ConfigTime 1553167952

```

```
Type 36892
Accepting Yes # принтер принимает задания
Shared Yes
JobSheets none none
QuotaPeriod 0
PageLimit 0
KLimit 0
OpPolicy default
ErrorPolicy stop-printer # остановить принтер при ошибке
Option job-hold-until indefinite
</DefaultPrinter>
```

17.15.1.4. Очередь печати

Очередь печати – механизм, который позволяет буферизовать и организовать задания, посылаемые на принтер. Необходимость организации такого механизма обуславливается тем, что принтер является медленно действующим устройством, и задания не могут быть распечатаны мгновенно.

Очевидно, что в многопользовательской среде возникает конкуренция со стороны пользователей при доступе к принтерам, поэтому задания нужно располагать в очереди. Для этого используется буферный каталог `/var/spool/cups/`.

Файлы типов MIME перечисляют поддерживаемые MIME-типы (`text/plain`, `application/postscript`) и правила для автоматического обнаружения формата файла. Они используются сервером для определения поля `Content-Type` для GET- и HEAD-запросов и обработчиком запросов протоколов сетевой печати IPP (Internet Printing Protocol), чтобы определить тип файла.

Правила преобразования MIME перечисляют доступные фильтры. Фильтры используются, когда задание направляется на печать, таким образом, приложение может послать файл удобного (для него) формата системе печати, которая затем преобразует документ в требуемый печатный формат. Каждый фильтр имеет относительную «стоимость», связанную с ним, и алгоритм фильтрования выбирает набор фильтров, который преобразует файл в требуемый формат с наименьшей общей «стоимостью».

Файлы PPD описывают возможности всех типов принтеров. Для каждого принтера имеется один PPD-файл. Файлы PPD для не-PostScript-принтеров определяют дополнительные фильтры посредством атрибута `cupsFilter` для поддержки драйверов принтеров.

В ОС стандартным языком описания страниц является язык PostScript. Большинство прикладных программ (редакторы, веб-браузеры) генерируют программы печати на этом языке.

Когда нужно напечатать ASCII-текст, программа печати может быть ASCII-текстом. Имеется возможность управления размером шрифтов при печати ASCII-текста.

Управляющая информация используется для контроля доступа пользователя к принтеру и аудита печати. Также имеется возможность печати изображений в форматах GIF, JPEG, PNG, TIFF и документов в формате PDF.

Фильтр – программа, которая читает из стандартного входного потока или из файла, если указано его имя. Все фильтры поддерживают общий набор опций, включающий имя принтера, идентификатор задания, имя пользователя, имя задания, число копий и опции задания. Весь вывод направляется в стандартный выходной поток.

Фильтры предоставлены для многих форматов файлов и включают, в частности, фильтры файлов изображения и растровые фильтры PostScript, которые поддерживают принтеры, не относящиеся к типу PostScript. Иногда несколько фильтров запускаются параллельно для получения требуемого формата на выходе.

Программа `backend` – это специальный фильтр, который отправляет печатаемые данные устройству или через сетевое соединение. В состав системы печати включены фильтры для поддержки устройств, подключаемых с помощью параллельного и последовательного интерфейсов, а также шины USB.

Клиентские программы используются для управления заданиями и сервером печати.

Управление заданиями включает выполнение следующих действий:

- формирование;

- передачу серверу печати;
- мониторинг и управление заданиями в очереди на печать.

Управление сервером включает выполнение следующих действий:

- запуск/остановку сервера печати;
- запрещение/разрешение постановки заданий в очередь;
- запрещение/разрешение вывода заданий на принтер.

Основные пользовательские настройки содержатся в файлах конфигурации

`client.conf` и `~/.cups/lpoptions`.

Для удаленного использования сервера печати нужно от имени пользователя с идентификатором `root` выполнить следующие команды:

```
cupscctl --remote-admin --remote-printers --remote-any  
cupscctl ServerAlias=*
```

В случае использования сервера печати в едином пользовательском пространстве (далее – ЕПП) нужно задание соответствующего типа аутентификации: для работы в ЕПП значение параметра должно быть `DefaultAuthType Negotiate`, без использования ЕПП значение параметра должно быть `DefaultAuthType Basic`.

В файле конфигурации клиента `client.conf` должен быть задан один параметр `ServerName`, определяющий имя сервера печати, например:

```
ServerName computer.domain
```

В общем случае вывод данных на принтер происходит следующим образом:

- 1) программа формирует запрос на печать задания к серверу печати;
- 2) сервер печати принимает подлежащие печати данные, формирует в буферном каталоге файлы с содержимым задания и файлы описания задания, при этом задание попадает в соответствующую очередь печати;
- 3) сервер печати просматривает очереди печати для незанятых принтеров, находит в них задания и запускает конвейер процессов, состоящий из фильтров и заканчивающийся выходным буфером, информация из которого поступает в принтер посредством драйверов ОС;
- 4) контроль и мониторинг процесса печати выполняется с помощью программ `lpq`, `lpc`, `lprm`, `lpstat`, `lpmove`, `cancel`.

17.15.2. Установка принтера

Перед началом установки нужно убедиться в том, что в случае локального подключения принтер присоединен к соответствующему порту компьютера и включен, а в случае сетевого подключения принтер корректно сконфигурирован для работы в сети.

Окно «Настройки принтера» можно запустить следующими способами:

- в графической среде: выбрать на панели инструментов МАТЕ «Меню» → «Приложения» → «Администрирование» → «Параметры печати»;
- из командной строки: командой `system-config-printer`.

Примечание. Если возникает ошибка «Служба печати недоступна», следует нажать кнопку «Запустить службу». Потребуется ввести пароль пользователя root.

Можно также в терминале от имени системного администратора root выполнить команду:

```
# systemctl restart cups
```

После этого следует вернуться к окну «Настройки принтера» и нажать на кнопку «Обновить».

Для добавления принтера в диалоговом окне «Настройки принтера» нужно нажать кнопку «Добавить» (рис. 546).

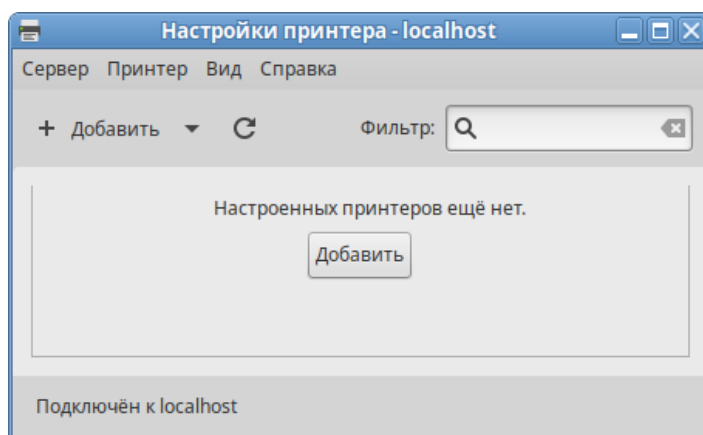


Рис. 546 – Настройки принтера

Далее в открывшемся окне нужно нажать на кнопку «Добавить» и выбрать принтер, который нужно подключить и нажать на кнопку «Далее» (рис. 547).

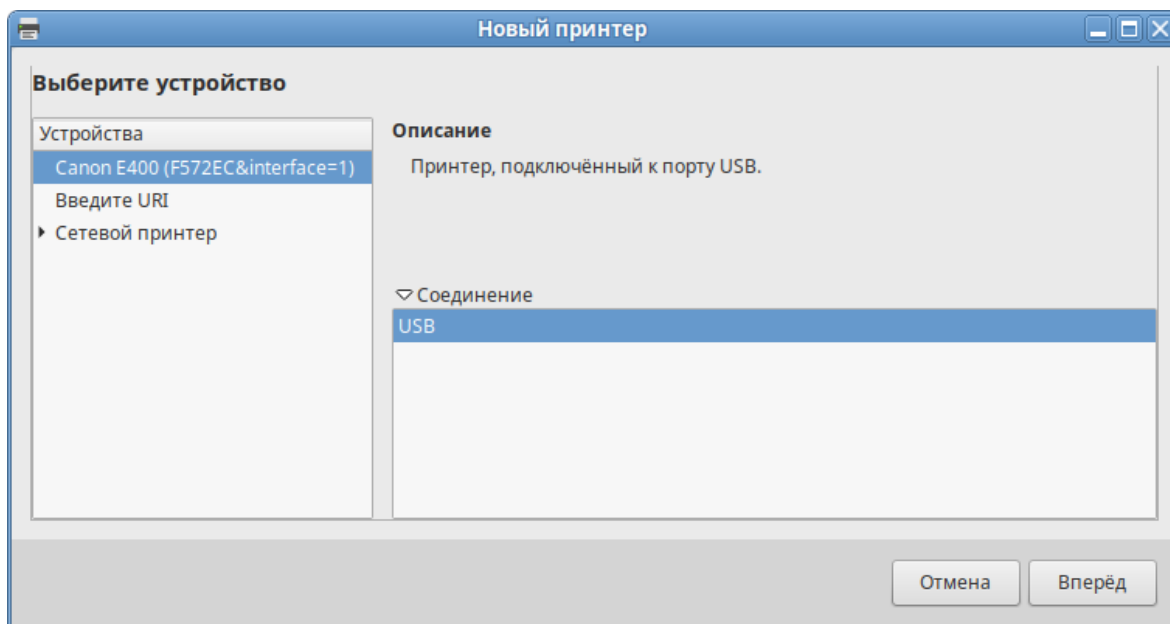


Рис. 547 – Выбор принтера

На следующих шагах настройки принтера нужно выбрать драйвер для принтера. Драйвер можно выбрать из базы данных, содержащей различные файлы описания принтеров (PPD-файлы) от производителей или предоставить файл описания PostScript-принтера (рис. 548).

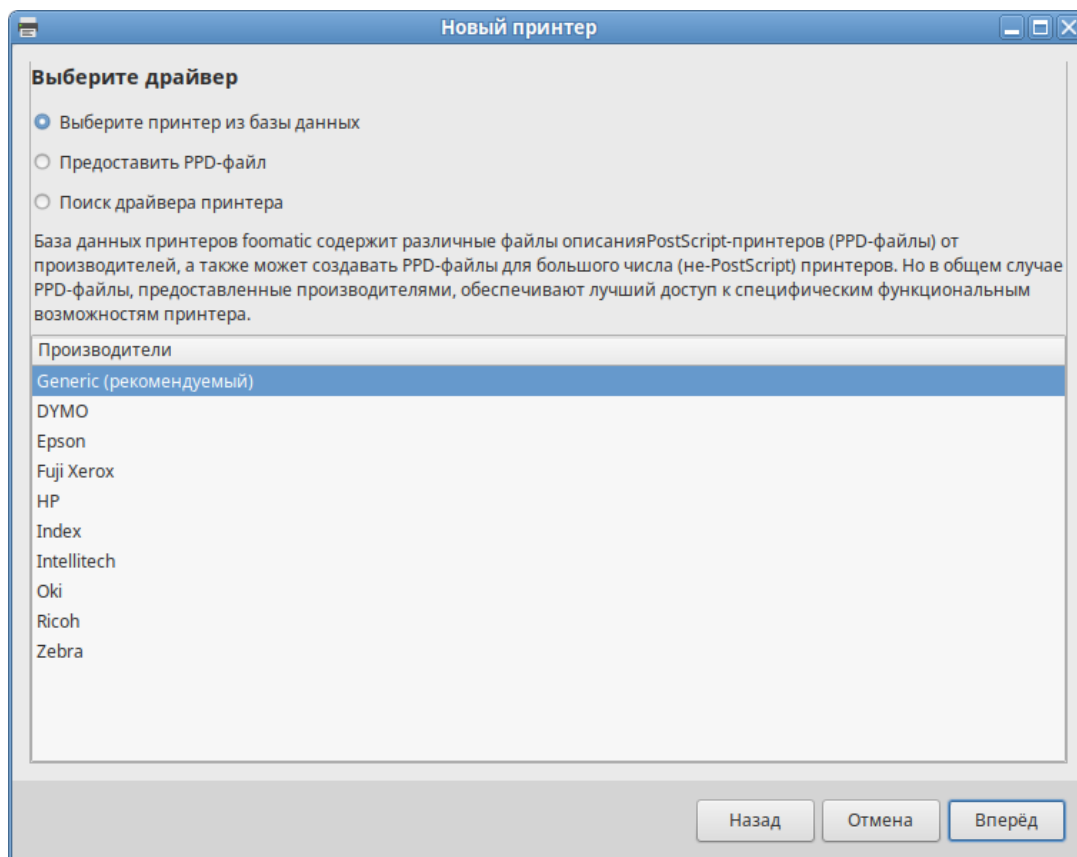


Рис. 548 – Выбор источника драйвера принтера

После выбора драйвера в окне «Новый принтер» можно изменить название и описание принтера (рис. 549).

После нажатия кнопки «Применить» установка принтера завершена, принтер станет доступным для печати (рис. 550).

Изменить настройки принтера (разрешение, размер используемой по умолчанию бумаги, принтер по умолчанию и т. д.) можно в любой момент, выбрав в контекстном меню принтера пункт «Свойства».

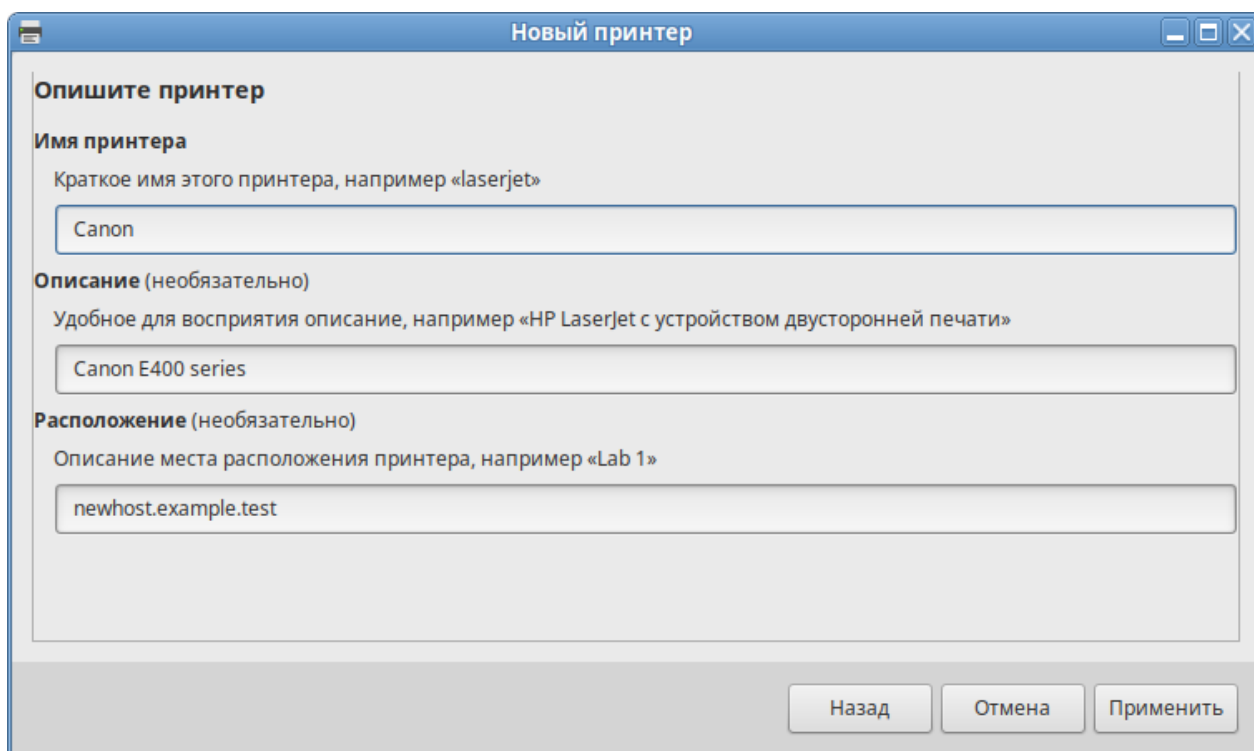


Рис. 549 – Название и описание принтера

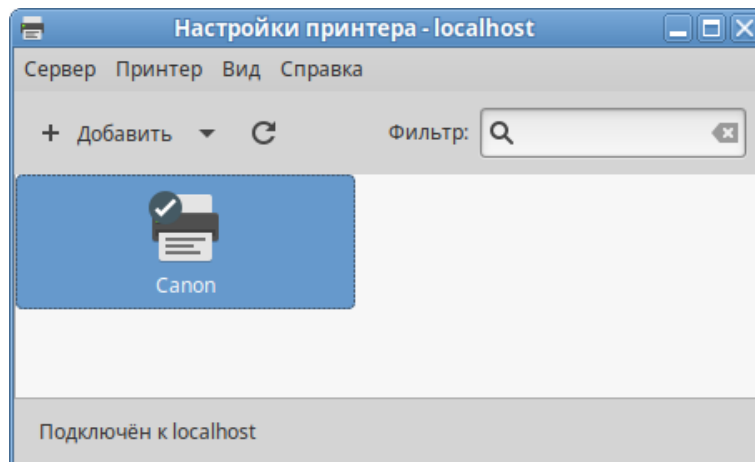


Рис. 550 – Выбор принтера

17.15.3. Настройка сервера печати для сети

Если в сети имеются несколько принтеров или, когда принтеры не подключены непосредственно к тому компьютеру, на котором работает главный сервер CUPS, то целесообразно настроить сервер cupsd, так, чтобы он мог принимать задания на печать из сети.

По умолчанию сервер CUPS работает с локально установленными принтерами, для того, чтобы он мог обрабатывать задания из сети, в конфигурационный файл `/etc/cups/cupsd.conf` нужно внести следующие изменения:

- разрешить доступ к серверу – добавить в секцию Location директиву

```
Allow from:
<Location />
    Order allow,deny
    Allow localhost
    Allow from ip-address/netmask
</Location>
```

- включить отображение (обнаружение) общего принтера:

```
Browsing On
BrowseOrder allow,deny
BrowseAllow 192.168.1.* #локальная сеть
BrowseAddress 192.168.1.*:631#локальная сеть
```

Примечание. Включить отображение (обнаружение) общего принтера можно также отметив пункт «Разрешить совместный доступ к принтерам, подключенным к этой системе» в веб-интерфейсе на вкладке «Администрирование».

После внесения изменений нужно перезапустить службу cups:

```
# systemctl restart cups
```

На клиентах также должен быть установлен CUPS. После установки системы печати на клиенте, CUPS-принтеры, присутствующие в сети, автоматически находятся менеджерами принтеров. В качестве альтернативы, можно воспользоваться веб-интерфейсом CUPS на клиентской машине по адресу `http://localhost:631`. Если принтер не был обнаружен автоматически, введите IPP или HTTP-адрес (URI) сетевого CUPS принтера:

```
ipp://server-name-or-ip/printers/printername
или
http://server-name-or-ip:631/printers/printername
```

Если CUPS клиент не находит в сети принтеры, доступные через сервер CUPS, то иногда может помочь создание или изменение файла `/usr/local/etc/cups/client.conf` с добавлением записи, подобной следующей:

```
ServerName server-ip
```

В этом случае `server-ip` нужно заменить на IP-адрес сервера CUPS в сети.

17.15.4. Команды управления печатью

При печати через локальный сервер печати данные сначала формируются на локальном сервере, как для любой другой задачи печати, после чего посылаются на принтер, подключенный к данному компьютеру.

Вся информация, которая требуется для драйвера принтера (используемое физическое устройство, удаленный компьютер и принтер для удаленной печати), содержится в файлах `/etc/cups/printers.conf` и `/etc/cups/ppd/<имя_очереди>.ppd`.

Примечание. Далее термин «принтер» в этом разделе используется для обозначения принтера, соответствующего одной записи в файле `/etc/cups/printers.conf`. Под термином «физический принтер» подразумевается устройство, с помощью которого производится печать на бумаге. В файле `/etc/cups/printers.conf` может быть несколько записей, описывающих один физический принтер различными способами.

В системе печати CUPS приняты следующие команды для управления печатью:

- `/usr/bin/lpr` – постановка заданий в очередь, совместима с командой `lpr` системы печати BSD UNIX;
- `/usr/bin/lp` – постановка заданий в очередь, совместима с командой `lp` системы печати System V UNIX;
- `/usr/bin/lpq` – просмотр очередей печати;
- `/usr/sbin/lpc` – управление принтером, является частичной реализацией команды `lpc` системы печати BSD UNIX;
- `/usr/bin/lprm` – отмена заданий, поставленных в очередь на печать;
- `/usr/sbin/cupsd` – сервер печати;
- `/usr/sbin/lpadmin` – настройка принтеров и классов принтеров;

- `/usr/sbin/lpmove` – перемещение задания в другую очередь;
- `/usr/bin/fly-admin-printer` – настройка системы печати, установка и настройка принтеров, управление заданиями.

CUPS предоставляет утилиты командной строки для отправления заданий и проверки состояния принтера. Команды `lpstat` и `lpc status` также показывают сетевые принтеры (принтер@сервер), когда разрешен обзор принтеров.

С помощью команды `lp` выполняется передача задачи принтеру, то есть задача ставится в очередь на печать. В результате выполнения этой команды файл передается серверу печати, который помещает его в каталог `/var/spool/cups/`.

Остановить работу сервиса печати можно с помощью команды:

```
# systemctl stop cups
```

Запустить сервис печати можно с помощью команды:

```
# systemctl start cups
```

17.15.4.1. Настройка принтера

Настроить принтер в ОС можно также с помощью команды `lpadmin`. Ее запуск с опцией `-p` выполняется для добавления или модификации принтера:

```
/usr/sbin/lpadmin -p printer [опции]
```

Для `lpadmin` существуют также опции по регулированию политики лимитов и ограничений по использованию принтеров и политики доступа к принтерам.

Для удаления принтера нужно выполнить `lpadmin` с опцией `-x`:

```
/usr/sbin/lpadmin -x printer
```

17.15.4.2. Проверка очереди печати

Команда `lpq` предназначена для проверки очереди печати (используемой `lpd`) и вывода состояния заданий на печать, указанных при помощи номера задания, либо системного идентификатора пользователя, которому принадлежит задание.

`lpq` выводит для каждого задания имя его владельца, текущий приоритет задания, номер задания и размер задания в байтах, без параметров выводит состояние всех заданий в очереди.

17.15.4.3. Удаление задания из очереди печати

Команда `lprm` предназначена для удаления задания из очереди печати. Для определения номера задания нужно использовать команду `lpq`. Для удаления задания нужно быть его владельцем или пользователем с идентификатором `root`.

Системные каталоги, определяющие работу системы печати ОС, также содержат файлы, которые не являются исполняемыми:

- `/etc/cups/printers.conf` – содержит описания принтеров в ОС;
- `/etc/cups/ppd/<имя_очереди>.ppd` – содержит описания возможностей принтера, которые используются при печати заданий и при настройке принтеров;
- `/var/log/cups/error_log` – содержит протокол работы принтера, в этом файле могут находиться сообщения об ошибках сервера печати или других программ системы печати;
- `/var/log/cups/access_log` – содержит все запросы к серверу печати;
- `/var/log/cups/page_log` – содержит сообщения, подтверждающие успешную обработку страниц задания фильтрами и принтером.

17.15.4.4. Настройка сетевого принтера из консоли

Для настройки принтера из консоли нужно выполнить следующие действия:

- 1) получить права администратора;
- 2) просмотреть содержимое каталога `model` на наличие драйверов:

```
ls /usr/share/cups/model
```

Примечание. Для работы с дополнительными драйверами доступных устройств установите пакет `printer-driver-splix`.

- 3) если драйвер устройства присутствует перейти к шагу 7) (настройка нового устройства);
- 4) найти нужное устройство:

```
lpinfo -m | grep название_модели
```

- 5) просмотреть данные о драйвере устройства:

```
foomatic-ppdfile -A | grep название_модели
```

6) сформировать файл .ppd:

```
foomatic-ppdfile -p `имя_ppd_драйвера` >
/usr/share/cups/model/имя_ppd_файла.ppd
```

7) произвести настройку нового устройства:

- если принтер подключен по сети:

```
lpadmin -p название_принтера -D еще_одно_название -m
название_ppd_файла.ppd -v socket://ip_принтера -E
```

- если принтер подключен по USB:

```
lpadmin -p название_принтера -D еще_одно_название -m
название_ppd_файла.ppd -v "usb://адрес_принтера" -E
```

8) печать документа:

```
lp -d название_принтера /путь_документ
```

Примечание. Список доступных устройств можно просмотреть, выполнив команду: `lpinfo -v`

Пример вывода:

```
usb://Samsung/M262x%20282x%20Series?serial=ZD1UBJCD5000LVW
```

Список установленных принтеров: `lpstat -p -d`

Пример настройки сетевого принтера Kyocera Ecosys P2235dn:

1) получить права администратора;

2) посмотреть содержимое каталога `/usr/share/cups/model` на наличие драйверов:

```
ls /usr/share/cups/model
```

3) если драйвер устройства присутствует произвести настройку нового устройства (перейти к шагу 7));

4) найти нужное устройство:

```
lpinfo -m | grep Kyocera-P-2
```

5) посмотреть данные о драйвере устройства:

```
foomatic-ppdfile -A | grep Kyocera-P-2
```

6) сформировать файл .ppd:

```
foomatic-ppdfile -p `Kyocera-P-2000` >
/usr/share/cups/model/Kyocera.ppd
```

7) создать новое устройство:

```
lpadmin -p Kyocera -D Kyocera-P-2000 -m Kyocera.ppd -v
socket://10.120.70.90 -E
```

17.16. Организация терминального доступа XRDP

Для организации и реализации терминального доступа для обработки информации в ОС Альт СП возможно использование XRDP (Remote Desktop Protocol). Программа предоставляет рабочий стол X, обеспечивает графический вход с использованием протокола удаленного рабочего стола RDP. XRDP поддерживает удаленное управление графикой, двустороннюю передачу буфера обмена, перенаправление звука, диска. Передача RDP шифруется с использованием TLS по умолчанию.

17.16.1. Базовая настройка сервера терминалов

Примечание. В настройках сети сервера должен быть указан способ получения IP-адреса: «Вручную», указаны статические настройки сети: IP-адрес, маска, шлюз.

Для настройки сервера терминалов нужно установить пакет `xrdp`:

```
# apt-get install xrdp
```

Включить и добавить в автозагрузку сервисы:

```
# systemctl enable --now xrdp xrdp-sesman
```

Рекомендуется отключить эффекты рабочего стола. Это можно сделать, установив пакет `mate-reduced-resource`.

При использовании в качестве сервера терминалов ОС Альт СП (вариант исполнения Сервер) в профиле установки будет отсутствовать графическая оболочка (о том, как установить графическую оболочку и переключиться в графический режим см. п. 5.8).

17.16.2. Настройка сервера

Параметры настройки сервера хранятся в файле `/etc/xrdp/sesman.ini`. Файл конфигурации содержит разделы:

- «Globals» – определяет некоторые глобальные параметры конфигурации;
- «Security» – определяет параметры безопасности;
- «Sessions» – определяет параметры подключения, управление сеансами;
- «Session» definitions – определяет поддерживаемые типы сеансов. Конфигурация каждого типа сеанса определяется как отдельный раздел по имени типа сеанса `Xorg`, `Xvnc`;

- «Logging» – определяет параметры подсистемы логирования;
- «Chansrv» – определяет параметры подключения диска, которые поддерживает RDP.

Некоторые настройки сервера, установленные по умолчанию:

- ListenPort=3389 – порт, который прослушивает xrdp-sesman (если настроен межсетевой экран нужно включить этот порт в разрешенные);
- TerminalServerUsers=tsusers – группа, в которую нужно добавить пользователей для организации доступа к серверу. Данная группа создается локально при установке сервера, если рассматривать доменную авторизацию, то нужно внести изменения в файл конфигурации `/etc/sss/sss.conf` и в настройках `sesman.ini` вместо локальной группы указать доменную;
- TerminalServerAdmins=tsadmins – группа, в которую нужно добавить пользователей для организации административного доступа к серверу;
- MaxLoginRetry=4 – максимальное количество попыток подключения;
- MaxSessions=50 – максимальное количество подключений к серверу;
- KillDisconnected=false – разрыв сеанса при отключении пользователя;
- AllowRootLogin=false (true/false) – управление авторизацией под учетной записью root;
- FuseMountName=thinclient_drivers – название монтируемого каталога.

Конфигурацию сервера возможно настроить в соответствии с требованиями безопасности.

17.16.3. Настройки доступа пользователей

Для доступа к терминальному сеансу пользователь должен быть включен в группу `tsusers`:

```
# gpasswd -a <пользователь> tsusers
```

Для разрешения монтирования папки пользователь должен быть включен в группу `fuse`:

```
# gpasswd -a <пользователь> fuse
```

17.16.4. Подключение звука

Для возможности прослушивания звука из терминального сеанса локально нужно установить на терминальный сервер пакет `pulseaudio-module-xrdp`:

```
# apt-get install pulseaudio-module-xrdp
```

17.16.5. Подключение USB-устройств

Для организации инфраструктуры перенаправления USB-устройств на сеанс сервера XRDP нужно установить пакет `xrdp-usb`, который состоит из двух пакетов:

- терминальный сервер – `xrdp-usb-session`;
- терминальный клиент – `xrdp-usb-terminal`.

Пакет `xrdp-usb-session` позволяет добавлять подключение разрешенных администратором USB-устройств с клиента.

Установка пакета `xrdp-usb-session` на сервер:

```
# apt-get install xrdp-usb-session
```

Перезапустить службу `xrdp-sesman`:

```
# systemctl restart xrdp-sesman.service
```

Выполнить настройку клиента:

1) установить пакет `xrdp-usb-terminal`:

```
# apt-get install xrdp-usb-terminal
```

2) добавить пользователя клиентского компьютера в группу `disk`:

```
# gpasswd -a <пользователь> disk
```

3) перезагрузить систему (чтобы загрузились все модули и запустилась служба `usbipd`);

4) убедиться, что служба `usbipd` запущена:

```
# systemctl status usbipd
```

5) подключить USB-устройства и просмотреть идентификаторы подключенных устройств:

```
# lsusb
```

```
Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 003: ID 090c:1000 Silicon Motion, Inc. - Taiwan
(formerly Feiya Technology Corp.) Flash Drive
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

- б) из полученного вывода выбрать ID устройства, которое нужно передать при подключении к терминальной сессии, скопировать нужный идентификатор и прописать его в файле `/etc/xrdp-usb`:

```
# Config file for xrdp-usb-terminal
# Add redirected usb ids one per line
# Example
#072f:90cc      # Advanced Card Systems, Ltd : ACR38 SmartCard
Reader (072f:90cc)
#072f:*        # All devices from specified vendor
090c:1000      # ID устройства
```

17.16.6. Настройка клиента для подключения к серверу терминалов

Примечание. Следует избегать одновременных сеансов RDP и обычных для одного и того же пользователя. Systemd не позволит полноценно работать в сеансе RDP.

Для подключения к серверу терминалов, на клиентском компьютере должен быть установлен клиент удаленного доступа. Для подключения к серверу терминалов можно использовать программы удаленного доступа FreeRDP, Remmina, Connector и т. д.

Перед подключением нужно на клиенте выполнить команду:

```
$ usbip-export
```

Для подключения можно использовать `xfreerdp` (должен быть установлен пакет `xfreerdp`):

```
$ xfreerdp [файл] [параметры] [/v:<сервер>[:порт]]
```

Описание некоторых параметров:

- `/v:<server>[:port]` – IP-адрес или имя сервера;
- `/u:<user>` – пользователь;
- `/p:<password>` – пароль;
- `/w:<width>` – ширина окна;
- `/h:<height>` – высота окна;
- `/f` – полноэкранный режим.

Например:

```
$ xfreerdp /v:192.168.0.148 /u:user /p:password
```

Примечание. Если не указывать пользователя или пароль, появится окно входа.

На рис. 551 показано подключение к терминальной сессии с использованием xfreerdp.

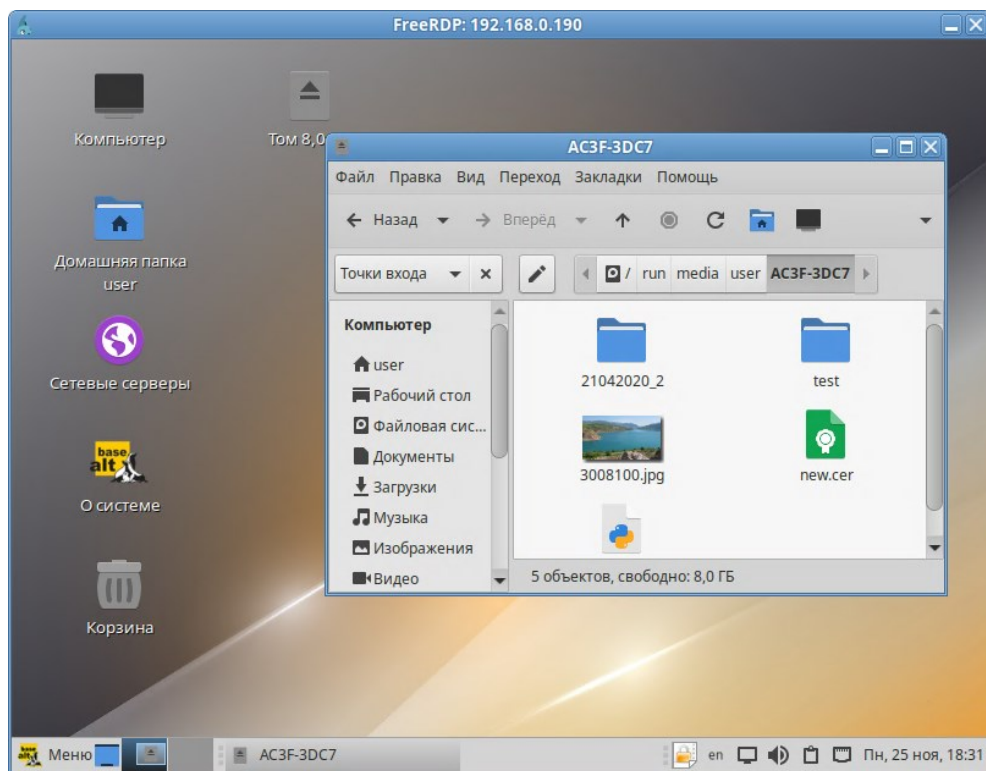


Рис. 551 – FreeRDP. Подключение к удаленному рабочему столу

В качестве клиента удаленного доступа также можно использовать программу Remmina:

- 1) установить пакеты remmina и remmina-plugins-rdp:

```
# apt-get install remmina remmina-plugins-rdp
```
- 2) запустить Remmina, выбрав в меню «Приложения» → «Интернет» → «Remmina»;
- 3) в окне Remmina нажать кнопку создания нового подключения (рис. 552) и в открывшемся окне (рис. 553) указать настройки RDP-подключения (IP-адрес терминального сервера, имя пользователя, пароль и т. д.), нажать кнопку «Сохранить и подключить». В результате будет создано подключение (рис. 554).

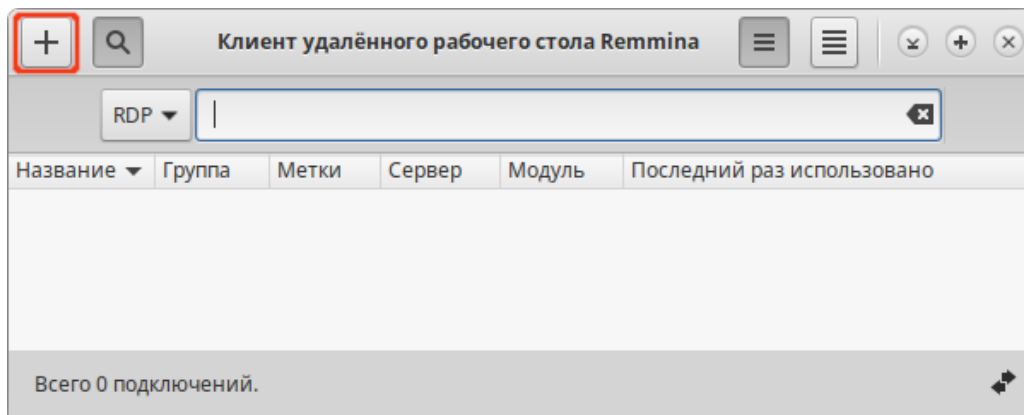


Рис. 552 – Кнопка создания нового подключения

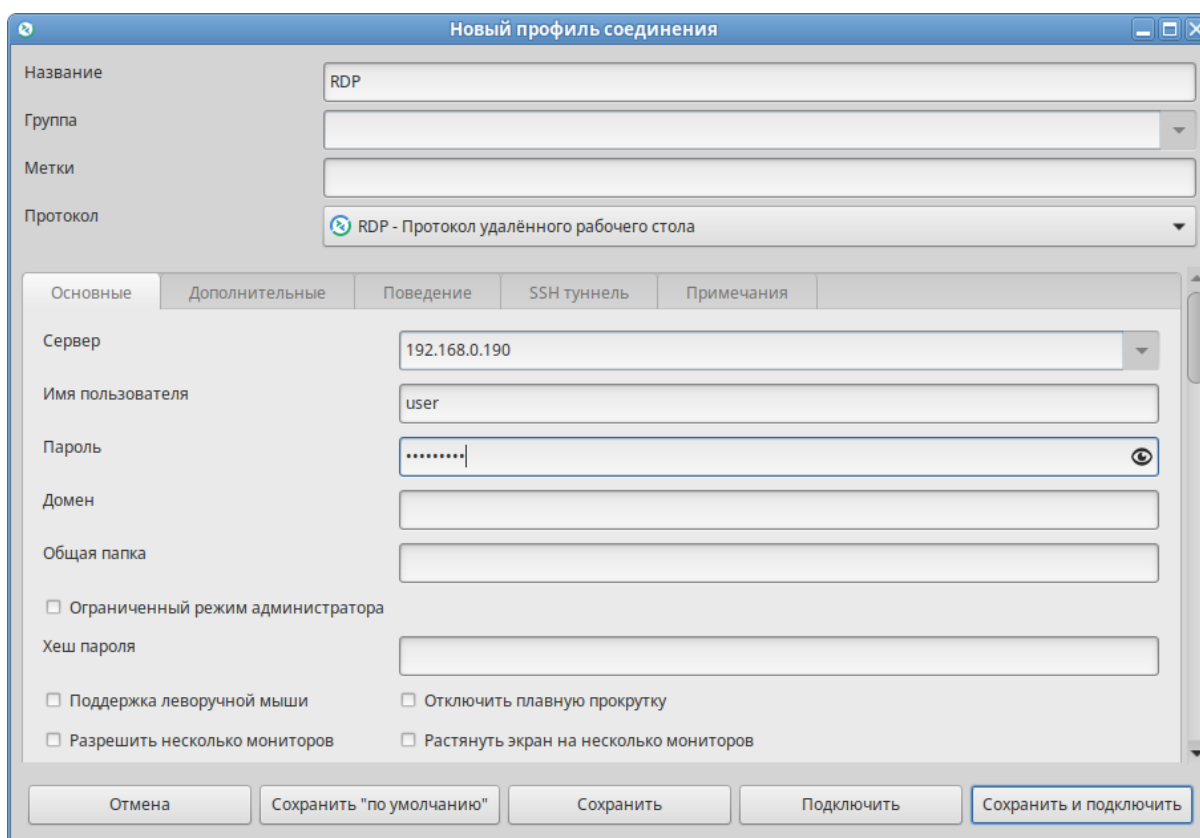


Рис. 553 – Настройки RDP-подключения

Примечание. Если автоматического монтирования не происходит, следует выполнить команду:

```
$ udisksctl mount -b /dev/sdb1
```

где /dev/sdb1 – USB-устройство (можно посмотреть в выводе команды lsblk).

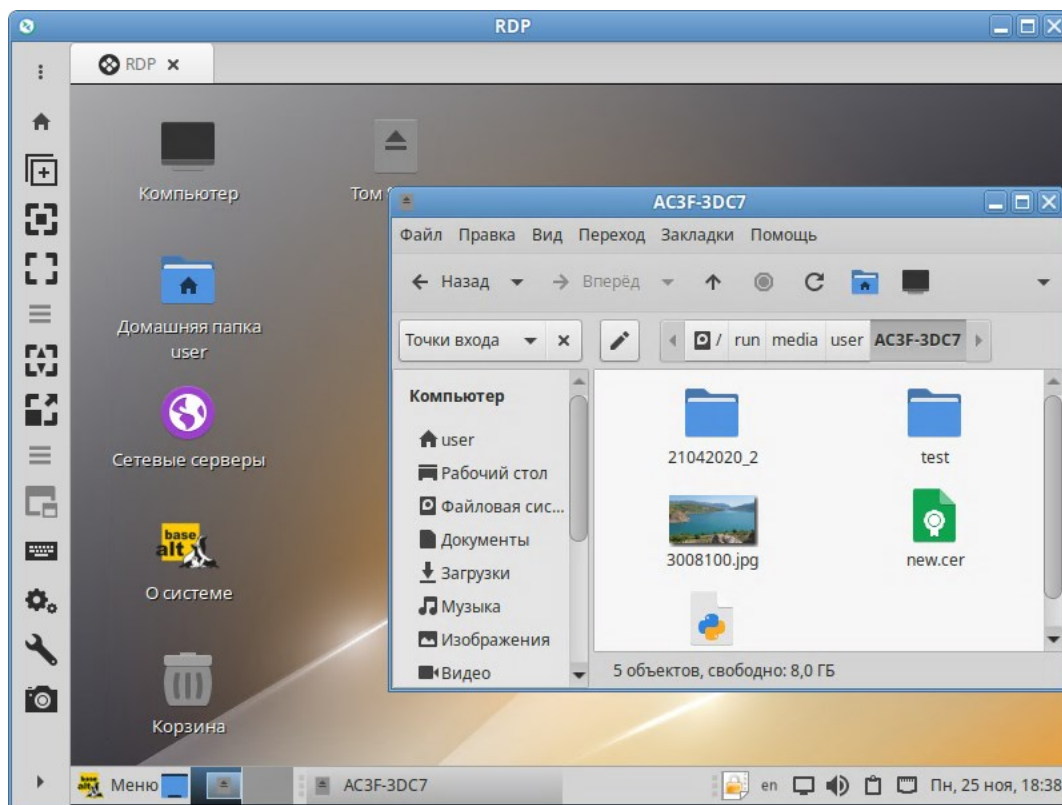


Рис. 554 – Remmina. Подключение к удаленному рабочему столу

В качестве клиента удаленного доступа можно использовать программу MyConnector. MyConnector позволяет осуществлять удаленный доступ к компьютерам с различными ОС с использованием распространенных типов подключений, таких как RDP, VNC, NX, XDMCP, SSH, SFTP. MyConnector реализует интерфейс для пользователя к предустановленным программам для запуска их с введенными параметрами.

Подключение с помощью MyConnector:

1) установить пакет myconnector на клиентский компьютер:

```
# apt-get install myconnector
```

2) запустить Myconnector, выбрав в меню «Приложения» → «Интернет» → «MyConnector»;

3) в окне подключения (рис. 555) указать IP-адрес терминального сервера. Нажать на кнопку «Дополнительные параметры» и в открывшемся окне (рис. 556) указать настройки RDP-подключения. Нажать на кнопку «Подключение» для подключения к терминальной сессии (рис. 557).

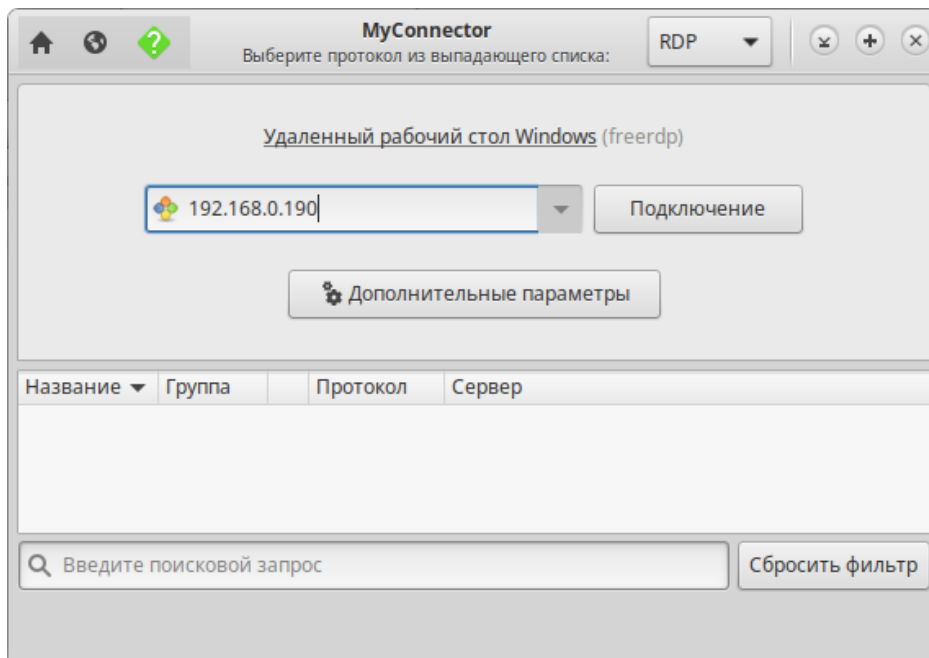


Рис. 555 – MyConnector. Окно подключения

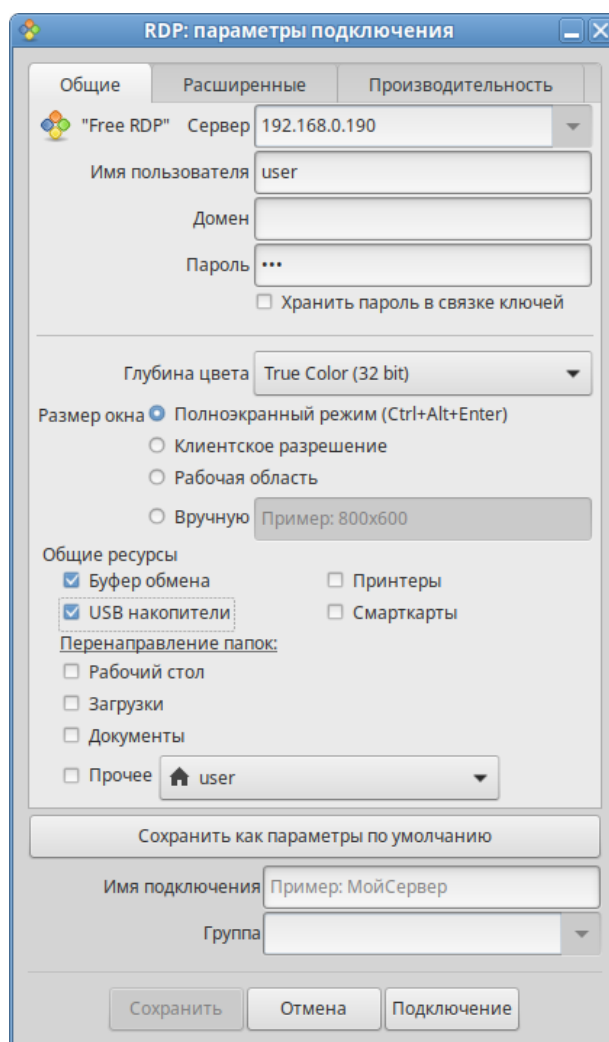


Рис. 556 – Настройки RDP-подключения

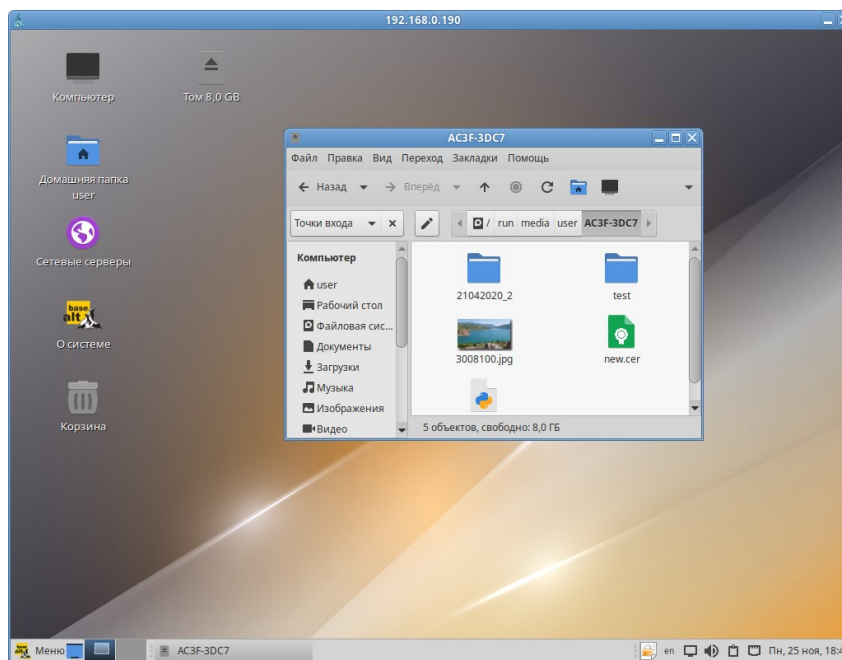


Рис. 557 – MyConnector. Подключение к удаленному рабочему столу

17.16.7. Управление XRDP

Просмотр информации об активных пользователях:

```
# ps aux |grep xrdp |grep xorg
user          5689   0.6   2.5  943524 100112 ?        Ssl   17:48   0:09
Xorg  :10 -auth .Xauthority -config xrdp/xorg.conf -noreset -nolisten tcp -
logfile .xorgxrdp.%s.log
```

В выводе команды видно, что подключен пользователь user и его PID 5689.

Следующая команда отключит пользователя user и завершит все его процессы:

```
# pkill -9 -u user
```

17.17. Timeshift

Timeshift – программа для автоматического периодического создания копий системы (снимков/snapshots).

Timeshift предназначен, прежде всего, для сохранения системных файлов и настроек. Пользовательские данные по умолчанию не архивируются, поэтому в случае сбоя системы, восстанавливаются системные файлы, а данные пользователей остаются в актуальном состоянии (конечно, если они не были повреждены).

Резервные копии не могут быть восстановлены на уровне отдельных файлов, восстановление всегда происходит в полном объеме настроек Timeshift.

Запустить Timeshift можно из МАТЕ «Меню» → «Приложения» → «Системные» → «Timeshift» или из командной строки:

```
$ timeshift-launcher
```

Запуск Timeshift требует прав администратора, поэтому необходимо ввести пароль администратора (рис. 558).

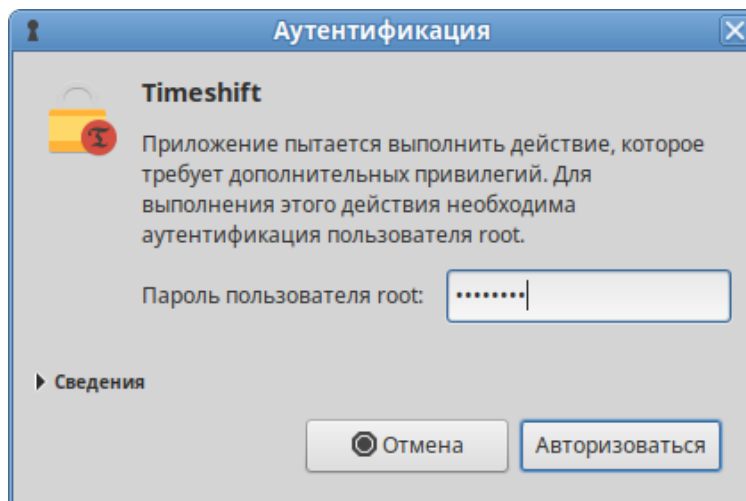


Рис. 558 – Запрос пароля для запуска Timeshift

При первом запуске Timeshift будет запущен «Мастер установки». Запустить мастер установки или открыть окно настроек резервного копирования также можно, нажав соответствующую кнопку на панели инструментов в окне Timeshift (рис. 559).

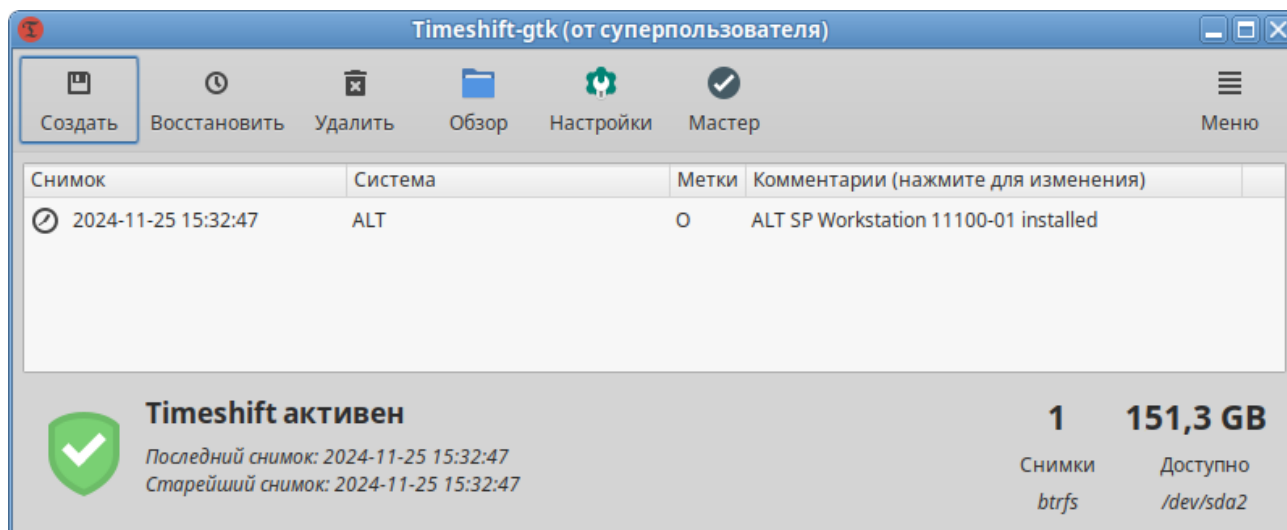


Рис. 559 – Окно программы Timeshift

17.17.1. Настройка резервного копирования

17.17.1.1. Режим RSYNC

Особенности режима RSYNC:

- снимки создаются путем копирования системных файлов при помощи `rsync` и создания жестких ссылок на неизменные файлы из предыдущего снимка;
- все файлы копируются при создании первого снимка. Последующие снимки являются инкрементальными. Неизменные файлы будут связаны с предыдущим снимком, если он доступен;
- создание первого снимка может занять до 10 минут;
- системный раздел может быть отформатирован в любой файловой системе. Резервный раздел может быть отформатирован в любой файловой системе Linux, поддерживающей жесткие ссылки. Сохранение снимков на несистемный или внешний диск позволяет восстановить систему, даже если системный диск поврежден;
- можно задать исключения для файлов и каталогов для экономии дискового пространства;
- систему нужно перезагрузить после восстановления снимка.

Тип снимков можно выбрать на вкладке «Тип» окна настроек Timeshift (рис. 560) или на первом шаге работы мастера установки.

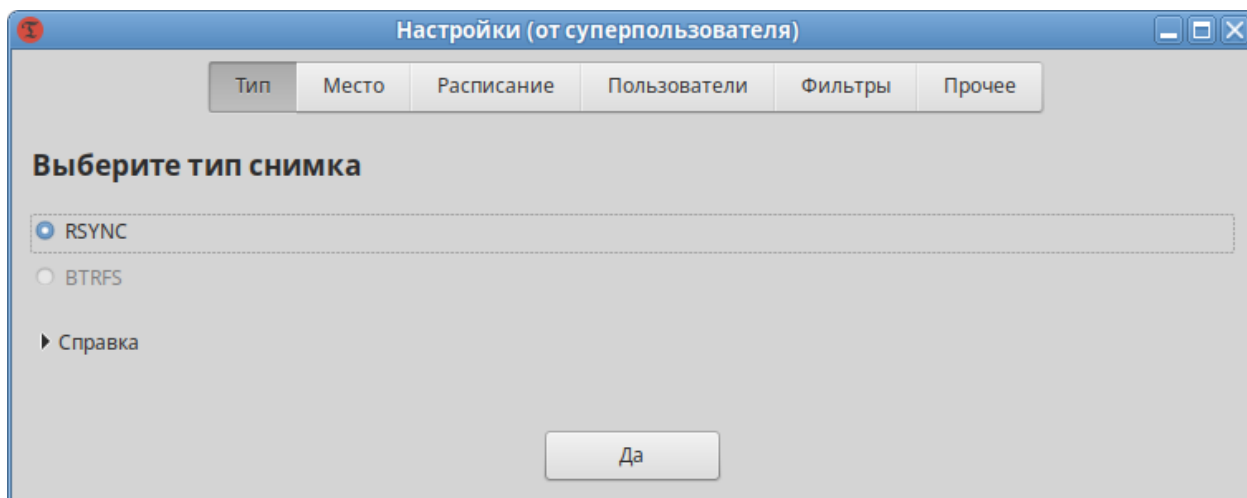


Рис. 560 – Выбор режима RSYNC

На вкладке «Место» можно выбрать диск, где будут храниться снимки (рис. 561). RSYNC снимки имеют большой размер, поэтому желательно хранить их на другом (не системном) диске или разделе. По умолчанию снимки сохраняются в системном (корневом) разделе в /timeshift, также можно выбрать другие разделы Linux.

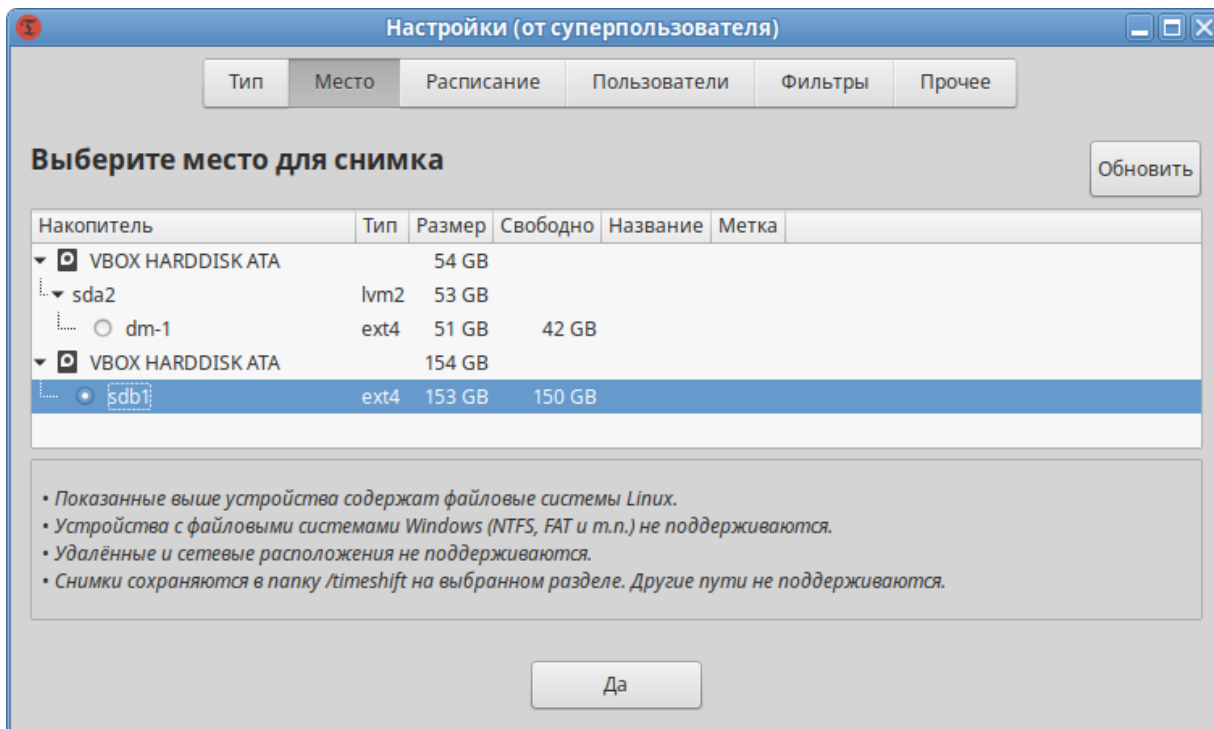


Рис. 561 – Выбор места хранения снимков RSYNC

На вкладке «Расписание» (рис. 562) следует выбрать уровни создания снимков (ежемесячно, еженедельно, ежедневно, ежечасно, при загрузке) и указать количество сохраняемых снимков для каждого уровня.

Примечание. Снимки уровня «Загрузка» создаются при каждом запуске системы (с задержкой в 10 минут). Они выполняются в фоне и не влияют на скорость загрузки системы.

По умолчанию домашние каталоги пользователей не включаются в резервную копию. На вкладке «Пользователи» можно изменить это поведение. Например, если выбрать опцию «Включить только скрытые файлы» (рис. 563), будет выполнено резервное копирование и восстановление скрытых файлов и каталогов в домашнем каталоге пользователя (эти каталоги содержат пользовательские файлы конфигурации).

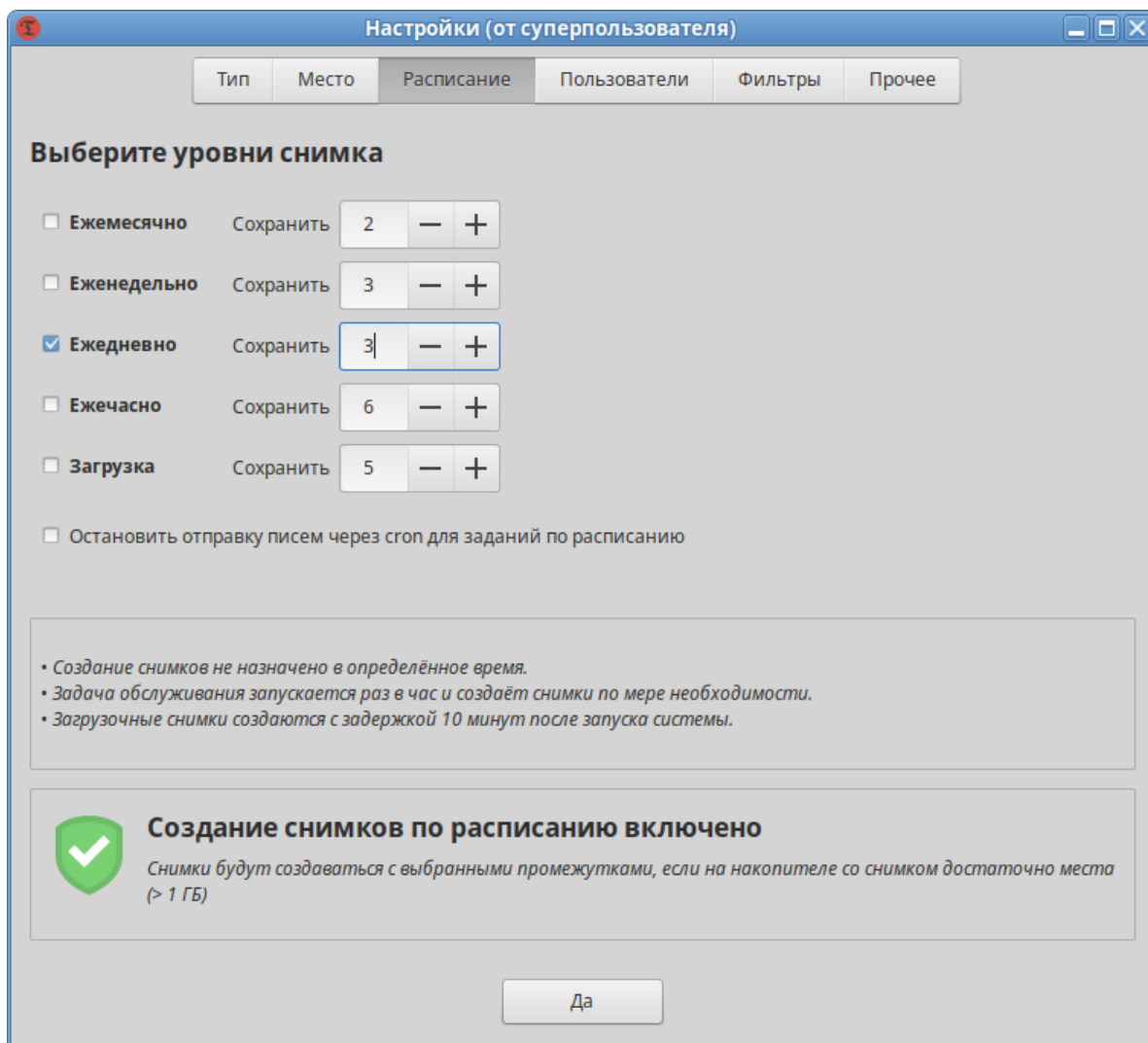


Рис. 562 – Расписание для снимков RSYNC

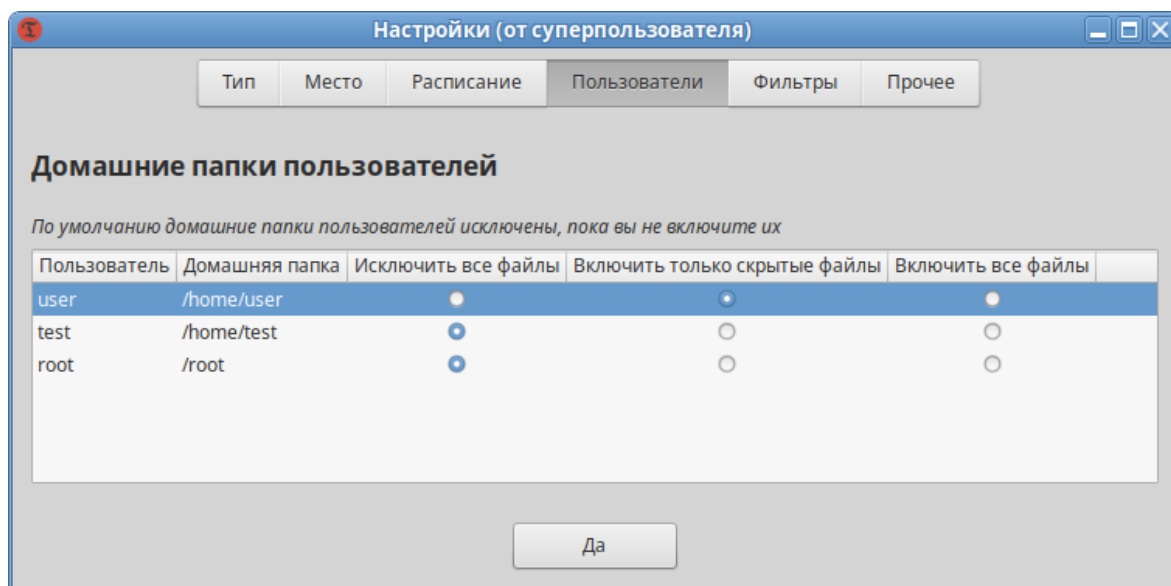


Рис. 563 – Вкладка «Пользователи»

На вкладке «Фильтры» (рис. 564) можно указать, какие файлы/каталоги включать/исключать из резервного копирования (динамические каталоги исключаются по умолчанию: /dev, /proc, ...).

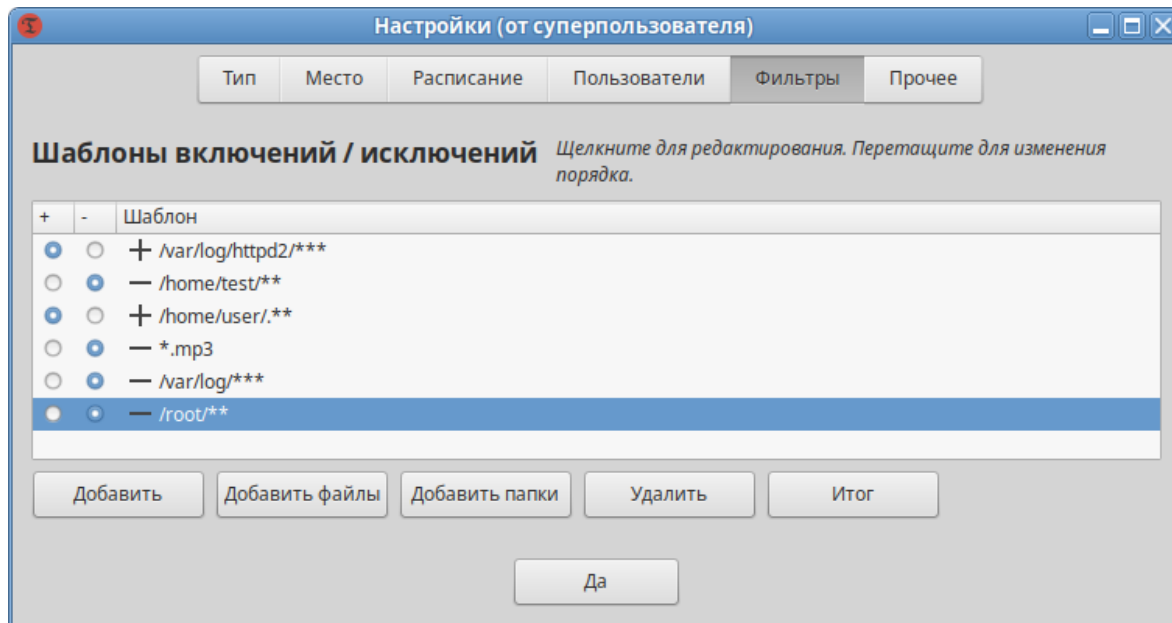


Рис. 564 – Timeshift. Вкладка «Фильтры»

В данном примере из резервной копии будут исключены все файлы mp3, все системные журналы, кроме журналов веб-сервера Apache. Просмотреть итоговый список исключений (рис. 565) можно, нажав кнопку «Итог» на вкладке «Фильтры». Отредактировать шаблон можно, дважды щелкнув левой кнопкой мыши по строке шаблона.

На вкладке «Прочее» (рис. 566) можно выбрать формат даты.

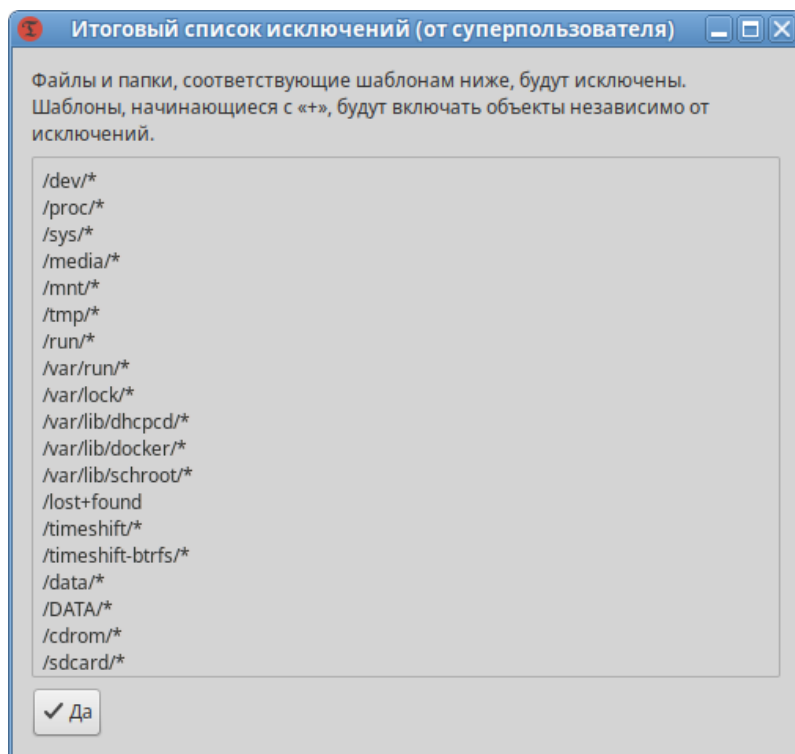


Рис. 565 – Итоговый список исключений

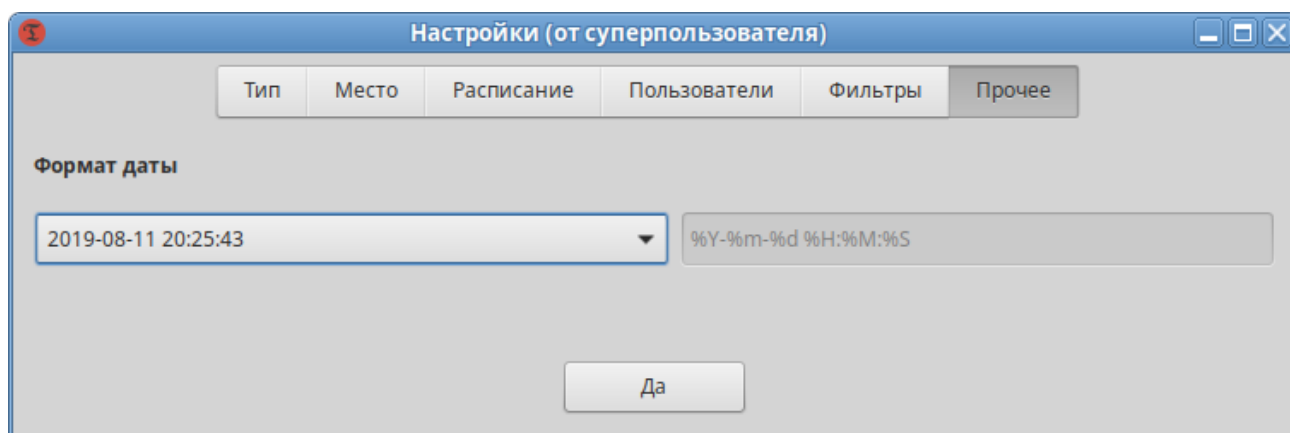


Рис. 566 – Итоговый список исключений

17.17.1.2. Режим BTRFS

Особенности режима BTRFS:

- снимки создаются с использованием встроенных средств файловой системы BTRFS;
- снимки создаются и восстанавливаются мгновенно (создание снимков – это атомарная транзакция на уровне файловой системы);

- снимки восстанавливаются путем замены системных подразделов. Поскольку файлы никогда не копируются, не удаляются и не перезаписываются, риск потери данных отсутствует. Существующая система сохраняется как новый снимок после восстановления;
- снимки сохраняются на том же диске, с которого они созданы (системном диске). Хранение на других дисках не поддерживается. Если системный диск выйдет из строя, снимки, хранящиеся на нем, будут потеряны вместе с системой;
- нет возможности исключать файлы и каталоги;
- размер снимков BTRFS изначально равен нулю. При изменении системных файлов, данные записываются в новые блоки данных, которые занимают дисковое пространство (копирование при записи). Файлы в снимке продолжают указывать на исходные блоки данных;
- снимки можно восстановить без немедленной перезагрузки запущенной системы;
- ОС должна быть установлена на раздел BTRFS с разбивкой на подразделы @ и @home. Другие виды разделов не поддерживаются.

Примечание. Для установки ОС на раздел BTRFS с разбивкой на подразделы @ и @home можно при установке системы, на этапе «Подготовка диска» создать следующие подтома (рис. 567):

- подтом @ с точкой монтирования в /;
- подтом @home с точкой монтирования в /home.

Тип снимков BTRFS можно выбрать на вкладке «Тип» окна настроек Timeshift (рис. 567) или на первом шаге работы мастера установки.

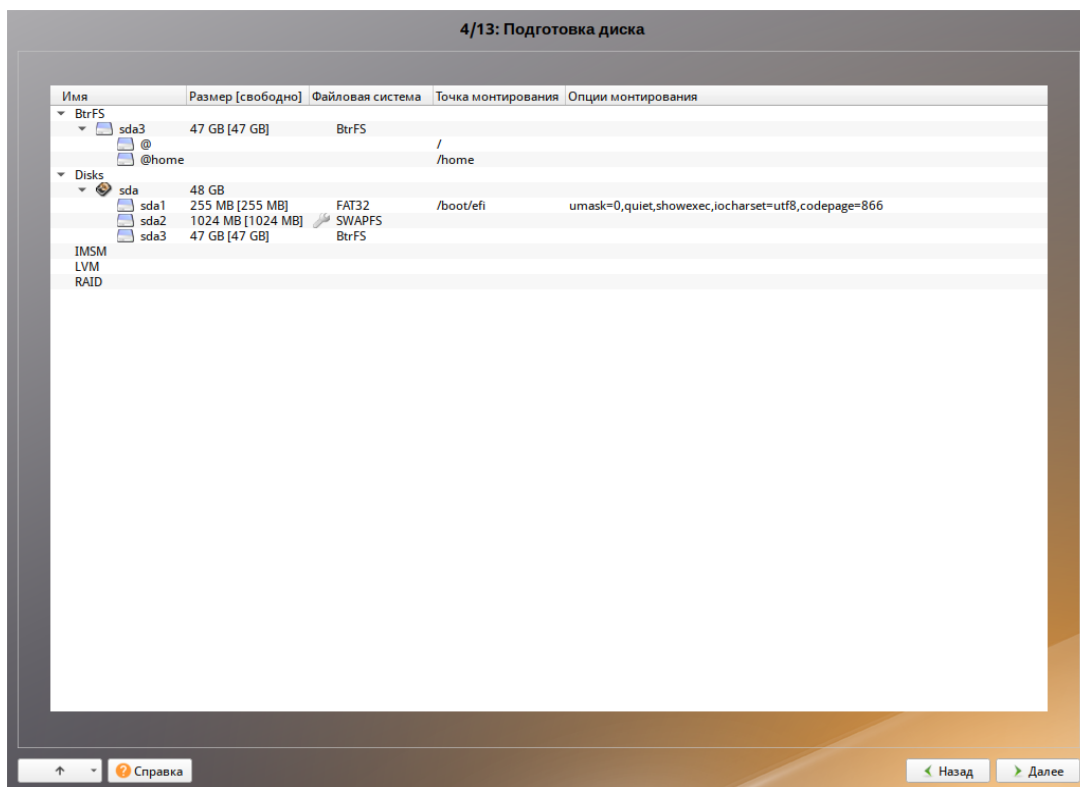


Рис. 567 – Корень системы с файловой системой BTRFS

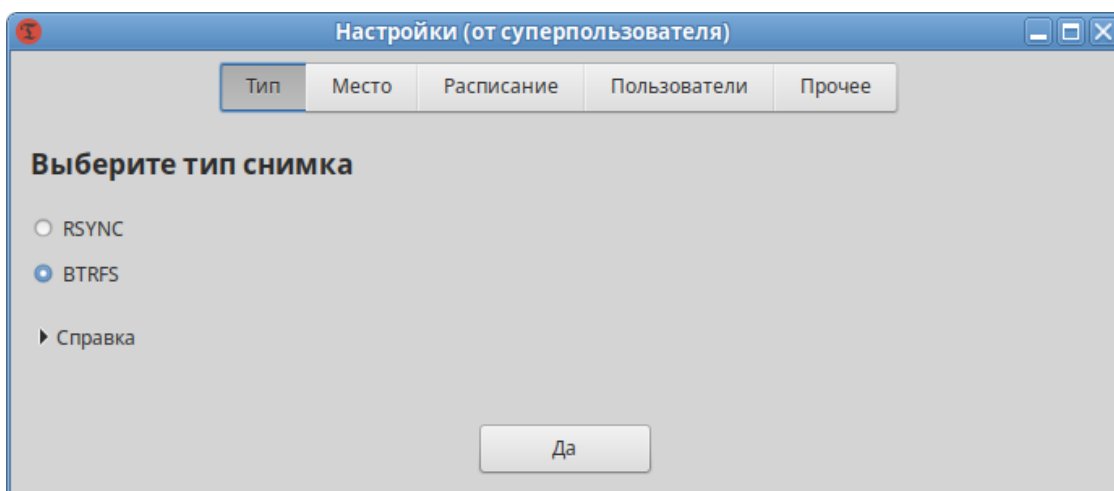


Рис. 568 – Выбор режима BTRFS

Снимки BTRFS сохраняются в системном разделе, другие разделы не поддерживаются (рис. 569).

На вкладке «Расписание» следует выбрать уровни создания снимков (ежемесячно, еженедельно, ежедневно, ежечасно, при загрузке) и указать количество сохраняемых снимков для каждого уровня (рис. 570).

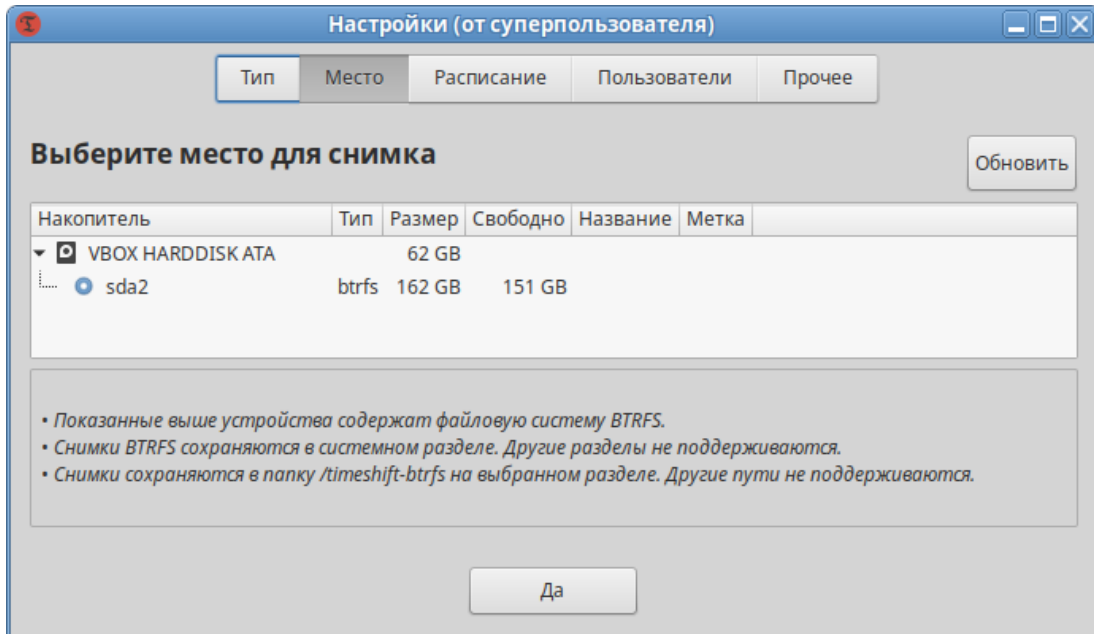


Рис. 569 – Выбор места хранения снимков BTRFS

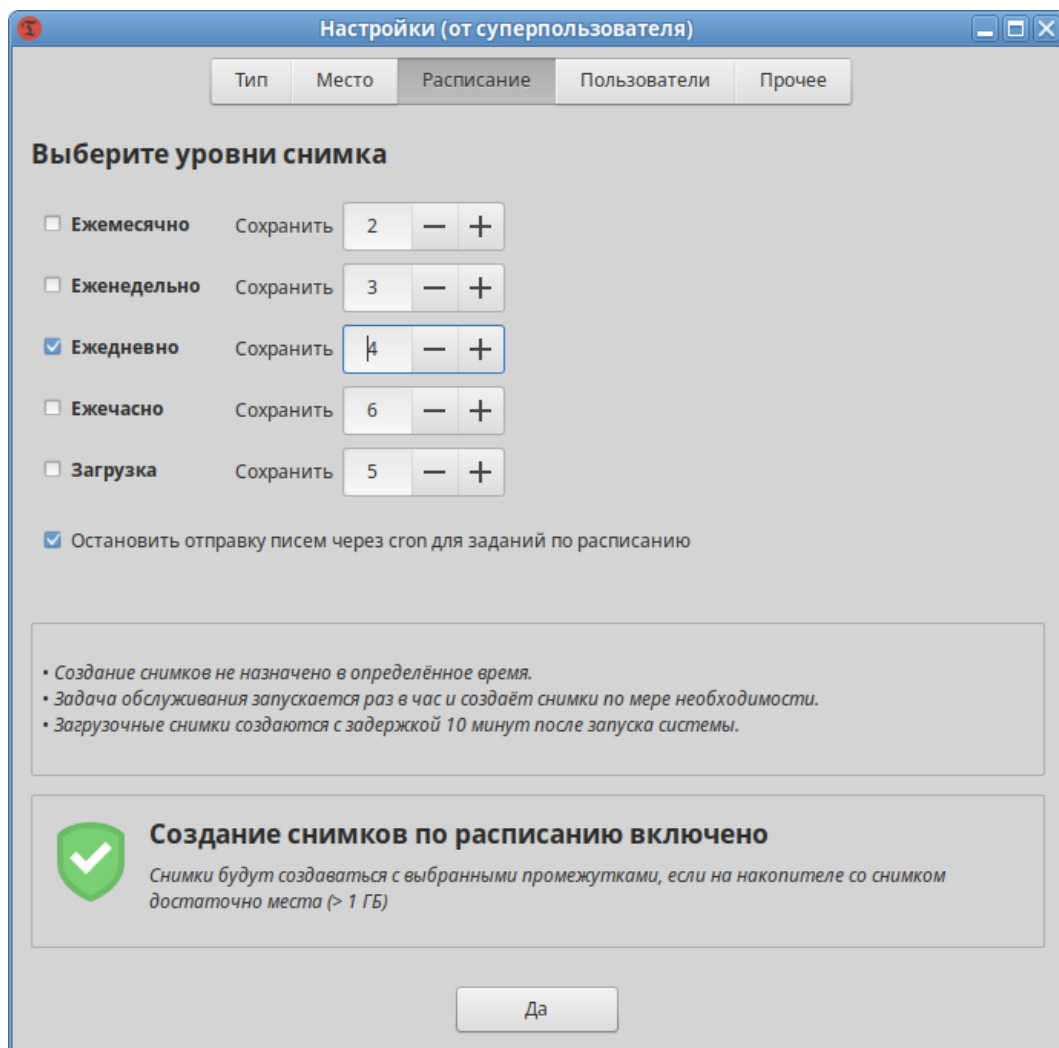


Рис. 570 – Расписание для снимков BTRFS

По умолчанию домашние каталоги пользователей не включаются в резервную копию. На вкладке «Пользователи» можно изменить это поведение и включить подраздел @home в создаваемые снимки (рис. 571).

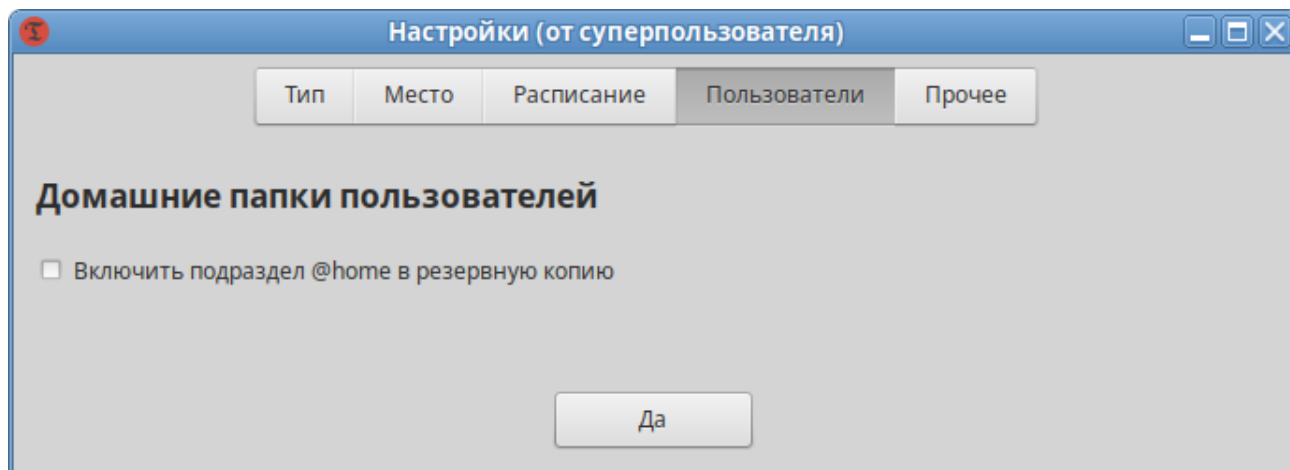


Рис. 571 – Включить подраздел @home в создаваемые снимки

На вкладке «Прочее» можно выбрать формат даты.

17.17.2. Создание снимков

Снимки будут создаваться автоматически согласно настроенному расписанию.

Для создания снимка в ручном режиме следует нажать кнопку «Создать» на панели инструментов (рис. 572). Резервная копия будет создана на устройстве хранения, который был указан в настройках.

17.17.3. Восстановление системы

Снимки можно восстановить как из работающей системы (оперативное восстановление), так и из другой системы, на которой установлен Timeshift (автономное восстановление).

Для восстановления снимка следует выбрать снимок в главном окне и нажать кнопку «Восстановить» (рис. 573).

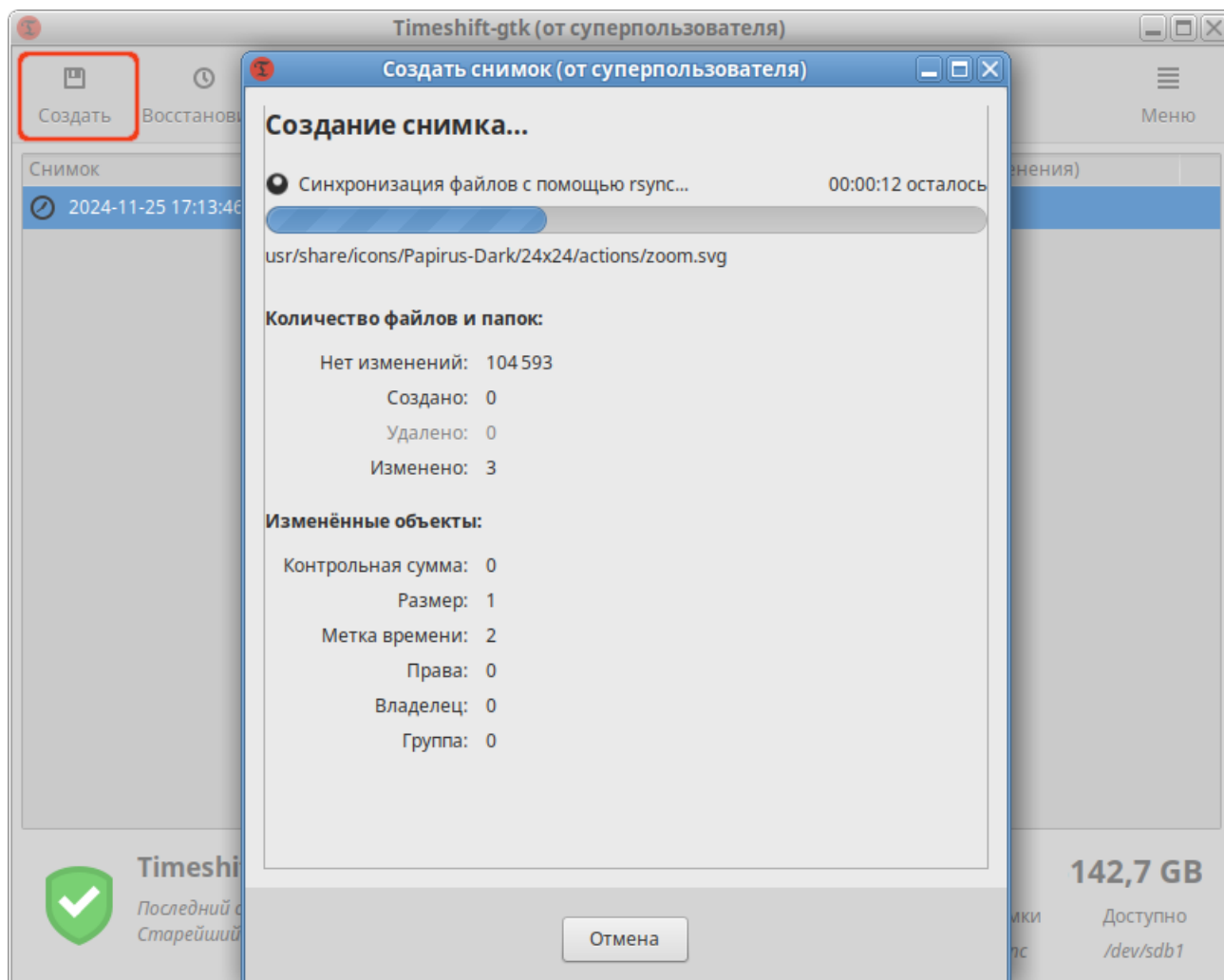


Рис. 572 – Создание снимка в режиме RSYNC

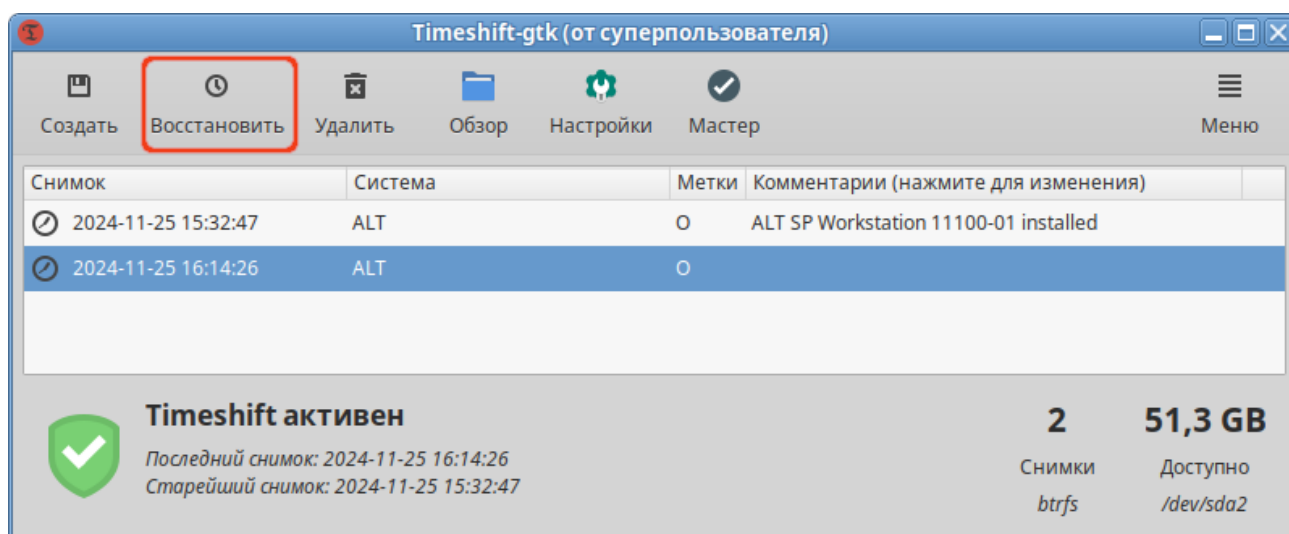


Рис. 573 – Снимки системы и кнопка «Восстановить»

При восстановлении снимка в режиме RSYNC после нажатия кнопки «Восстановить» можно выбрать устройство, куда будут восстановлены файлы (рис. 574), указать нужно ли переустанавливать GRUB, нажав кнопку «Настройки загрузчика (дополнительные)». На следующем шаге будут показаны файлы, которые будут созданы/восстановлены/удалены в процессе восстановления снимка (рис. 575).

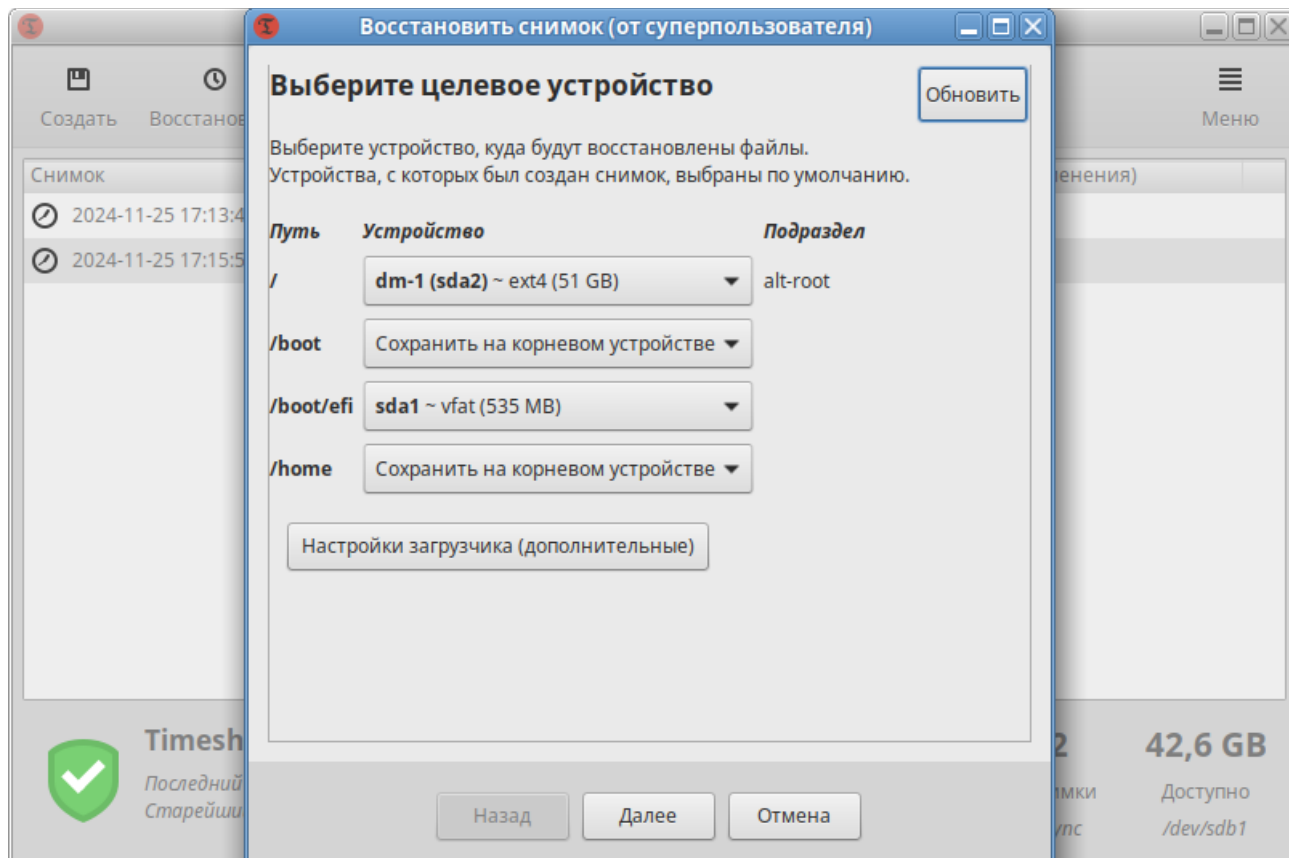


Рис. 574 – Выбор целевого устройства

Примечание. Если основная система не загружается, то можно загрузиться в режиме восстановления и развернуть снимок в командной строке.

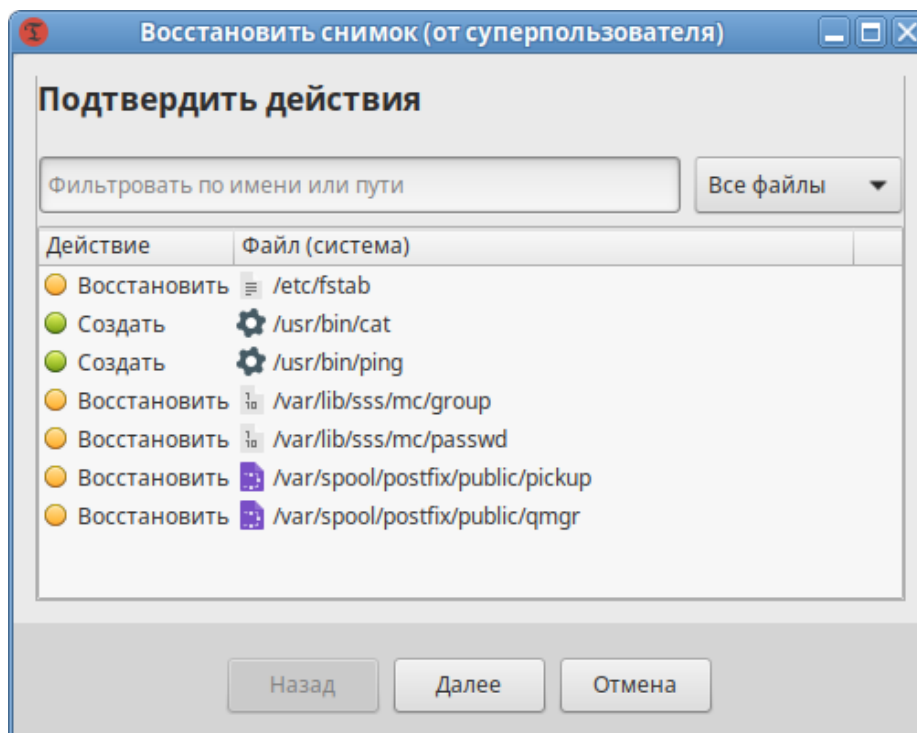


Рис. 575 – Восстановление снимка в режиме RSYNC

17.17.4. Работа с Timeshift в командной строке

Примечание. Одновременно может работать только один экземпляр Timeshift, поэтому для работы с Timeshift из командной строки необходимо закрыть окно программы Timeshift.

Вывод справки о команде:

```
$ timeshift
```

Если параметры не указаны, например, при создании снимка, значения по умолчанию будут загружены из конфигурации приложения.

Просмотр списка снимков:

```
# timeshift --list
Mounted '/dev/sdb1' at '/run/timeshift/6683/backup'
Device : /dev/sdb1
UUID   : 136a6133-f354-4d84-b4d1-07a52b7d8203
Path   : /run/timeshift/6683/backup
Mode   : RSYNC
Status : OK
2 snapshots, 42.6 GB free
```

Num	Name	Tags	Description
0	> 2024-11-25_17-13-46	0	
1	> 2024-11-25_17-15-52	0	

Пример создания снимка (в режиме RSYNC):

```
# timeshift --create --comments "after update" --tags D

Mounted '/dev/sdb1' at '/run/timeshift/6727/backup'
-----
Creating new snapshot...(RSYNC)
Saving to device: /dev/sdb1, mounted at path:
/run/timeshift/6727/backup
Linking from snapshot: 2024-11-25_17-15-52
Syncing files with rsync...
Created control file:
/run/timeshift/6727/backup/timeshift/snapshots/2024-11-25_17-31-45/info.json
RSYNC Snapshot saved successfully (14s)
Tagged snapshot '2024-11-25_17-31-45': ondemand
-----
```

Пример создания (в режиме BTRFS):

```
# timeshift --create --comments "after update" --tags D

Using system disk as snapshot device for creating snapshots in BTRFS
mode
Mounted '/dev/sda2' at '/run/timeshift/5005/backup'
btrfs: Quotas are not enabled
Creating new backup...(BTRFS)
Saving to device: /dev/sda2, mounted at path:
/run/timeshift/5005/backup
Created directory: /run/timeshift/5005/backup/timeshift-
btrfs/snapshots/2024-11-25_16-32-28
Created subvolume snapshot: /run/timeshift/5005/backup/timeshift-
btrfs/snapshots/2024-11-25_16-32-28/@
Created control file: /run/timeshift/5005/backup/timeshift-
btrfs/snapshots/2024-11-25_16-32-28/info.json
BTRFS Snapshot saved successfully (0s)
Tagged snapshot '2024-11-25_16-32-28': ondemand
-----
```

Создание снимка, если он запланирован (есть в расписании):

```
# timeshift --check
```

Восстановить снимок (параметры будут запрошены в интерактивном режиме):

```
# timeshift --restore
```

Восстановить снимок:

```
# timeshift --restore --snapshot '2024-11-25_17-13-46'
```

Восстановить определенный снимок в раздел:

```
# timeshift --restore --snapshot '2024-11-25_17-15-52' --target /dev/sdb1
```

Удалить снимок:

```
# timeshift --delete --snapshot '2024-11-25_17-15-52'
```

Если основная система не загружается, то нужно загрузиться в режиме восстановления и выполнить следующие действия (на примере режима RSYNC):

1) установить timeshift:

```
# apt-get update && apt-get install timeshift
```

2) посмотреть список снимков на устройстве:

```
# timeshift --list --snapshot-device /dev/sdb1
```

3) запустить восстановление:

```
# timeshift --restore --snapshot-device /dev/sdb1 --snapshot  
'2024-11-25_17-13-46' --target /dev/sda2 --grub-device /dev/sda
```

4) перезагрузить систему.

17.18. Информация о системе и об аппаратной части компьютера

17.18.1. Команда inxi

inxi – это инструмент командной строки, который позволяет отображать информацию о системе и об аппаратной части компьютера. Часто используется в качестве инструмента отладки для технической поддержки, чтобы быстро определить конфигурации системы и оборудование пользователей.

Установка пакета inxi:

```
# apt-get install inxi
```

Команда:

```
inxi [-AbBCdDEfFGhiIjJlLmMnNopPrRsSuUVwyYzZ]
```

```
inxi [-c <целое число>] [--sensors-exclude SENSORS] [--  
sensors-use SENSORS] [-t [c|m|cm|mc][целое число]] [-v <целое  
число>] [-W LOCATION] [--weather-unit {m|i|mi|im}] [-y WIDTH]
```

```
inxi [--edid] [--memory-modules] [--memory-short] [--recommends]  
[--sensors-default] [--slots]
```

```
inxi [-x|-xx|-xxx|-a] -OPTION(s)
```

В таблице 104 приведены некоторые стандартные опции команды inxi.

Т а б л и ц а 104 – Стандартные опции команды inxi

Ключ	Описание
-A	<p>Выводит информацию об аудио/звуковых устройствах, включая драйвер устройства. Для отображения всех обнаруженных звуковых API/серверов, включая неактивные, нужно использовать ключ -Ax:</p> <pre>\$ inxi -Ax Audio: Device-1: Intel Alder Lake PCH-P High Definition Audio vendor: Lenovo driver: sof-audio-pci-intel-tgl bus-ID: 00:1f.3 API: ALSA v: k6.1.12-un-def-alt1 status: kernel-api Server-1: JACK v: 1.9.22 status: off Server-2: PulseAudio v: 16.1 status: active</pre>
-b	<p>Выводит общую информацию в краткой форме. Аналогично выводу <code>\$ inxi -v 2</code>.</p>
-B	<p>Выводит данные батареи системы (при наличии батареи): (ID-x), заряд, состояние, а также дополнительную информацию.</p> <pre>\$ inxi -B Battery: ID-1: BAT0 charge: 54.5 Wh (100.0%) condition: 54.5/57.0 Wh (95.6%)</pre>
-c	<p>Задаёт цветовую тему для стилизации выводимой информации. Предусмотрено 43 темы (0-42):</p> <pre>\$ inxi -c 5</pre> <p>Просмотреть все предустановленные темы можно, выполнив команду:</p> <pre>\$ inxi -c 94</pre>
-C	<p>Выводит данные о процессоре (дополнительные данные доступны с ключами -x, -xxx и -a):</p> <pre>\$ inxi -C CPU: Info: 10-core (2-mt/8-st) model: 12th Gen Intel Core i7-1255U bits: 64 type: MST AMCP cache: L2: 6.5 MiB Speed (MHz): avg: 2480 min/max: 400/4700:3500 cores: 1: 2873 2: 3438 3: 1903 4: 2600 5: 1787 6: 2600 7: 2600 8: 2316 9: 2600 10: 2600 11: 2600 12: 1853</pre>
-d	<p>Выводит данные накопителей на оптических дисках</p>
-D	<p>Выводит информацию о жестких дисках: идентификатор диска, тип (FireWire, съемный, USB), производитель (если обнаружен), модель и размер. Также показывает общее пространство на дисках и занятое место:</p> <pre>\$ inxi -D Drives: Local Storage: total: 1.4 TiB used: 426.1 GiB (29.8%) ID-1: /dev/nvme0n1 vendor: Micron model: MTFDKCD512TFK size: 476.94 GiB ID-2: /dev/nvme1n1 vendor: Western Digital model: WD PC SN740 SDDPTQD- 1T00 size: 953.87 GiB</pre>
-E	<p>Выводит информацию об устройствах bluetooth:</p> <pre>\$ inxi -E Bluetooth: Device-1: Intel AX201 Bluetooth driver: btusb type: USB Report: hciconfig ID: hci0 state: up address: 3C:21:9C:AE:28:B4 bt-v: 3.0</pre>

Продолжение таблицы 104

Ключ	Описание
-F	<p>Выводит общую информацию. Включает все буквы верхнего регистра, а также <code>-s</code> и <code>-n</code>. Не выводит дополнительные подробные данные, такие как <code>-d -f -l -m -o -p -r -t -u -x</code>, если эти ключи не используются в команде, например:</p> <pre>\$ inxi -Frmxx</pre>
-G	<p>Выводит информацию о графических устройствах, включая сведения о драйверах устройств и дисплеев. При использовании ключей <code>-Gxx</code> также выводится информация о мониторах.</p> <pre>\$ inxi -G Graphics: Device-1: Intel Alder Lake-UP3 GT2 [Iris Xe Graphics] driver: i915 v: kernel Device-2: Syntek Integrated Camera driver: uvcvideo type: USB Display: x11 server: X.Org v: 1.21.1.8 driver: X: loaded: modesetting unloaded: fbdev,vesa dri: iris gpu: i915 resolution: 1: 1920x1080~60Hz 2: 1920x1080~60Hz API: OpenGL v: 4.6 Mesa 23.0.4 renderer: Mesa Intel Graphics (ADL GT2)</pre>
-i	<p>Отображает локальные и WAN IP-адреса. По соображениям безопасности, эти данные не отображаются в выводе с <code>-F</code></p>
-I	<p>Выводит следующую информацию: процессы, время бесперебойной работы, память, оболочка:</p> <pre>\$ inxi -I Info: Processes: 338 Uptime: 3h 15m Memory: available: 38.88 GiB used: 9.91 GiB (25.5%) Shell: Bash inxi: 3.3.27</pre> <p>Для получения дополнительной информации, можно использовать параметры <code>-Ix</code>, <code>-Ixx</code> и <code>-Ia</code>:</p> <pre>\$ inxi -Ia Info: Processes: 337 Uptime: 3h 16m wakeups: 4 Memory: available: 38.88 GiB used: 9.94 GiB (25.6%) Init: systemd v: 252 target: graphical (5) default: graphical tool: systemctl Compilers: gcc: 12 Packages: pm: rpm pkgs: N/A note: see --rpm Shell: Bash v: 4.4.23 running-in: xfce4- terminal inxi: 3.3.27</pre>
-j	<p>Показывает все активные типы подкачки (раздел, файл, zram). Чтобы отобразить метки разделов или UUID (если они доступны и уместны), следует использовать с <code>-l</code> или <code>-u</code>.</p> <pre>\$ inxi -ju Swap: ID-1: swap-1 type: partition size: 7.46 GiB used: 0 KiB (0.0%) dev: /dev/nvme0n1p2 uuid: 3cee8e1f-494c-4622-90d9-5f3da9ab2082</pre>
-J	<p>Выводит данные USB для подключенных концентраторов и устройств. Концентраторы также показывают количество портов</p>
-l	<p>Выводит метки разделов. Следует использовать с ключами <code>-j</code>, <code>-o</code>, <code>-p</code> и <code>-P</code>. Если ни один из этих ключей не указан, ничего не выводит</p>
-L	<p>Выводит информацию о логическом томе для LVM, LUKS, bcache и т. д.</p>

Продолжение таблицы 104

Ключ	Описание
-m	<p>Выводит информацию о памяти (RAM). Не отображается с ключами -b или -F, если -m не указывается явно. Данный ключ использует dmidecode, который должен запускаться от имени пользователя root:</p> <pre># inxi -m Memory: System RAM: available: 38.88 GiB used: 9.95 GiB (25.6%) Array-1: capacity: 256 GiB slots: 8 EC: None Device-1: Controller0-ChannelA-DIMM0 type: DDR4 size: 32 GiB speed: 3200 MT/s Device-2: Controller0-ChannelB-DIMM0 type: no module installed ...</pre>
-M	Выводит информацию о машине: устройство, материнская плата, BIOS.
-n	Выводит расширенную информацию о сетевом устройстве.
-N	<p>Выводит информацию о сетевых устройствах, включая драйвер устройства. С ключом -x показывает идентификатор шины, номер порта.</p> <pre>\$ inxi -N Network: Device-1: Intel Alder Lake-P PCH CNVi WiFi driver: iwlwifi Device-2: Intel Ethernet I219-V driver: e1000e</pre>
-o	Выводит информацию о несмонтированном разделе (включая UUID и LABEL, если они доступны)
-P	Выводит полную информацию о всех смонтированных разделах. Чтобы отобразить метки разделов или UUID (если они доступны и уместны), следует использовать с ключами -l или -u.
-P	<p>Выводит основную информацию о разделах (показывает, если обнаружено: / /boot /boot/efi /home /opt /tmp /usr /usr/home /var /var/tmp /var/log):</p> <pre>\$ inxi -P Partition: ID-1: / size: 460.79 GiB used: 426.1 GiB (92.5%) fs: ext4 dev: /dev/nvme0n1p3 ID-2: swap-1 size: 7.46 GiB used: 0 KiB (0.0%) fs: swap dev: /dev/nvme0n1p2</pre>
-r	Выводит информацию о репозиториях
-R	Выводит данные RAID. Показывает устройства RAID, состояния, уровни, размер устройства/массива и компоненты
-s	<p>Выводит данные от датчиков (если эти датчики установлены/настроены): температура материнской платы/процессора/графического процессора; скорость вентилятора:</p> <pre>\$ inxi -s Sensors: System Temperatures: cpu: 48.0 C mobo: N/A Fan Speeds (RPM): fan-1: 1800 fan-2: 1800</pre>
-S	Выводит информацию о системе: имя хоста, ядро, окружение рабочего стола, дистрибутив. С ключами -xx также показывает DM

Окончание таблицы 104

Ключ	Описание
-t	<p>Выводит процессы:</p> <p>-t c – только процессор; -t m – только память; -t cm – процессор/память (по умолчанию).</p> <p>Если указано число, показывает данное количество процессов для каждого типа (по умолчанию 5).</p> <pre>\$ inxi -t cm3 Processes: CPU top: 3 of 348 1: cpu: 27.6% command: virtualboxvm pid: 7152 2: cpu: 17.3% command: virtualboxvm pid: 5544 3: cpu: 7.3% command: x pid: 2700 System RAM: available: 38.88 GiB used: 10.21 GiB (26.3%) Memory top: 3 of 348 1: mem: 1376.0 MiB (3.4%) command: virtualboxvm pid: 5544 2: mem: 1306.8 MiB (3.2%) command: virtualboxvm pid: 7152 3: mem: 808.8 MiB (2.0%) command: telegram pid: 5163</pre>
-u	<p>Выводит UUID разделов. Для отображения меток разделов следует использовать с ключами -j, -o, -p и -P. Если ни один из этих ключей не указан, ничего не выводит</p>
-v	<p>Задаёт уровень детализации. Если номер уровня детализации не указан, предполагается значение 0. Не следует использовать с -b или -F. Поддерживаются уровни 0 – 8:</p> <p>0 – вызов inxi без параметров; 1 – базовый уровень, включает: -s + базовая информация о центральном процессоре (ЦП) + -G + базовая информация о дисках + -I; 2 – включает информацию: о сетевых устройствах (-N), информацию о машине (-M), данные батареи (-B). То же самое, что и inxi -b; 3 – включает: данные о ЦП (-C), данные батареи (-B), сетевые устройства (-n) (тоже, что и -x); 4 – включает основную информацию о разделах (-P) для /, /home, /var/, /boot. Показывает полную информацию о жестких дисках (-D); 5 – включает: информацию об аудиоустройствах (-A), данные от датчиков (-s), RAM (-m), информацию о bluetooth, метки разделов (-l), все активные типы подкачки (-j), UUID (-u), информацию об оптических устройствах, данные RAID; 6 – включает полную информацию о всех смонтированных (-p) и не смонтированных разделах (-o), оптических устройствах (-d), USB (-J), RAID (тоже, что и -xx); 7 – включает локальные и WAN IP-адреса (-i), информацию о bluetooth, информацию о логических томах (-L), RAID, все данные CPU (тоже, что и -xxx); 8 – включает всю доступную информацию, репозитории (-r), процессы (-tcm), слоты PCI (--slots).</p> <pre>\$ inxi -v 7</pre>

Ключи можно комбинировать, если они не конфликтуют. Например:

```
$ inxi -AG
```

Graphics:

```
Device-1: Intel Alder Lake-UP3 GT2 [Iris Xe Graphics] driver: i915 v: kernel
```

```
Device-2: Syntek Integrated Camera driver: uvcvideo type: USB
```

```
Display: x11 server: X.Org v: 1.21.1.8 driver: X: loaded: modesetting
```

ЛКНВ.11100-01 90 03

```

unloaded: fbdev,vesa dri: iris gpu: i915 resolution: 1: 1920x1080~60Hz
2: 1920x1080~60Hz
API: OpenGL v: 4.6 Mesa 23.0.4 renderer: Mesa Intel Graphics (ADL GT2)
Audio:
Device-1: Intel Alder Lake PCH-P High Definition Audio
driver: sof-audio-pci-intel-tgl
API: ALSA v: k6.1.12-un-def-alt1 status: kernel-api
Server-1: PulseAudio v: 16.1 status: active

```

Для получения более подробных данных о различных параметрах можно использовать один или несколько ключей `-x` (всего три дополнительных уровня данных: `-x`, `-xx`, `-xxx`). Эти ключи можно добавить в любой список опций, например: `-bxx` или `-Sxxx`.

Для получения более технических параметров (параметров администратора) используется ключ `--admin` или `-a`.

Чтобы обеспечить базовую конфиденциальность и безопасность, `inxi` позволяет отфильтровывать такие данные, как MAC-адрес сетевой карты, серийные номера, IP-адрес WAN и LAN, домашний каталог пользователя. Для активации фильтрации используется ключ `-z`, например:

```

$ inxi -iz
Network:
Device-1: Intel Alder Lake-P PCH CNVi WiFi driver: iwlwifi
IF: wlp0s20f3 state: up mac: <filter>
IP v4: <filter> type: dynamic noprefixroute scope: global
IP v6: <filter> type: noprefixroute scope: global
IP v6: <filter> type: noprefixroute scope: global
IP v6: <filter> type: noprefixroute scope: link
Device-2: Intel Ethernet I219-V driver: e1000e
IF: enp0s31f6 state: up speed: 1000 Mbps duplex: full mac: <filter>
IP v4: <filter> type: dynamic noprefixroute scope: global
IP v6: <filter> type: noprefixroute scope: global
Message: Output throttled. IPs: 4; Limit: 10; Override: --limit [1-x;-1
all]
WAN IP: <filter>

```

Следующая команда проверяет зависимости и программы, которые требуются для работы `inxi`, а затем показывает, какие пакеты нужно установить, чтобы добавить поддержку каждой функции:

```
$ inxi --recommends
```

Пример использования цветовой темы с выводом детальной информации в файл для анализа, команда выполняется от администратора, так как не вся информация доступна пользователю:

```
# inxi -c2 -v8 > inxi.txt
```

17.18.2. Команда `glxinfo`

Команда `glxinfo` позволяет получить информацию о OpenGL и реализации GLX в Xwindows.

Установка пакета:

```
# apt-get install glxinfo
```

Примеры:

- краткий вывод:

```
$ glxinfo -B
```

- показать информацию об активной видеокарте:

```
$ glxinfo -B | grep 'Device:'  
Device: Mesa Intel(R) Graphics (ADL GT2) (0x46a8)
```

- получить информацию о поддержке OpenGL renderer:

```
$ glxinfo | grep rendering  
direct rendering: Yes
```

- посмотреть информацию по графике intel (NVIDIA):

```
$ glxinfo | grep OpenGL
```

- узнать версию сервер/клиент, версию драйвера:

```
$ glxinfo | grep version
```

- посмотреть количество памяти, доступное видеокарте:

```
$ glxinfo | egrep -i 'device|memory'  
egrep: warning: egrep is obsolescent; using grep -E  
Device: Mesa Intel(R) Graphics (ADL GT2) (0x46a8)  
Video memory: 39808MB  
Unified memory: yes
```

17.19. Xpra

Xpra – это инструмент, который запускает программы X11, обычно на удаленном хосте, и направляет их отображение на локальный компьютер без потери состояния (позволяет отключение и повторное подключение без прерывания перенаправленного приложения).

Xpra может предоставить удаленный доступ, как к отдельным приложениям, так и к новым/существующим сеансам рабочего стола.

Хрга не имеет root-доступа: т.е. приложения, перенаправленные хрга, отображаются на локальном рабочем столе как обычные окна, управляемые локальным оконным менеджером. Хрга также использует собственный протокол, который самонастраивается и относительно нечувствителен к задержкам.

На сервере утилита Хрга запускает в режиме демона нужную программу с заданным идентификатором сеанса, а на клиенте происходит присоединение к сеансу с этим идентификатором.

Доступ к сеансам можно получить по SSH или через защищенные паролем сокетом TCP (с SSL или без).

17.19.1. Установка

Для установки на сервере и на клиенте выполните команду:

```
# apt-get install xpra
```

Можно использовать клиент `html5`, и в этом случае на клиенте ничего устанавливать не нужно. А на сервере, начиная с хрга версии 4.4.4, нужно дополнительно установить пакет `xpra-html5`:

```
# apt-get install xpra-html5
```

17.19.2. Режимы работы

17.19.2.1. Запуск приложения

Запуск приложения или бесшовный режим (`seamless`) – позволяет пересылать клиенту отдельные окна приложений, эти окна появляются на рабочем столе клиента так же, как и другие локальные приложения.

Все операции по управлению окнами выполняются непосредственно клиентской ОС или оконным менеджером, поэтому любые задержки между клиентом и сервером не мешают действиям по управлению окнами (сворачивание, перемещение, изменение размера окна).

Пример запуска приложения `xterm` удаленно, через SSH, без предварительного запуска хрга на сервере:

```
$ xpra start ssh://user@192.168.0.101 --start="xterm"
```

Примечание. Хрга и запускаемое приложение должны быть установлены на сервере.

Вместо параметра `--start=команда`, можно использовать параметр `--start-child=команда`, позволяющий учитывать параметр `--exit-with-children`. Если параметр `--exit-with-children=yes`, то сервер `xpra` будет отслеживать состояние дочерних элементов, запущенных `--start-child`, и автоматически завершится, когда последний из них завершит работу.

Запуск приложения, с предварительным запуском сервера `xpra`:

1) на сервере: запустить экземпляр сервера `xpra`, автоматически выбрать дисплей и запустить программу (например, `xterm`) на этом виртуальном дисплее:

```
$ xpra start --start=xterm
Entering daemon mode; any further errors will be reported to:
'/run/user/500/xpra/1/server.log'
```

2) с клиента подключиться к этому экземпляру сервера:

```
$ xpra attach ssh://user@192.168.0.101/1
```

Локальное подключение:

- запустить экземпляр сервера `xpra` на дисплее 101 (или автоматически выбрать дисплей) и запустить программу (например, `firefox`) на этом виртуальном дисплее:

```
$ xpra start :101 --start=firefox
Entering daemon mode; any further errors will be reported to:
'/run/user/500/xpra/101/server.log'
```

- подключиться к этому экземпляру сервера:

```
$ xpra attach :101
```

Подключение с использованием сокетов TCP:

- запустить экземпляр сервера `xpra`:

```
$ xpra start --start=xterm --bind-tcp=0.0.0.0:10000
Entering daemon mode; any further errors will be reported to:
'/run/user/500/xpra/S9454/server.log'
Actual display used: :1
Actual log file name is now: '/run/user/500/xpra/1/server.log'
```

- подключиться к серверу, используя выбранный порт:

```
$ xpra attach tcp://192.168.0.109:10000
```

ВНИМАНИЕ!

Использование параметра `--bind-tcp` без использования параметра `tcp-auth` не рекомендуется и представляет серьезную угрозу безопасности (особенно при `0.0.0.0`), т. к. кто угодно может подключиться к этому порту и получить доступ к сеансу. Доступ к сеансам Xpra в режиме TCP и `websocket` можно защитить, используя аутентификацию и шифрование.

17.19.2.2. Запуск новой графической сессии

Режим рабочего стола (`desktop`) позволяет запустить вложенный сервер X11.

Запуск приложения:

```
$ xpra start-desktop --start=firefox
```

Та же команда, но с запуском сеанса и подключением к нему со стороны клиента:

```
$ xpra attach ssh://user@10.81.1.130/2
```

Где 2 номер дисплея.

Чтобы запустить оконный менеджер (WM) или среду рабочего стола (DE) достаточно в примере выше заменить команду `xterm` командой, которая запускает WM или DE, например:

```
$ xpra start-desktop ssh://user@192.168.0.99 --exit-with-children --start-child=mate-session
```

Подключение:

```
$ xpra attach ssh://user@192.168.0.154:101 --min-size=1200x800 --clipboard-direction=both --clipboard=yes --opengl=no
```

Примечание. Чтобы сеанс завершился при выходе из WM, следует использовать `--start-child` и `--exit-with-children`.

17.19.2.3. Получение управления запущенной графической сессией (shadow режим)

Этот режим позволяет использовать `xpra` для удаленного доступа к существующему сеансу рабочего стола (обычно подключенному к реальному физическому дисплею).

Примечание. Shadow режим поддерживается на всех платформах, включая MS Windows и Mac OS X, но не на Wayland. В некоторых случаях, использование этого режима, может вызвать высокую нагрузку на процессор как на сервере, так и на клиенте. На большинстве платформ затеняемый дисплей должен быть активен: не заблокирован и не выключен.

Если к машине, к дисплею X11 которой нужно получить удаленный доступ, есть SSH-доступ, можно на клиенте запустить команду:

```
$ xpra shadow ssh://user@HOST/
```

В результате выполнения этой команды будет произведено подключение по SSH к HOST, запущен теневой сервер xpra и произведено подключение к нему. Теневой сервер будет остановлен после отключения.

При этом на сервере в трее появится значок («Exit» – остановить сервер, «Read Only» – запретить управление, только просмотр рабочего стола) (рис. 576).

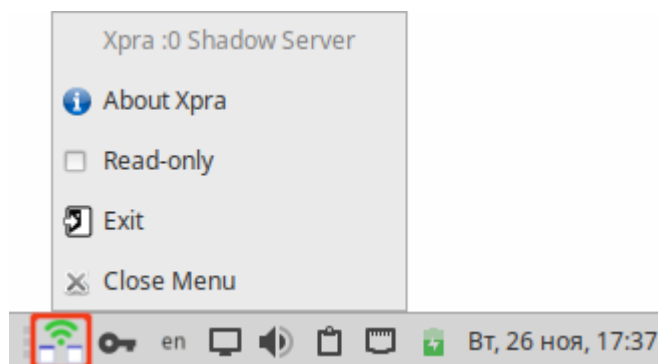


Рис. 576 – Значок Xpra

Если запуск через SSH не поддерживается или нужно запустить теневой сервер вручную и, возможно, настроить дополнительные параметры, можно запустить его из оболочки. Пример запуска управления запущенной графической сессией через TCP-сокеты:

```
$ xpra shadow :0 --bind-tcp=0.0.0.0:9876
```

17.19.3. Использование

17.19.3.1. Некоторые команды xpra

Некоторые команды xpra приведены в таблице 105.

Т а б л и ц а 105 – Команды xpra

Команда	Описание	Пример
xpra start	Запустить новый сервер xpra (при запуске удаленного сервера со строкой подключения ssh://HOST/DISPLAY новый сеанс также будет присоединен)	\$ xpra start :7 \$ xpra start --start=gimp
xpra start-desktop	Запустить вложенный сервер X11, все дочерние команды будут запускаться на вложенном сервере X11	\$ xpra start-desktop --start=xfce4-session
xpra attach	Подключиться к работающему серверу xpra. Любые приложения, использующие этот сервер, будут перенаправляться на текущий экран	\$ xpra attach :7 \$ xpra attach ssh://user@test/7
xpra detach	Отсоединить данный дисплей xpra	\$ xpra detach :7
xpra screenshot	Сделать снимок экрана и сохранить его в файле с указанным именем (снимки экрана можно делать только при подключенном клиенте)	\$ xpra screenshot my.jpg
xpra version	Вывести версию сервера	\$ xpra version 4.4.4-r0
xpra info	Вывести версию, статус и статистику	
xpra top	Отобразить ключевые атрибуты работоспособности сервера	
xpra control	Изменить параметры запущенного сервера. Список команд можно получить, указав «help» в качестве команды (например, xpra control :1 help)	\$ xpra control :1 min-quality 20
xpra stop	Подключиться к работающему серверу xpra и запросить его немедленное завершение. Обычно это приводит к тому, что любые приложения, использующие этот сервер, также прекращают работу	
xpra exit	Подключиться к работающему серверу xpra и запросить его немедленное завершение. В отличие от команды xpra stop, процесс Xvfb и его клиенты X11 (если таковые имеются) останутся запущенными	
xpra showconfig	Вывести конфигурацию xpra. В качестве дополнительных аргументов можно указать определенные параметры, или использовать специальное значение all, чтобы отобразить все параметры	\$ xpra showconfig clipboard-direction clipboard-direction = 'both'
xpra list	Вывести список всех серверов xpra, запущенные текущим пользователем на текущей машине	
xpra shadow	Предоставить доступ к рабочему столу (существующему дисплею X11). Если активен только один дисплей X11 и его номер меньше 10, он может быть обнаружен автоматически. Для этого режима работы настоятельно рекомендуется использовать видеокодек (h264 или vp8)	

Окончание таблицы 105

Команда	Описание	Пример
xpra проху	Позволяет одному серверу проксировать соединения для нескольких других, потенциально выступая в качестве точки входа для балансировки нагрузки или аутентификации для многих сеансов. Прокси-сервер будет создавать новый процесс для каждого прокси-соединения, этот прокси-процесс создаст неаутентифицированный новый сокет домена unix, который можно использовать с подкомандами info, version и stop	

17.19.3.2. Строка подключения

Локальный дисплей (только для локальных дисплеев локального пользователя):

```
:DISPLAY
```

Подключение с использованием SSH:

```
ssh://[USERNAME[:PASSWORD]@]HOST[:SSH_PORT]/[DISPLAY][?QUERYSTRING]
```

QUERYSTRING можно использовать для указания прокси-сервера

```
ssh: ?proxy=ssh://[ИМЯ ПОЛЬЗОВАТЕЛЯ[:ПАРОЛЬ]@]HOST[:SSH_PORT].
```

В этом случае xpra установит SSH-соединение с указанным «прокси-сервером» и с этого хоста xpra установит SSH-соединение с сервером xpra.

Для обратной совместимости режим SSH также поддерживает синтаксис:

```
ssh:[USERNAME[ PASSWORD]@HOST:DISPLAY
```

Пароль нужно указывать только тогда, когда он требуется модулю аутентификации сервера.

Примечание. При подключении по ssh может потребоваться указать системный ssh-клиент:

```
$ xpra start --ssh=ssh ssh://user@192.168.0.101 --start=scratch-desktop
```

Или дописать в файл ~/.xpra/xpra.conf строку:

```
ssh = ssh
```

В режиме TCP используются номера портов, а не номера дисплеев. Если через один TCP-порт доступно несколько дисплеев (например, при использовании прокси-сервера), то можно также указать номер дисплея:

```
tcp://[USERNAME@]HOST:PORT[/DISPLAY]
```

Режим SSL (добавляет безопасный уровень сокетов поверх режима TCP):

```
ssl://[USERNAME@]HOST:PORT[/DISPLAY]
```

Подключиться по протоколу websocket:

```
ws://[USERNAME[:PASSWORD]@]HOST:PORT/[DISPLAY]
```

Подключиться по защищенному протоколу websocket (websocket с SSL):

```
wss://[USERNAME[:PASSWORD]@]HOST:PORT/[DISPLAY]
```

17.19.3.3. Дисплей

При запуске xpra сервера (`xpra start`) можно не использовать номер дисплея, в этом случае он будет выбран автоматически. Номер дисплея будет указан в выводе команды, также его можно увидеть, выполнив команду `xpra list`.

В противном случае, при запуске сервера xpra может потребоваться указать номер дисплея. Для этого можно выбрать любое число и поставьте перед ним двоеточие (например, `:7`, `:12` и `:3117`). Нужно учитывать, что:

- каждый X или xpra сервер, работающие на одном хосте должны использовать уникальный номер дисплея;
- первые несколько цифр (0, 1, 2) обычно используются реальными X серверами.

При указании сервера xpra в клиентской программе (`xpra attach`, `xpra detach`, `xpra stop`, `xpra exit`, `xpra version`, `xpra info`, `xpra list`, `xpra screenshot`) можно использовать указание дисплея в формате `:DISPLAY` при подключении к локальному узлу или одну из форм `ssh://[USER@]HOST/DISPLAY` при подключении к удаленному узлу. Если на узле запущен только один сеанс xpra, то номер дисплея можно не указывать.

Если при запуске сервера был указан параметр `--bind-tcp`, `--bind-ssl`, `--bind-udp=[HOST]:PORT`, `--bind-ws`, `--bind-wss` или `--bind-vssock`, то к нему можно подключаться используя следующие строки:

```
tcp://HOST:PORT[/DISPLAY],
udp://HOST:PORT[/DISPLAY],
ssl://HOST:PORT[/DISPLAY],
ws://HOST:PORT[/DISPLAY],
wss://HOST:PORT[/DISPLAY] или vssock://HOST:PORT[/DISPLAY].
```

17.19.3.4. Сеть и аутентификация

Хрга поддерживает разные типы сетевых подключений (`tcp`, `ssl`, `ws`, `wss`, `vnc`, `ssh`, `vsock`, `quic` и т. д.), и большинство из них можно шифровать и мультиплексировать через один порт.

Безопасность зависит от типа подключения клиента `xpra` (`ssl`, `quic` и `ssh` считаются самыми безопасными, поскольку они обеспечивают проверку хоста и шифрование в одном протоколе).

Доступ к сеансам хрга через сокеты TCP можно защитить с помощью модулей аутентификации, но так как они не защищают само сетевое соединение от атак «человек посередине», то для защиты от таких атак можно использовать один из трех вариантов:

- шифрование AES;
- SSL;
- SSH.

17.19.3.4.1. Модули аутентификации

Примечание. При использовании для подключения к серверу SSH разделы шифрование и аутентификация можно пропустить (по умолчанию сокеты, используемые `ssh`, не используют аутентификацию).

Модули аутентификации приведены в таблице 106.

Т а б л и ц а 106 – Модули аутентификации

Модуль	Описание	Примечание
<code>allow</code>	Аутентификация всегда успешна (используется имя пользователя, предоставленное клиентом)	Небезопасно, и должно использоваться только для тестирования
<code>none</code>	Аутентификация всегда успешна (используется имя пользователя, под которым работает сервер)	Небезопасно, и должно использоваться только для тестирования
<code>fail</code>	Аутентификация всегда не успешна (пароль не запрашивается)	Полезно для тестирования
<code>reject</code>	Аутентификация всегда не успешна (пароль запрашивается)	Полезно для тестирования

Продолжение таблицы 106

Модуль	Описание	Примечание
env	Пароль сопоставляется с указанной переменной среды (по умолчанию XPRA_PASSWORD).	--auth=env:name=SOME_OTHER_ENV_VAR_NAME
password	Пароль сопоставляется с паролем, указанным с помощью опции value	--auth=password:value=mysecret
file	Сравнивает пароль с паролем, записанным в файле, указанным с помощью опции filename	--auth=file:filename=./password.txt Содержимое файла пароля будет рассматриваться как двоичные данные, ограничений на кодировку символов или размер файла нет. Следует остерегаться завершающих символов новой строки, которые будут включены в данные пароля (пример создания файла с паролем: echo -n "mypassword" > password.txt)
multifile	Сопоставляет имя пользователя и пароль с содержимым файла аутентификации, указанным с помощью опции filename	Файл аутентификации должен содержать учетные данные пользователей в формате: username password uid gid displays env_opts session_opts Имя пользователя и пароль не должны содержать символ вертикальной черты (), который используется в качестве разделителя. Этот модуль устарел, вместо него следует использовать sqlite
ram	Проверяет имя пользователя и пароль с помощью системы RAM	Аутентификация ОС Linux
win32	Проверяет имя пользователя и пароль с помощью win32security	Аутентификация MS Windows
sys	Системная аутентификация	Автоматически выбирает соответствующий системный модуль аутентификации (либо ram, либо win32)
sqlite, mysql, sql	Сверяет имя пользователя и пароль с файлом базы данных sqlite, указанным с помощью параметра filename (sqlite), или с базой данных, указанной с помощью параметра uri (mysql и sql)	Аутентификация будет обработана с использованием следующего запроса (настраивается с помощью параметра password_query): SELECT password FROM users WHERE username=(?) Сеансы, доступные для каждого пользователя, будут запрашиваться с помощью запроса (настраивается с помощью параметра session_query): SELECT uid, gid, displays, env_options, session_options FROM users WHERE username=(?)
exec	Делегирует процедуру аутентификации внешней команде. Команда указывается с помощью атрибута command	Команда должна вернуть 0, чтобы разрешить доступ, любое другое значение будет запрещать доступ
peercred	Аутентификация SO_PEERCREC	

Окончание таблицы 106

Модуль	Описание	Примечание
hosts	Проверяет хост с помощью системной библиотеки tcpwrappers	Подробнее см. в hosts.allow и hosts.deny
kerberos-password	Проверяет имя пользователя и пароль с помощью проверки подлинности Kerberos	Модуль не использует билеты Kerberos, и пароль будет отправлен на сервер в виде открытого текста. Следует использовать только для тестирования
kerberos-ticket	Проверяет билет Kerberos, полученный клиентом	
gss	Проверяет билет GSS, полученный клиентом	
u2f	Запрашивает у клиента токен U2F	
ldap	Проверяет имя пользователя и пароль на сервере LDAP, используя библиотеку python-ldap	
ldap3	Проверяет имя пользователя и пароль на сервере LDAP, используя библиотеку python-ldap3	

Предпочтительный способ указания аутентификации – в опции сокета.

Примеры:

```
$ XPRA_PASSWORD=mysecret
$ xpra start --start=xterm --bind-tcp=0.0.0.0:10000,auth=env

$ SOME_OTHER_ENV_VAR_NAME=mysecret
$ xpra start --bind-tcp=0.0.0.0:10000,auth=env:name=SOME_OTHER_ENV_VAR_NAME

$ xpra start --bind-tcp=0.0.0.0:10000,auth=password:value=mysecret

$ xpra start --bind-
tcp=0.0.0.0:10000,auth=file:filename=/path/to/mypasswordfile.txt

$ xpra start --bind-
tcp=0.0.0.0:10000,auth=sqlite:filename=/path/to/userlist.sdb
```

Разные сокеты могут использовать разные модули аутентификации:

```
$ xpra start --start=xterm -d auth \
--bind-tcp=0.0.0.0:10000,auth=hosts,auth=file:filename=password.txt --bind \
--bind-tcp=0.0.0.0:10001,auth=sys
```

17.19.3.5. Журналирование

Журналирование управляется опцией `--debug (-d)`.

Например, запуск сервера xpra с включенной отладкой фокуса:

```
$ xpra start -d focus --start=xterm
```

Список возможных категорий журналов можно получить, выполнив команду:

```
$ xpra -d help
```

Для записи в журнал событий всех категорий используется значение `all` (следует избегать применение этого значения, так как вывод будет очень подробным и сложным для восприятия).

Добавление к категории знака «-» отключает для данной категории ведение журнала. Например, регистрировать все категории, кроме `window` и `focus`:

```
$ xpra start :10 -d all,-window,-focus
```

Категорию журналирования также можно включить с помощью переменных среды. Это может потребоваться, если нет возможности изменить командную строку, или если регистрация должна происходить очень рано.

Например, включить отладку «геометрии» с помощью подкоманды `attach`:

```
XPRA_GEOMETRY_DEBUG=1 xpra attach
```

У запущенного сервера xpra можно изменить параметры журналирования с помощью подкоманды `control` (эту команду можно использовать как на сервере, так и на клиенте):

```
$ xpra control :DISPLAY debug enable CATEGORY
```

Сервер также может пересылать команды управления отладкой подключенным к нему клиентам:

```
$ xpra control :DISPLAY client debug enable geometry
```

Можно включить сразу несколько категорий:

```
$ xpra control :2 debug enable window geometry screen
```

Включить только регистраторы, которые соответствуют категориям с `+`:

```
$ xpra control :2 debug disable focus+grab
```

Конфиденциальная информация, такая как пароли и ключи обычно не отображается в журнале, но все же, используя журнал можно собрать достаточно данных, чтобы представлять реальную угрозу.

Хорошей превентивной мерой является отключение удаленного ведения журнала и выключение канала управления сервером.

`xpra shell` – это очень мощная функция отладки, которая обеспечивает полный доступ ко всем структурам данных, хранящимся на клиенте и сервере. По умолчанию эта функция отключена.

17.19.4. Клиент HTML5

Пример запуска экземпляра сервера:

```
$ xpra start --start=xterm --bind-tcp=0.0.0.0:10000 --html=on
```

Или:

```
$ xpra start --start=xterm --bind-ws=0.0.0.0:10000
```

Теперь можно получить доступ к этому сеансу в веб-браузере (рис. 577).

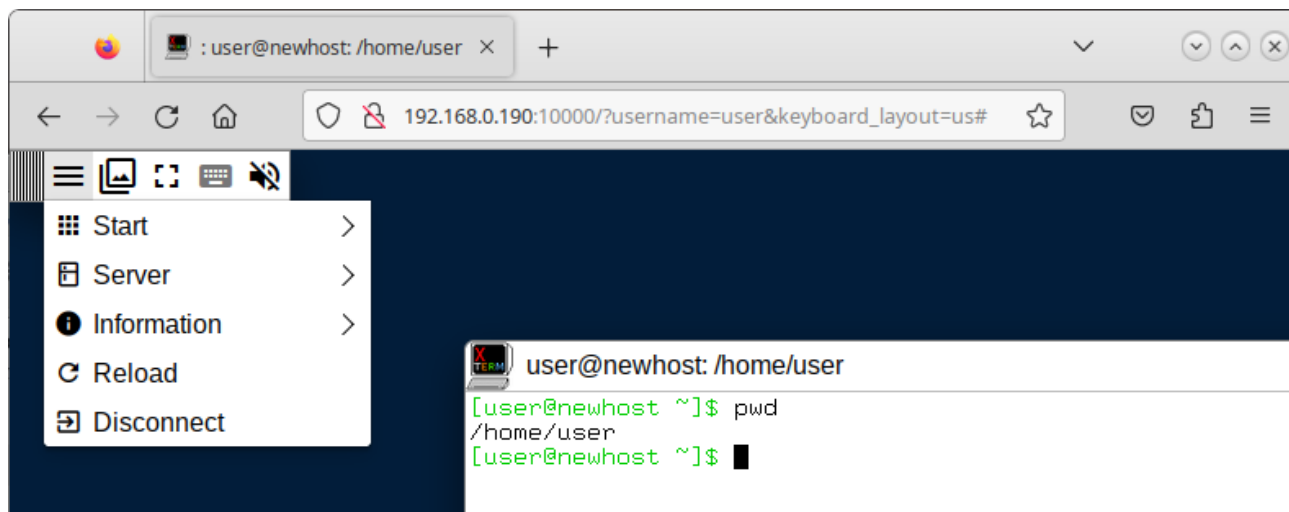


Рис. 577

Параметры подключения можно указать с помощью диалоговой формы подключения (<http://host:port/connect.html>) или указать как параметры URL, например: http://192.168.0.99:10000/?username=user&keyboard_layout=us.

Значения по умолчанию можно указать в файле:

```
/etc/xpra/html5-client/default-settings.txt.
```

Описание параметров подключения приведены в таблице 107.

Т а б л и ц а 107 – Описание параметров подключения

Параметр	Описание
Параметры подключения	
server	Имя хоста или IP-адрес хрга-сервера
port	Номер порта хрга-сервера
username	Аутентификация на сервере
password	Аутентификация на сервере
ssl	Включить SSL-соединение с сервером хрга
insecure	Разрешить отправку паролей по незашифрованным соединениям (No)
path	Путь WebSocket для подключения (обычно не требуется)
display	Дисплей для подключения (для прокси-серверов)
password	Аутентификация на сервере
encryption	Для включения шифрования, следует указать AES-CBC, AES-CTR или AES-CFB
key	Ключ шифрования AES
sharing	Разрешить другим клиентам подключаться к тому же сеансу (No)
steal	Взять на себя управление сеансом и отключить всех существующих клиентов (Yes)
reconnect	Автоматически переподключаться при обрыве соединения (Yes)
bandwidth_limit	Бюджет пропускной способности в битах в секунду (0 – без ограничений)
override_width	Ширина рабочего стола клиента, ширина окна веб-браузера в пикселях (по умолчанию – ширина окна веб-браузера)
Функции	
keyboard	Включить ввод с клавиатуры
keyboard_layout	Раскладка клавиатуры, которую будет использовать клиент (по умолчанию язык веб-браузера)
clipboard	Включить общий доступ к буферу обмена.
printing	Включить переадресацию принтера
file_transfer	Включить передачу файлов
swap_keys	Поменять местами клавиши Command и Control
scroll_reverse_x	Реверс оси X указателя мыши
floating_menu	Показывать плавающее меню
toolbar_position	Положение панели инструментов по умолчанию (например, top, top-right)
autohide	Скрыть большую часть панели инструментов до наведения на нее указателя
sound	Переадресация звука с сервера («выход динамика»)
video	Разрешить использование программного декодирования видео
Дополнительные параметры	
audio_codec	Используемый аудиоформат (detected)
encoding	Кодировка изображения, например, png, jpeg, webp и т. д. (auto)
remote_logging	Отправлять важные события на сервер
action	Режим подключения, например, start, shadow (connect)
shadow_display	Дисплей, если action=shadow
submit	Показать диагностику при отключении
start	Запустить сервер
exit_with_children	Завершить сессию, когда завершается последняя команда запуска (при запуске нового сеанса)
exit_with_client	Завершить сеанс при закрытии соединения (при запуске нового сеанса)

Значения параметров `server`, `port` и `ssl` отражают соединение, которое использовалось для загрузки клиента HTML5 (то, что указано в строке URL-адреса веб-браузера), и эти значения обычно не нужно изменять.

Примечание. Если в окне клиента при вводе с клавиатуры ничего не происходит, попробуйте изменить раскладку клавиатуры (параметр `keyboard_layout`).

17.19.5. Графический интерфейс

Графический интерфейс хпра («Меню» → «Приложения» → «Интернет» → «Хпра») (рис. 578).

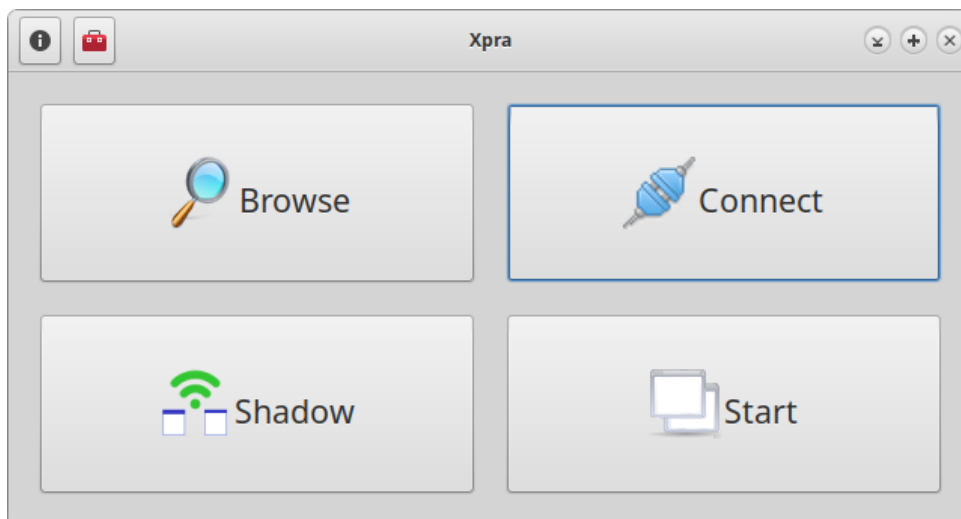


Рис. 578

«Browse» – просмотреть список и подключиться к локальному дисплею (рис. 579).

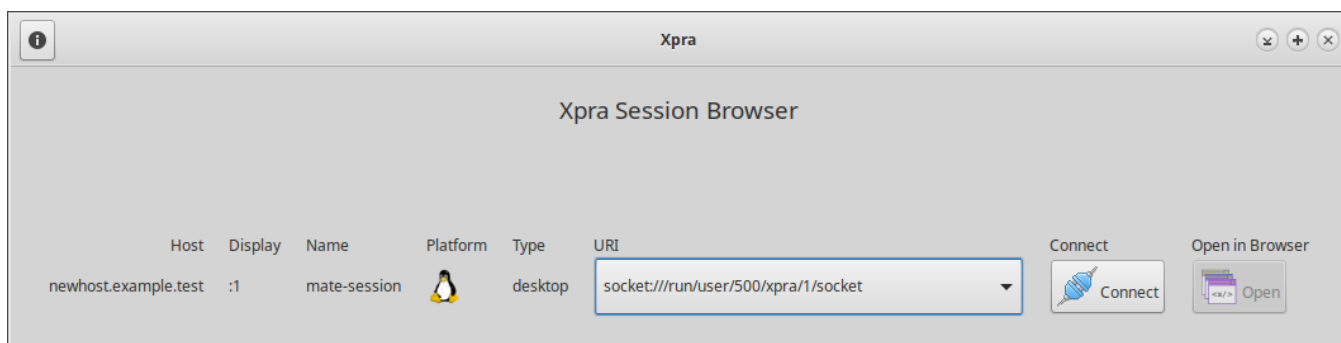


Рис. 579

«Connect» – подключиться к удаленному серверу (рис. 580).

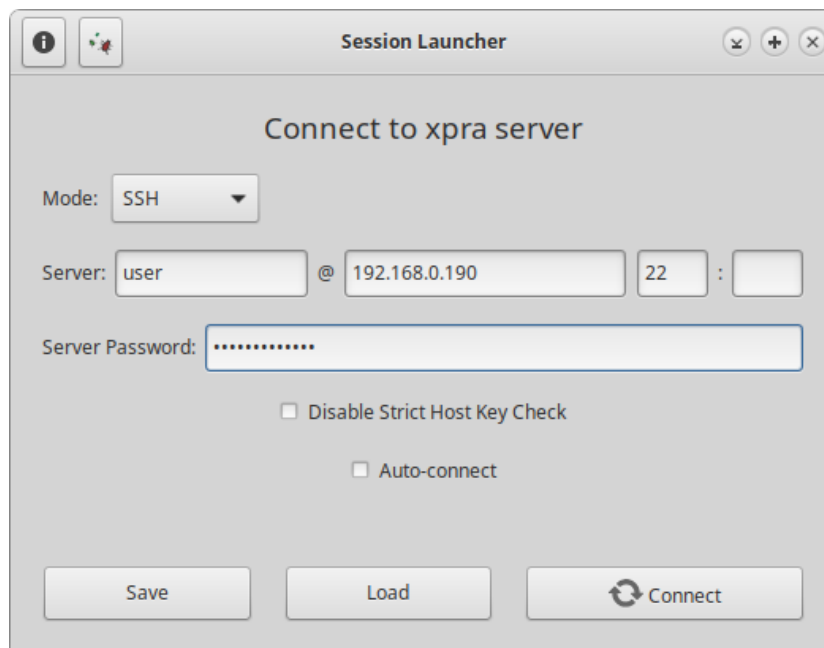


Рис. 580

«Shadow» – предоставить доступ к рабочему столу.

«Start» – запустить сервер xpra (рис. 581).

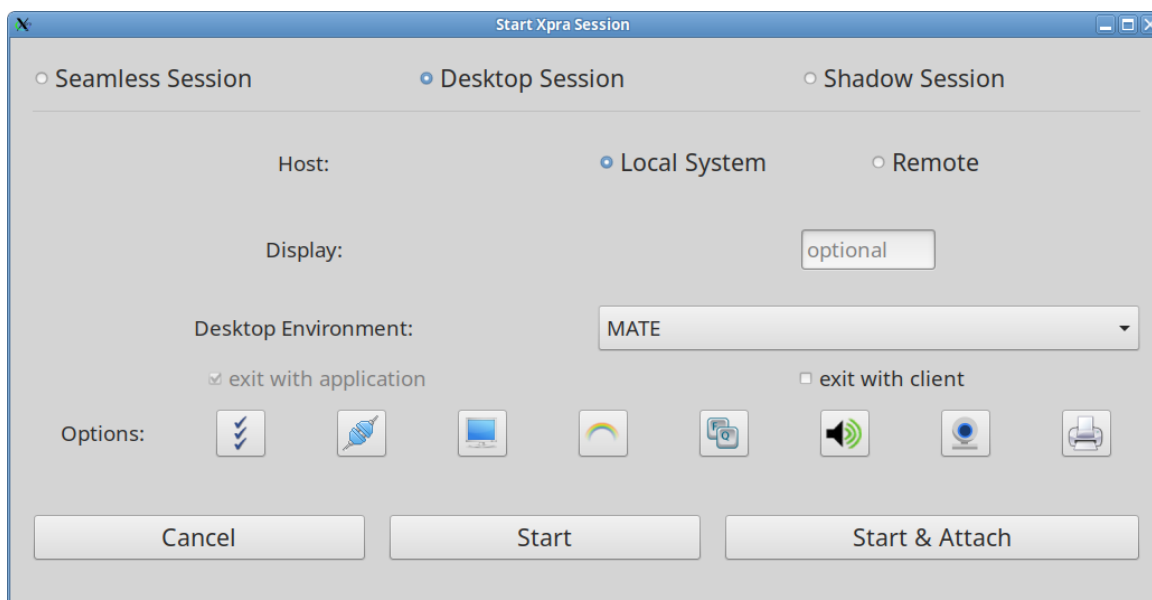


Рис. 581

Для организации полноценной инфраструктуры виртуальных рабочих столов (VDI) доступен OpenUDS, см. документ «Руководство администратора. Виртуализация и контейнеризация. ЛКНВ.11100-01 92 02».

17.20. Установка корневого сертификата

Для поддержки работы сайтов с российскими сертификатами и установки комплекта корневых сертификатов СА России достаточно установить пакет `ca-certificates-digital.gov.ru`:

```
# apt-get install ca-certificates-digital.gov.ru
```

В результате в хранилище доверенных сертификатов должны появиться сертификаты «Russian Trusted Root CA» и «Russian Trusted Sub CA»:

```
$ trust list |grep "Russian Trusted" -B 2 -A 2
```

```
pkcs11:id=%E1%D1%81%E5%CE%5A%5F%04%AA%D2%E9%B6%9D%66%B1%C5%FA%AC%2C%87;  
type=cert  
  type: certificate  
  label: Russian Trusted Root CA  
  trust: anchor  
  category: authority  
--  
pkcs11:id=%D1%E1%71%0D%0B%2D%81%4E%6E%8A%4A%8F%4C%23%B3%4C%5E%AB%69%0B;  
type=cert  
  type: certificate  
  label: Russian Trusted Sub CA  
  trust: anchor  
  category: authority
```

Сертификаты «Russian Trusted Root CA» и «Russian Trusted Sub CA» в Firefox (рис. 582).

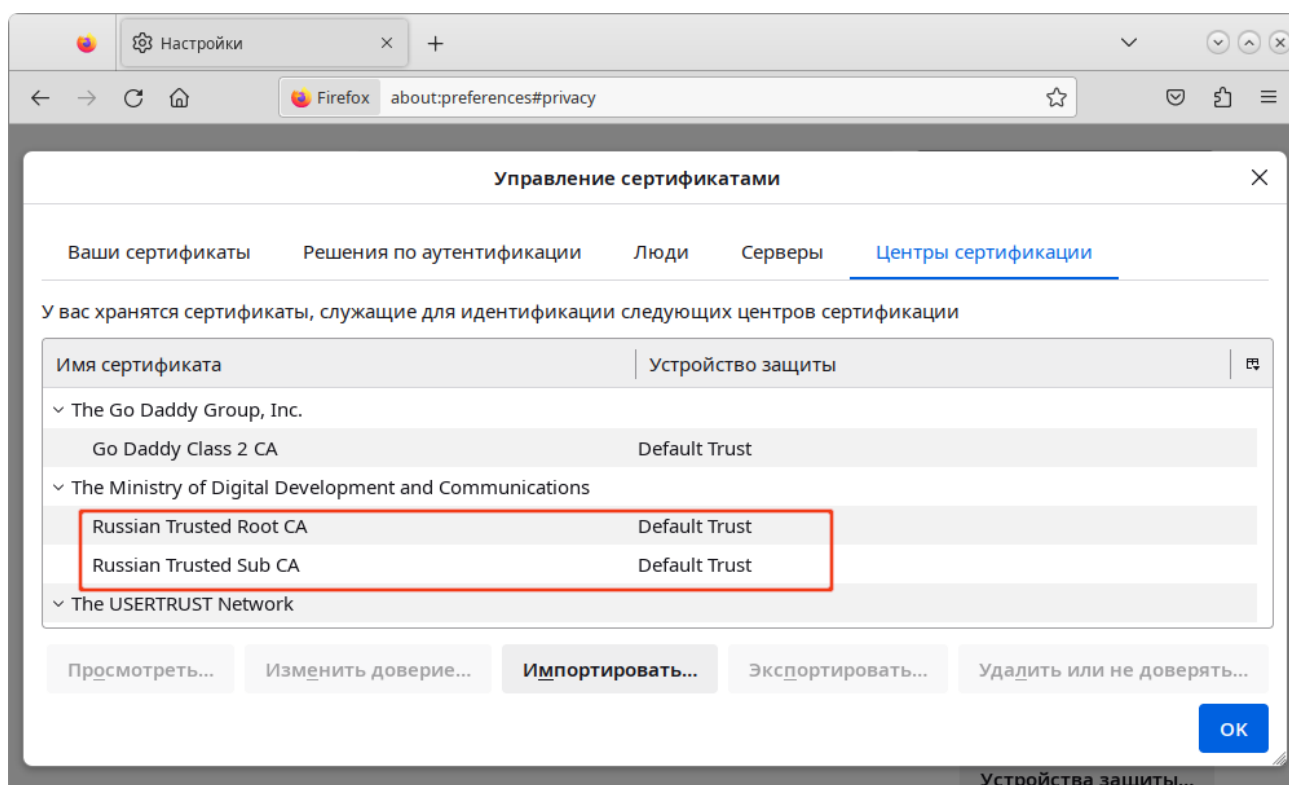


Рис. 582 – Корневые сертификаты СА России в Firefox

17.21. Выявление уязвимостей в образах контейнеров (trivy)

Trivy – сканер уязвимостей в образах контейнеров, файловых системах и репозиториях Git. Кроме того, trivy может находить ошибки в файлах конфигурации, жестко запрограммированные конфиденциальные данные, использование несовместимых лицензий в проекте.

Для установки утилиты следует выполнить команду:

```
# apt-get install trivy
```

17.21.1. Использование

Синтаксис команды trivy:

```
trivy <команда> [--scanners <сканер1,сканер2>] <цель>
```

Доступные команды:

- image (i) – сканировать образ контейнера;
- filesystem (fs) – сканировать локальную файловую систему;
- repository (repo) – сканировать git-репозиторий (удаленно);
- vm – сканировать образ виртуальной машины;
- kubernetes (k8s) – сканировать кластер кубернетес;
- aws – сканировать учетную запись AWS;
- config – сканировать файлы конфигурации;
- rootfs – сканировать rootfs;
- sbom – сканировать используемые пакеты ОС и программные зависимости (SBOM);
- completion – сгенерировать скрипт автозаполнения для указанной оболочки;
- module – управление модулями;
- plugin – управление плагинами;
- server – режим сервера;
- version – вывести версию.

Сканеры:

- vuln – известные уязвимости (CVE) (по умолчанию);
- config – проблемы с IAC и неправильные настройки;
- secret – конфиденциальная информация и секреты (по умолчанию);
- license – лицензии на программное обеспечение.

Для получения подробной информации о команде можно выполнить команду:

```
$ trivy <команда> --help
```

17.21.2. Примеры

17.21.2.1. Образы контейнеров

Сканирование образа контейнера на уязвимости:

```
$ trivy image alt:p10
```

Сканирование образа контейнера на наличие уязвимостей HIGH и CRITICAL с сохранением результата в формате JSON в файл:

```
$ trivy image --severity HIGH,CRITICAL -f json -o test.json alt:p10
```

Вывести проблемы с лицензиями:

```
$ trivy image --scanners license alt:p10
```

Проверка конфигурации только в метаданных образа контейнера:

```
$ trivy image --scanners vuln,misconfig --image-config-scanners  
misconfig alt:p10
```

Сканирование локального образа контейнера в Podman:

```
$ podman images
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
registry.altlinux.org/alt/nginx	latest	862baa6fbed9	3 months ago	136 MB
registry.altlinux.org/alt/alt	p10	ff2762c6c8cc	6 months ago	118 MB

```
$ trivy image ff2762c6c8cc
```

Примечание. Для возможности сканирования локальных образов, должен быть запущен podman.socket:

```
$ systemctl --user start podman.socket
```

17.21.2.2. Клиент/сервер

Trivy может работать в режиме клиент/сервер. На сервере Trivy хранится база данных уязвимостей, а клиенту Trivy не нужно ее загружать.

Запуск сервера:

```
$ trivy server --listen localhost:8081
```

Примечание. Для возможности подключения извне, необходимо вместо localhost указать 0.0.0.0 или IP-адрес сервера.

Удаленное сканирование образа:

```
$ trivy image --server http://192.168.0.169:8081 alt:p10
```

Удаленное сканирование файловой системы:

```
$ trivy fs --server http://localhost:8081 --severity CRITICAL ./
```

17.21.3. Локальная база данных Trivy

Пакет `trivy-db` содержит базу данных уязвимостей для Trivy. Базу данных Trivy, установленную из пакета, можно использовать только в клиент-серверном режиме (`trivy-server` должен быть запущен через `trivy.service`).

Для возможности использования локальной базы данных Trivy необходимо:

1) установить пакеты `trivy-db` и `trivy-server`:

```
# apt-get install trivy-db trivy-server
```

2) запустить сервер и добавить его в автозагрузку:

```
# systemctl enable --now trivy.server
```

Пример сканирования файловой системы, с использованием локальной базы данных (с машины, на которой запущен `trivy-server`):

```
$ trivy fs --server http://localhost:4954 ./
```

Пример сканирования файловой системы (с удаленной машины):

```
$ trivy fs --server http://192.168.0.169:4954 ./
```

где 192.168.0.169 – IP-адрес машины, на которой запущен `trivy-server`.

18. УПРАВЛЕНИЕ ПРОГРАММНЫМИ ПАКЕТАМИ

После установки ОС Альт СП при первом запуске доступен тот или иной набор ПО. Количество предустановленных программ зависит от набора программ конкретного дистрибутива или от выбора, сделанного при установке системы. Если интересующие программы не были обнаружены в системе, то имеется возможность доустановить их из разных источников.

Дополнительное ПО может находиться на установочном диске и (или) в специальных банках программ (репозиториях), расположенных в сети Интернет и (или) в локальной сети. Программы, размещенные в указанных источниках, имеют вид подготовленных для установки пакетов.

Для установки, удаления и обновления программ и поддержания целостности системы в ОС семейства Linux используются менеджеры пакетов типа «rpm». Для автоматизации этого процесса и применяется усовершенствованная система управления программными пакетами APT (Advanced Packaging Tool).

⚠ Перед установкой программ внимательно ознакомьтесь с п. 18.4 «Управление установкой (инсталляцией) компонентов программного обеспечения».

Автоматизация достигается созданием одного или нескольких внешних репозиториев, в которых хранятся пакеты программ и относительно которых производится сверка пакетов, установленных в системе. Репозитории могут содержать как официальную версию дистрибутива, обновляемую его разработчиками по мере выхода новых версий программ, так и локальные наработки, например, пакеты, разработанные внутри компании.

Таким образом, в распоряжении APT находятся две базы данных: одна описывает установленные в системе пакеты, вторая – внешний репозиторий. APT отслеживает целостность установленной системы и, в случае обнаружения противоречий в зависимостях пакетов, руководствуется сведениями о внешнем репозитории для разрешения конфликтов и поиска корректного пути их устранения.

Система АРТ состоит из нескольких утилит. Чаще всего используется утилита управления пакетами `apt-get`, которая автоматически определяет зависимости между пакетами и строго следит за их соблюдением при выполнении любой из следующих операций: установка, удаление или обновление пакетов.

18.1. Источники программ (репозитории)

18.1.1. Репозитории для АРТ

Репозитории, с которыми работает АРТ, отличаются от обычного набора пакетов наличием мета информации – индексов пакетов, содержащихся в репозитории, и сведений о них. Поэтому, чтобы получить всю информацию о репозитории, АРТ достаточно получить его индексы.

АРТ может работать с любым количеством репозиториях одновременно, формируя единую информационную базу обо всех содержащихся в них пакетах. При установке пакетов АРТ обращает внимание только на название пакета, его версию и зависимости, а расположение в том или ином репозитории не имеет значения. Если потребуется, АРТ в рамках одной операции установки группы пакетов может пользоваться несколькими репозиториями.

Подключая одновременно несколько репозиториях, нужно следить за тем, чтобы они были совместимы друг с другом по пакетной базе – отражали один определенный этап разработки. Совместимыми являются основной репозиторий дистрибутива и репозиторий обновлений по безопасности к данному дистрибутиву. В то же время смешение среди источников АРТ репозиториях, относящихся к разным дистрибутивам, или смешение стабильного репозитория с нестабильной веткой разработки (*Sisyphus*) чревато различными неожиданными трудностями при обновлении пакетов.

АРТ позволяет взаимодействовать с репозиторием с помощью различных протоколов доступа. Наиболее популярные – HTTP и FTP, однако существуют и некоторые дополнительные методы.

Для того чтобы АРТ мог использовать тот или иной репозиторий, информацию о нем нужно поместить в файл.

Файлы описания источников находятся в каталоге `/etc/apt/sources.list.d/` и имеют расширение `.list`, например:

```
altsp.list
sources.list
```

Так же, есть файл с предопределенным именем: `/etc/apt/sources.list`.

Утилита `apt-get`, в момент работы, просматривает одновременно все эти файлы.

Описания репозиториев заносятся в этот файл в следующем виде:

```
гpm [подпись] метод: путь база название
гpm-src [подпись] метод: путь база название
```

где:

- `гpm` или `гpm-src` – тип репозитория (скомпилированные программы или исходные тексты);
- `[подпись]` – необязательная строка-указатель на электронную подпись разработчиков. Наличие этого поля подразумевает, что каждый пакет из данного репозитория должен быть подписан соответствующей электронной подписью. Подписи описываются в файле `/etc/apt/vendors.list`;
- `метод` – способ доступа к репозиторию: `ftp`, `http`, `file`, `rsh`, `ssh`, `cdrom`, `copy`;
- `путь` – путь к репозиторию в терминах выбранного метода;
- `база` – относительный путь к базе данных репозитория;
- `название` – название репозитория.

Пример синтаксиса, описывающего источники приведен в п. 18.1.2.2.

Если первым символом идет символ комментария – строка считается простым текстом, а не описанием источника. У активной записи, в начале строки этот символ отсутствует.

Описание источника состоит из ключевых элементов:

- тип репозитория – применяется пакетная система `гpm` (все источники описывают `гpm`-репозитории);
- ключ подписи – пакеты в репозитории подписаны и могут быть проверены, если указать ключ. Списки доступных ключей хранятся в каталоге `/etc/apt/vendors.list` в файлах с расширением `.list`. Так же, есть файл `/etc/apt/vendors.list`. В примере использован ключ `[cert8]`;

- адрес – адрес расположения репозитория. Репозитории доступны несколькими способами (ftp://, http:// и rsync://). После описания способа доступа прописан адрес;
- тип данных – репозиторий может содержать как исполняемые пакеты, так и пакеты для разработчиков или пакеты с данными общего характера. Тип x86_64-i586 показывает, что в данном репозитории находятся исполняемые программы и библиотеки, собранные для 32-х разрядных систем (32bit). При использовании дистрибутива для 64-х разрядных процессоров, тип содержимого будет x86_64. В общем случае, запись источника с выполняемыми программами и библиотеками дополняет источник с типом noarch. Этот источник предоставляет пакеты, идентичные для обеих платформ x86. Как правило, это данные, небинарные библиотеки к Perl, Python и т. п.;
- название – название репозитория.

Для добавления в `sources.list` репозитория на CD/DVD-носителе информации в АРТ предусмотрена специальная утилита – `apt-cdrom`. Чтобы добавить запись о репозитории на носителе, достаточно вставить его в привод, например, для чтения (записи) CD (DVD)-носителей информации и выполнить команды создания директории, монтирования устройства, добавления носителя, указав актуальное имя устройства:

```
# mkdir /media/ALTLinux
# mount /dev/носитель /media/ALTLinux/
# apt-cdrom -m add
```

После этого в `sources.list` появится запись о подключенном диске примерно такого вида:

```
rpm cdrom:[ALT SP Workstation 10.2 11100-01 x86_64]/ ALTLinux main
```

После того как список репозитория в `sources.list` будет отредактирован, нужно обновить локальную базу данных АРТ о доступных пакетах, выполнив команду:

```
# apt-get update
```

В случае если в `sources.list` присутствует репозиторий, содержимое которого может изменяться, то прежде чем работать с АРТ, нужно синхронизировать локальную базу данных с удаленным сервером. Обновление данных осуществляется командой:

```
# apt-get update
```

Так происходит с любым постоянно разрабатываемым репозиторием, например, появляются обновления по безопасности (`updates`).

Локальная база данных создается заново каждый раз, когда в репозитории происходит изменение: добавление, удаление или переименование пакета. Для репозитория, находящегося на извлекаемых носителях информации и подключенных командой `apt-cdrom add`, синхронизация производится единожды в момент подключения.

При установке определенного пакета АРТ производит поиск самой новой версии этого пакета во всех известных ему репозиториях вне зависимости от способа доступа к ним.

Так, если в репозитории, доступном в сети Интернет, обнаружена более новая в сравнении с компакт-диском версия программы, то АРТ начнет загружать соответствующий пакет из сети Интернет.

Поэтому, если подключение к сети Интернет отсутствует или ограничено низкой пропускной способностью канала или высокой стоимостью, то следует закомментировать строчки (добавить в начало строки символ `#`) в `/etc/apt/sources.list`, относящиеся к ресурсам в сети Интернет.

18.1.2. Добавление репозитория с использованием терминала

18.1.2.1. Скрипт `apt-repo`

Для добавления репозитория можно воспользоваться скриптом `apt-repo`. Для выполнения большинства команд требуются права администратора.

Просмотреть список активных репозитория можно, выполнив команду:

```
apt-repo list
```

Для добавления репозитория в список активных репозиториях используется команда:

```
apt-repo add репозиторий
```

Для удаления или выключения репозитория используется команда:

```
apt-repo rm репозиторий
```

Для обновления информации о репозиториях необходимо выполнить команду:

```
apt-repo update
```

Для получения более подробной справки о команде можно выполнить команду:

```
man apt-repo
```

```
или apt-repo --help
```


18.1.2.2. Добавление репозитория вручную

Для редактирования списка репозиториях можно отредактируйте в любом текстовом редакторе файлы из каталога `/etc/apt/sources.list.d/` (см. п. 18.1.1). Нужны права администратора для изменения этих файлов.

В файле `altsp.list` может содержаться примерно такая информация:

```
$ cat /etc/apt/sources.list.d/altsp.list
# update.altsp.su (IVK, Moscow)

# ALT Certified 8
#rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTlinux
c10f2/branch/x86_64 classic
#rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTlinux
c10f/branch/x86_64-i586 classic
#rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTlinux
c10f2/branch/noarch classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTlinux
c10f2/branch/x86_64 classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTlinux
c10f2/branch/x86_64-i586 classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTlinux
c10f2/branch/noarch classic
```

 В файле `/etc/apt/sources.list.d/altsp.list` перечислены официальные источники программ для обновления ПИ, которые можно использовать для установки дополнительных программных пакетов с учетом ограничений лицензии на продукт.

По сути, каждая строчка соответствует некому репозиторию. Не активные репозитории – строки, начинающиеся с `#rpm`.

Для выключения репозитория достаточно закомментировать соответствующую строку (дописать символ решетки перед строкой). Для добавления нового репозитория необходимо дописать его вниз этого или любого другого файла.

После добавления репозитория необходимо обновить информацию о них, выполнив команду `apt-get update` или `apt-repo update`. Для выполнения этих команд нужны права администратора.

18.1.3. Программа управления пакетами Synaptic

Программа Synaptic также может использоваться для выбора репозитория, совместимого с дистрибутивом (рис. 583). Для указания конкретного репозитория в меню «Параметры» → «Репозитории» нужно отметить один из предлагаемых вариантов и нажать кнопку «ОК». К предложенному списку можно добавить репозитории, нажав на кнопку «Создать» и введя данные.

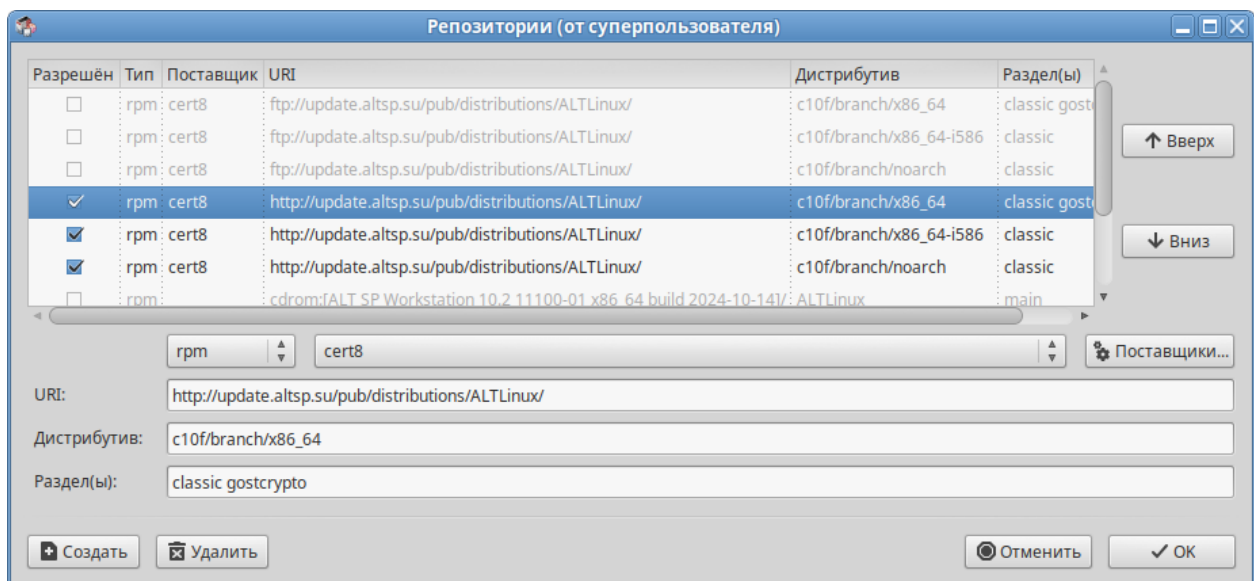


Рис. 583 – Пример списка репозитория

После выбора и добавления репозитория необходимо получить сведения о находящихся в них пакетах (кнопка «Получить сведения» или меню «Правка» → «Получить сведения о пакетах»). В противном случае, список доступных для установки программ будет не актуален.

18.2. Обновление информации о репозиториях в АРТ

Практически любое действие с системой АРТ начинается с обновления данных от активированных источников. Список источников нужно обновлять при поиске новой версии пакета, установке пакетов или обновлении установленных пакетов новыми версиями.

Обновление данных осуществляется командой:

```
# apt-get update
```

Программа загрузит данные с активированных источников в свой кеш.

Пример:

```
# apt-get update
```

```
Получено: 1 http://update.altsp.su c10f/branch/x86_64 release [3578B]
Получено: 2 http://update.altsp.su c10f/branch/x86_64-i586 release
[1033B]
```

```
Получено: 3 http://update.altsp.su c10f/branch/noarch release [2199B]
```

```
Получено 6810B за 5s (1292B/s).
```

```
Найдено http://update.altsp.su c10f/branch/x86_64/classic pkglist
```

```
Найдено http://update.altsp.su c10f/branch/x86_64/classic release
```

```
Найдено http://update.altsp.su c10f/branch/x86_64/gostcrypto pkglist
```

```
Найдено http://update.altsp.su c10f/branch/x86_64/gostcrypto release
```

```
Найдено http://update.altsp.su c10f/branch/x86_64-i586/classic pkglist
```

```
Найдено http://update.altsp.su c10f/branch/x86_64-i586/classic release
```

```
Найдено http://update.altsp.su c10f/branch/noarch/classic pkglist
```

```
Найдено http://update.altsp.su c10f/branch/noarch/classic release
```

```
Чтение списков пакетов... Завершено
```

```
Построение дерева зависимостей... Завершено
```

После выполнения этой команды, apt обновит свой кеш новой информацией.

18.3. Поиск пакетов (apt-cache)

Утилита apt-cache предназначена для поиска программных пакетов в репозитории, и позволяет искать не только по имени пакета, но и по его описанию.

Команда apt-cache search <подстрока> позволяет найти все пакеты, в именах или описании которых присутствует указанная подстрока. Пример поиска может выглядеть следующим образом:

```
$ apt-cache search ^gimp
```

```
gimp - The GNU Image Manipulation Program
```

```
libgimp - GIMP libraries
```

```
libgimp-devel - GIMP plugin and extension development kit
```

```
gimp-help-en - English help files for the GIMP
```

```
gimp-help-ru - Russian help files for the GIMP
```

```
gimp-plugin-separateplus - Improved version of the CMYK Separation
plug-in [...]
```

```
gimp-script-ISONoiseReduction - Gimp script for reducing sensor noise
[...]
```



```
gimp-plugin-gutenprint - GIMP plug-in for gutenprint
gimp-plugin-ufraw - GIMP plugin for opening and converting RAW files
[...]
```

Символ «^» в поисковом выражении, указывает на то, что нужно найти совпадения только в начале строки (в данном случае – в начале имени пакета).

Для того чтобы подробнее узнать о каждом из найденных пакетов и прочитать его описание, можно воспользоваться командой `apt-cache show`, которая покажет информацию о пакете из репозитория:

```
$ apt-cache show gimp-help-ru

Package: gimp-help-ru
Section: Graphics
Installed Size: 62888647
Maintainer: Valery Inozemtsev <shrek@altlinux.ru>
Version: 2.10.0-alt1:p10+286245.100.1.1@1633083328
Pre-Depends: rpmlib(PayloadIsXz)
Provides: gimp-help-ru (= 2.10.0-alt1:p10+286245.100.1.1)
Obsoletes: gimp-help-common (< 2.10.0-alt1)
Architecture: noarch
Size: 45251404
MD5Sum: 04b5c9d3b5bb3f33822761497f58c7cf
Filename: gimp-help-ru-2.10.0-alt1.noarch.rpm
Description: Russian help files for the GIMP
 Russian help files for the GIMP.
```

Команда `apt-cache` позволяет осуществлять поиск по русскому слову, однако в этом случае будут найдены только те пакеты, у которых есть описание на русском языке.

18.4. Управление установкой (инсталляцией) компонентов программного обеспечения

Установку пакетов может производить только администратор.

ВНИМАНИЕ!

Обновление пакетов выполняется при отсутствии нарушений целостности системы. Проверка целостности системы выполняется:

1) с помощью команды:

```
# integalert
```

При отсутствии изменений вывод команды: `integrity check OK`

2) или просмотром записей `osec` в системном журнале с помощью команды:

```
# journalctl | grep osec
```

При отсутствии изменений в записях журнала присутствует:

```
No changes[osec]
```

ВНИМАНИЕ!

Если в системе инициализированы средства контроля целостности IMA/EVM (должны быть инициализированы), то установка/обновление пакетов должны происходить с использованием команды `integrity-applier` (см. п. 18.4.1).

Подробнее информацию о контроле целостности см. в документе «Руководство по комплексу средств защиты. ЛКНВ.11100-01 99 03».

Если средства контроля целостности не используются, то обновление пакетов нужно производить в следующем порядке:

- 1) если используется `control++` (черные/белые списки), нужно выключить черные/белые списки, выполнив сброс текущего режима (просмотреть установленный режим можно, выполнив команду `control++ list`, активный режим будет дополнительно отмечен *):

```
# control++ --reset
```

- 2) установить пакеты/обновить систему при помощи `apt-get`;

- 3) включить установленный ранее режим черного/белого списка, выполнив команду (в зависимости от вывода в шаге 1)):

```
# control++ blacklist
```

или

```
# control++ wl
```

- 4) выполнить команду:

```
# integalert fix
```

18.4.1. Команда `integrity-applier`

Для того чтобы система сохранила все настройки безопасности установку/обновление пакетов нужно производить в следующем порядке:

- 1) войти в ОС и от администратора (`root`), выполнить команду отключения подсистемы IMA/EVM (если активирована):

```
# integrity-remover
```

Система будет перезагружена.

- 2) установить пакеты при помощи `apt-get` (см. п. 18.5) или обновить пакеты:

```
# apt-get update
```

```
# apt-get dist-upgrade
```

3) запустить инициализацию средств контроля целостности:

```
# integrity-applier -i
```

после выполнения данной команды будет запущен первый этап инициализации подсистемы IMA/EVM, в результате выполнения команды, система будет перезагружена;

4) после перезагрузки системы выполните авторизацию в терминале и получите права суперпользователя (root);

5) запустить второй этап инициализации подсистемы IMA/EVM – выполнить команду:

```
# integrity-applier -s
```

в результате выполнения команды, система будет перезагружена;

6) переименовать файл записи аудита /var/log/audit/audit.log:

```
# mv /var/log/audit/audit.log /var/log/audit/audit_old.log
```

7) выполнить запуск аудита:

```
# service auditd start
```

18.5. Установка или обновление пакета командой apt

Установка пакета с помощью АРТ выполняется командой:

```
# apt-get install имя_пакета
```

Перед установкой и обновлением пакетов нужно выполнить команду обновления индексов пакетов:

```
# apt-get update
```

Если пакет уже установлен и в подключенном репозитории нет обновлений для данного пакета, система сообщит об уже установленном пакете последней версии. Если в репозитории присутствует более новая версия или новое обновление – программа начнет процесс установки.

apt-get позволяет устанавливать в систему другие, пока еще не установленные пакеты, требуемые для работы. Он определяет, какие пакеты нужно установить, и устанавливает их, пользуясь всеми доступными репозиториями.

Установка пакета gimp командой apt-get install gimp приведет к следующему диалогу с АРТ:

```
# apt-get install gimp
Чтение списков пакетов... Завершено
```

ЛКНВ.11100-01 90 03

```

Построение дерева зависимостей... Завершено
Следующие дополнительные пакеты будут установлены:
icc-profiles libbabl libgegl libgimp libjavascriptcoregtk2 libopenraw
libspiro libwebkitgtk2 libwmf
Следующие НОВЫЕ пакеты будут установлены:
gimp icc-profiles libbabl libgegl libgimp libjavascriptcoregtk2
libopenraw libspiro libweb-kitgtk2 libwmf
0 будет обновлено, 10 новых установлено, 0 пакетов будет удалено и 0 не
будет обновлено.
Нужно получить 0В/24,6МВ архивов.
После распаковки потребуется дополнительно 105МВ дискового
пространства.
Продолжить? [Y/n] y
. . .
Получено 24,6МВ за 0s (44,1МВ/s).
Совершаем изменения...
Preparing... ##### [100%]
1: libbabl ##### [ 10%]
2: libwmf ##### [ 20%]
3: libjavascriptcoregtk2 ##### [ 30%]
4: libwebkitgtk2 ##### [ 40%]
5: icc-profiles ##### [ 50%]
6: libspiro ##### [ 60%]
7: libopenraw ##### [ 70%]
8: libgegl ##### [ 80%]
9: libgimp ##### [ 90%]
10: gimp ##### [100%]
Running /usr/lib/rpm/posttrans-filetriggers
Завершено.

```

Команда `apt-get install имя_пакета` используется и для обновления уже установленного пакета или группы пакетов. В этом случае `apt-get` дополнительно проверяет, не обновилась ли версия пакета в репозитории по сравнению с установленным в системе.

При помощи АРТ можно установить и отдельный бинарный rpm-пакет, не входящий ни в один из репозиториях. Для этого достаточно выполнить команду `apt-get install путь_к_файлу.rpm`. При этом АРТ проведет стандартную процедуру проверки зависимостей и конфликтов с уже установленными пакетами.

В результате операций с пакетами без использования АРТ может нарушиться целостность ОС Альт СП, и `apt-get` в таком случае откажется выполнять операции установки, удаления или обновления.

Для восстановления целостности ОС Альт СП нужно повторить операцию, задав опцию `-f`, заставляющую `apt-get` исправить нарушенные зависимости, удалить или заменить конфликтующие пакеты. Любые действия в этом режиме обязательно требуют подтверждения со стороны пользователя.

При установке пакетов происходит запись в системный журнал вида:

```
apt-get: имя-пакета installed
```

18.6. Удаление установленного пакета командой apt

Для удаления пакета используется команда `apt-get remove <имя_пакета>`.

Удаление пакета с сохранением его файлов настройки производится при помощи следующей команды:

```
# apt-get remove <значимая_часть_имени_пакета>
```

В случае, если при этом нужно полностью очистить систему от всех компонент удаляемого пакета, то применяется команда:

```
# apt-get remove --purge <значимая_часть_имени_пакета>
```

Для того чтобы не нарушать целостность системы, будут удалены и все пакеты, зависящие от удаляемого.

В случае удаления с помощью `apt-get` базового компонента системы появится запрос на подтверждение операции:

```
# apt-get remove filesystem
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие пакеты будут УДАЛЕНЫ:
[...]
ВНИМАНИЕ: Будут удалены важные для работы системы пакеты
Обычно этого делать не следует. Вы должны точно понимать возможные
последствия!
[...]
0 будет обновлено, 0 новых установлено, 1732 пакетов будет удалено и 1
не будет обновлено.
Необходимо получить 0В архивов.
После распаковки будет освобождено 5439МВ дискового пространства.
Вы делаете нечто потенциально опасное!
Введите фразу 'Yes, do as I say!' чтобы продолжить.
```

Каждую ситуацию, в которой АРТ выдает такое сообщение, нужно рассматривать отдельно. Однако, вероятность того, что после выполнения этой команды система окажется неработоспособной, очень велика.

При удалении пакетов происходит запись в системный журнал вида:

```
apt-get: имя-пакета removed
```

18.7. Альтернативная установка дополнительного ПО

Для установки дополнительного ПО можно использовать программу управления пакетами Synaptic.

⚠ Нельзя использовать одновременно два менеджера пакетов, так как это может привести к их некорректной работе.

18.7.1. Программа управления пакетами Synaptic

Запустить программу управления пакетами Synaptic можно, выбрав пункт «Меню МАТЕ» → «Приложения» → «Параметры» → «Программа управления пакетами Synaptic».

При запуске программы необходимо ввести пароль администратора системы.

Для облегчения поиска доступные для установки программы (Рис. 584) разделены на группы, выводимые в левой части окна программы. Справа расположен список самих программ с указанием их текущего состояния:

- синяя метка – пакет уже установлен;
- белая метка – пакет не установлен;
- синяя метка с восклицательным знаком – для установленного пакета имеется обновление.

При выборе пакета из списка в нижней части отображаются сведения о нем и его описание.

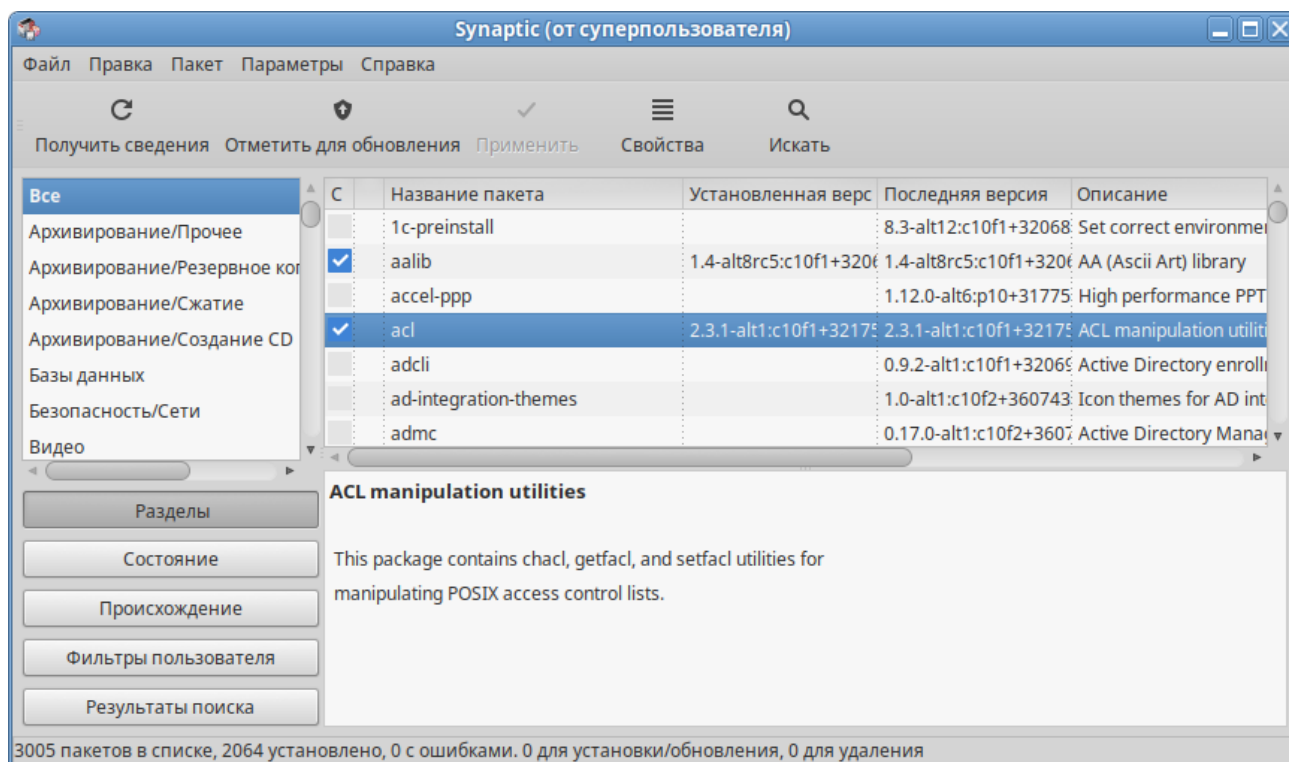


Рис. 584 – Программа управления пакетами Synaptic

Перед тем как устанавливать или обновлять пакет, нужно нажать на кнопку «Получить сведения» (или комбинацию клавиш <Ctrl>+<R>), для того чтобы скачать список самых последних версий ПО.

Для начала установки двойным щелчком мыши нужно отметить неустановленный пакет в правой половине окна и нажать на кнопку «Применить».

18.8. Обновление всех установленных пакетов apt-get

Полное обновление всех установленных в системе пакетов производится при помощи команды:

```
# apt-get dist-upgrade
```

Примечание. Команда `apt-get dist-upgrade` обновит систему, но ядро ОС не будет обновлено (см. п. 18.11).

В случае обновления всего дистрибутива АРТ проведет сравнение системы с репозиторием и удалит устаревшие пакеты, установит новые версии присутствующих в системе пакетов, отследит ситуации с переименованиями пакетов или изменения зависимостей между старыми и новыми версиями программ. Все, что потребуется поставить (или удалить) дополнительно к уже имеющемуся в системе, будет указано в отчете `apt-get`, которым АРТ предварит само обновление.

18.9. Обновление всех установленных пакетов Synaptic

Synaptic поддерживает два варианта обновления системы:

- интеллектуальное обновление (рекомендуется) – попытается разрешить конфликты пакетов перед обновлением системы. Действие интеллектуального обновления аналогично действию команды `apt-get dist-upgrade`;
- стандартное обновление – обновление обновит только те пакеты, которые не требуют установки дополнительных зависимостей.

По умолчанию Synaptic использует интеллектуальное обновление. Для того чтобы изменить метод обновления системы, нужно открыть диалоговое окно «Параметры» («Параметры» → «Параметры») и на вкладке «Основные» в списке «Обновить систему» выбрать требуемый способ.

Для обновления системы необходимо (рис. 585):

- 1) нажать на кнопку «Получить сведения» (или комбинацию клавиш <Ctrl>+<R>), для того чтобы скачать список самых последних версий ПО;
- 2) нажать на кнопку «Отметить для обновления» (или комбинацию клавиш <Ctrl>+<G>), для того чтобы Synaptic отметил доступные для обновления пакеты. При этом программа может вывести окно со списком вносимых изменений;
- 3) нажать на кнопку «Применить». Будет показан список изменений, который произойдет при обновлении пакетов. Тут следует обратить внимание на объем данных, который будет скачан из сети. После подтверждения Synaptic начнет загружать файлы, затем начнется непосредственно установка.

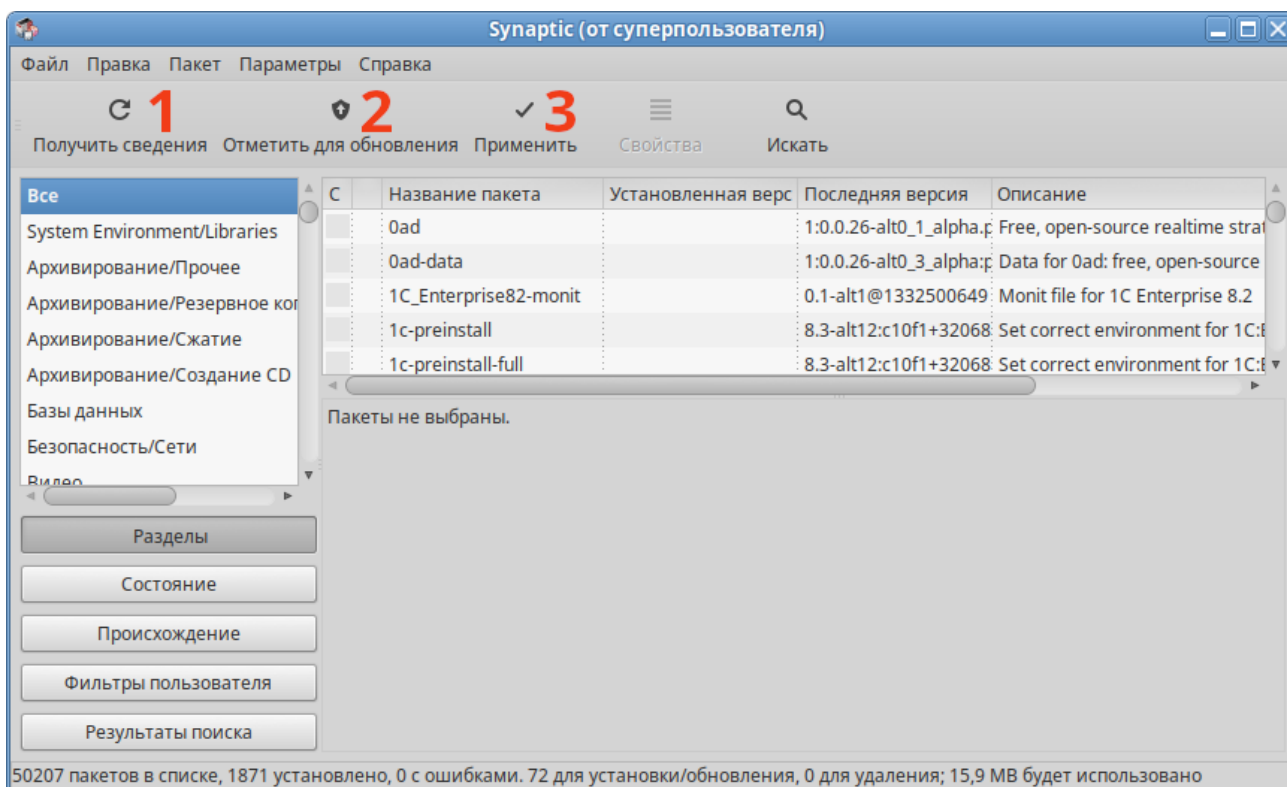


Рис. 585 – Обновление всех установленных пакетов

18.10. Обновление ядра и модулей ядра

18.10.1. В консоли

Для обновления ядра ОС используется команда:

```
# update-kernel
```


Примечание. Если индексы сегодня еще не обновлялись перед выполнением команды `update-kernel` нужно выполнить команду `apt-get update`.

Если нужно обновить/установить другой тип ядра, нужно выполнить команду:
`update-kernel -t <новый тип ядра>`

где <новый тип ядра> – `std-def`, `un-def` и т. п.

Примечание. Ключ `-t` и тип ядра (`std-def`, `un-def` и т. п.) следует указывать, только если нужно обновить ядро другого типа, так как по умолчанию обновляется текущий тип ядра. Узнать версию загруженного ядра можно командой:

```
$ uname -r
```

Новое ядро загрузится только после перезагрузки системы. Если с новым ядром что-то пойдет не так, можно будет вернуться к предыдущему варианту, выбрав его в начальном меню загрузчика.

После успешной загрузки на обновленном ядре можно удалить старые ядра, выполнив команду:

```
# remove-old-kernels
```

Команда `update-kernel` обновит и модули ядра, если в репозитории есть обновления модулей для текущего ядра.

Установка/обновление модулей ядра выполняется командой:

```
apt-get install kernel-modules-<модуль>-<тип ядра>
```

Например, для установки модуля LiME, если текущий тип ядра `un-def`, следует выполнить команду:

```
# apt-get install kernel-modules-LiME-un-def
```

Примечание. Перед установкой модулей ядра необходимо обязательно обновить ядро.

18.10.2. Графический инструмент обновления ядра

Модуль «Обновление ядра» (пакет `alterator-update-kernel`) реализует функционал утилиты `update-kernel`. Данный модуль предоставляет возможность:

- просматривать список установленных ядер;
- устанавливать, обновлять и удалять ядра;
- задавать ядро, загружаемое по умолчанию;
- устанавливать/удалять отдельные модули ядра.

Модуль «Обновление ядра» доступен как в графическом интерфейсе ЦУС (п. 7.1.1)(раздел «Система» → «Обновление ядра) (рис. 586), так и в веб-интерфейсе (п. 7.1.2) <https://ip-address:8080> (рис. 587).

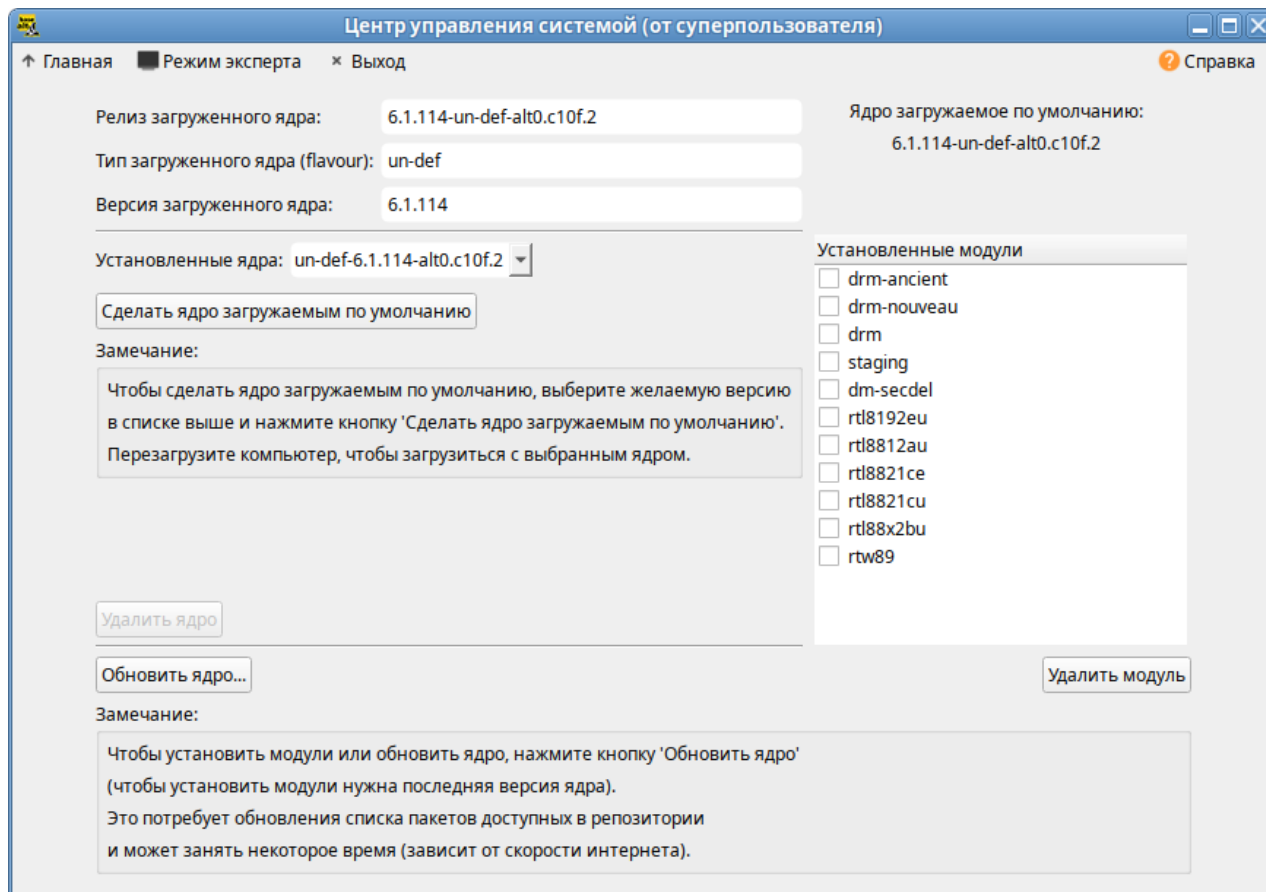


Рис. 586 – Интерфейс модуля «Обновление ядра»

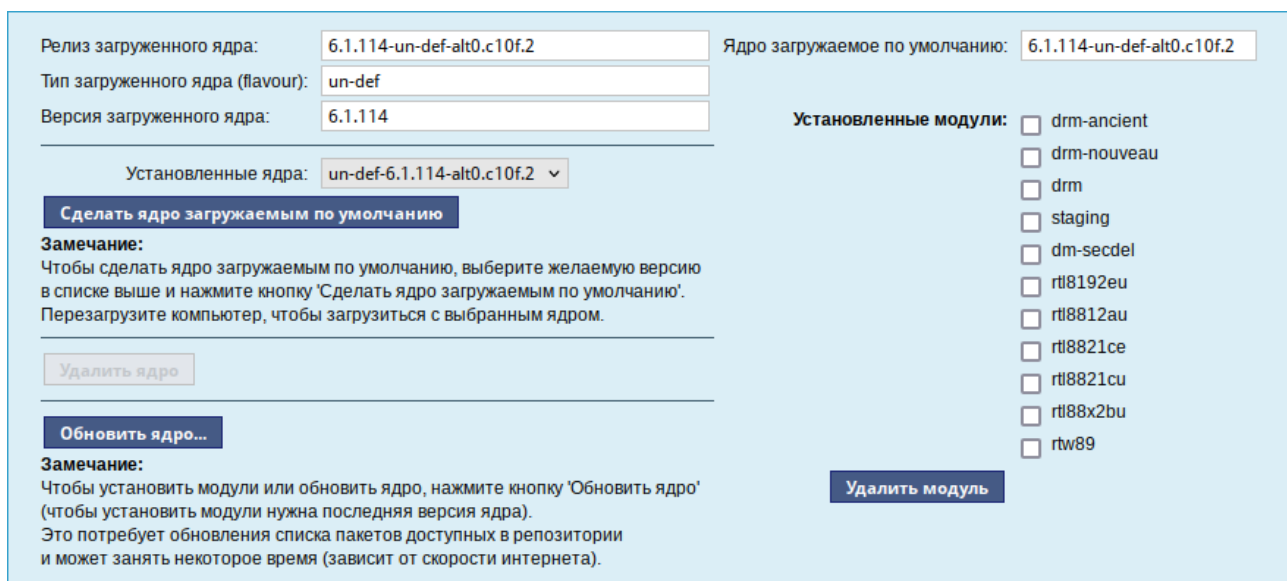


Рис. 587 – Веб-интерфейс модуля «Обновление ядра»

В главном окне модуля отображается ядро, загруженное по умолчанию, список установленных ядер (поле «Установленные ядра»), список установленных модулей ядра (поле «Установленные модули»).

18.10.2.1. Установка/обновление ядра и установка модулей ядра

При обновлении ядра, обновляются и модули ядра, но исходя из списка установленных для текущего ядра пакетов.

Примечание. Для установки модулей требуется последняя версия ядра.

Для того чтобы обновить ядро или установить модули ядра, нужно нажать кнопку «Обновить ядро...».

Примечание. При нажатии кнопки «Обновить ядро...» локальная база данных пакетов будет синхронизирована с удаленным репозиторием, это может занять некоторое время.

В открывшемся окне будет показано доступное к установке ядро или сообщение о том, что последнее ядро уже установлено в системе (рис. 588).

В выпадающем списке можно выбрать тип ядра. В окне «Доступные модули» отмечаются модули, которые будут установлены.

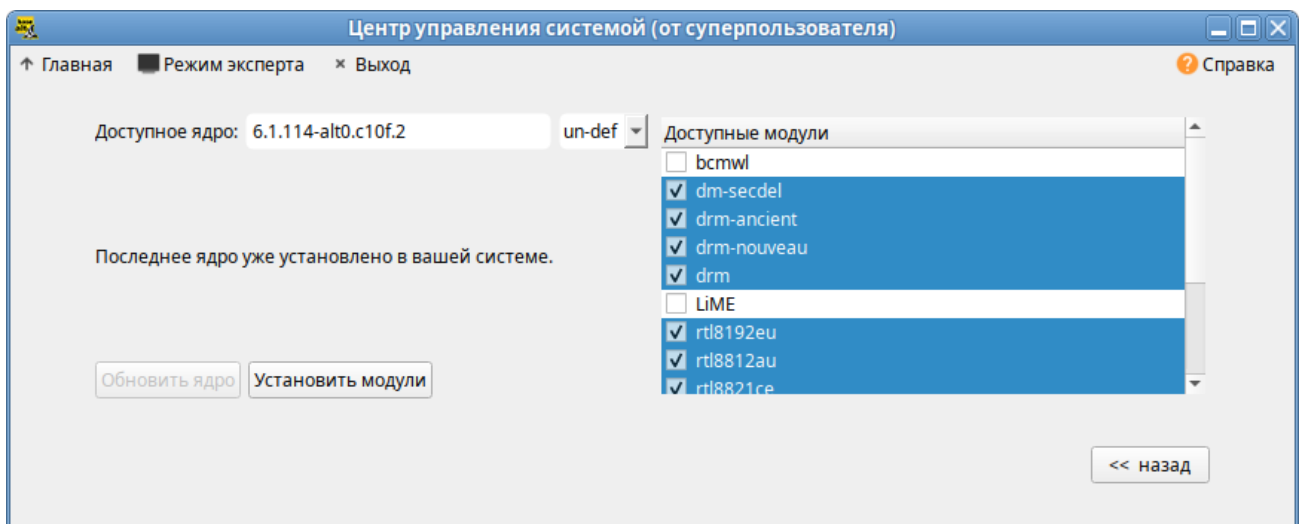


Рис. 588 – Доступное к установке ядро

Чтобы обновить ядро, нужно нажать кнопку «Обновить ядро». Откроется окно, в котором следует нажать кнопку «Да» для того, чтобы обновить ядро, или «Нет», чтобы отказаться от данного действия.

Установленное ядро станет загружаемым по умолчанию.

Если ядро не требует обновления, в окне «Доступные модули» можно отметить модули ядра, доступные к установке, и нажать на кнопку «Установить модули».

Новое ядро загрузится только после перезагрузки системы.

18.10.2.2. Сделать ядро загружаемым по умолчанию

В дистрибутиве можно установить несколько версий ядра одного и того же типа одновременно. После установки, или обновления ядра, старые ядра не удаляются. В случае возникновения проблем с новым ядром можно переключиться на ядро, установленное ранее.

Для этого следует выбрать нужное ядро в списке «Установленные ядра» (рис. 589) и нажать кнопку «Сделать ядро загружаемым по умолчанию».

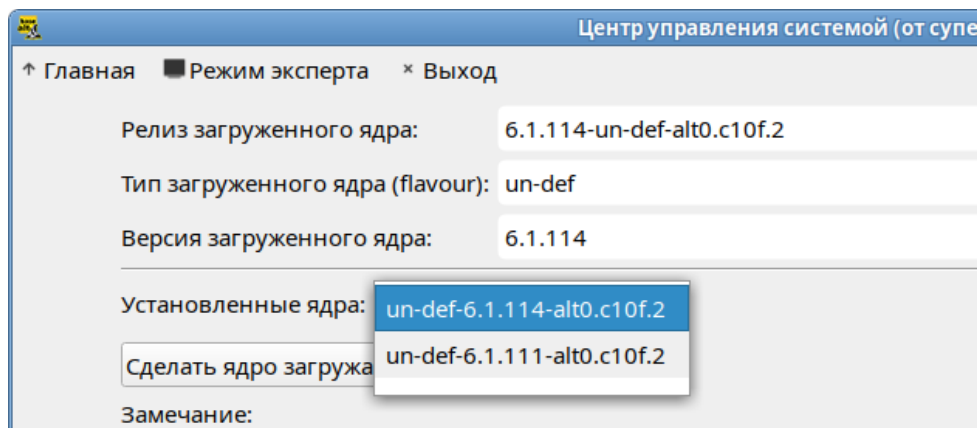


Рис. 589 – Список «Установленные ядра»

18.10.2.3. Удаление ядра

Накопленный при обновлениях набор ранее установленных ядер можно удалить для освобождения дискового пространства. Для этого следует выбрать нужное ядро в списке «Установленные ядра» и нажать кнопку «Удалить ядро».

18.10.2.4. Удаление модулей ядра

При установке ОС автоматически устанавливаются модули для различных аппаратных средств, включая различные модели видеокарт. Для уменьшения нагрузки при обновлениях неиспользуемые модули можно удалить. Для этого в списке «Установленные ядра» следует выбрать ядро, модули которого нужно удалить, затем в списке «Установленные модули» (рис. 590) выделить удаляемые модули и нажать на кнопку «Удалить модуль».

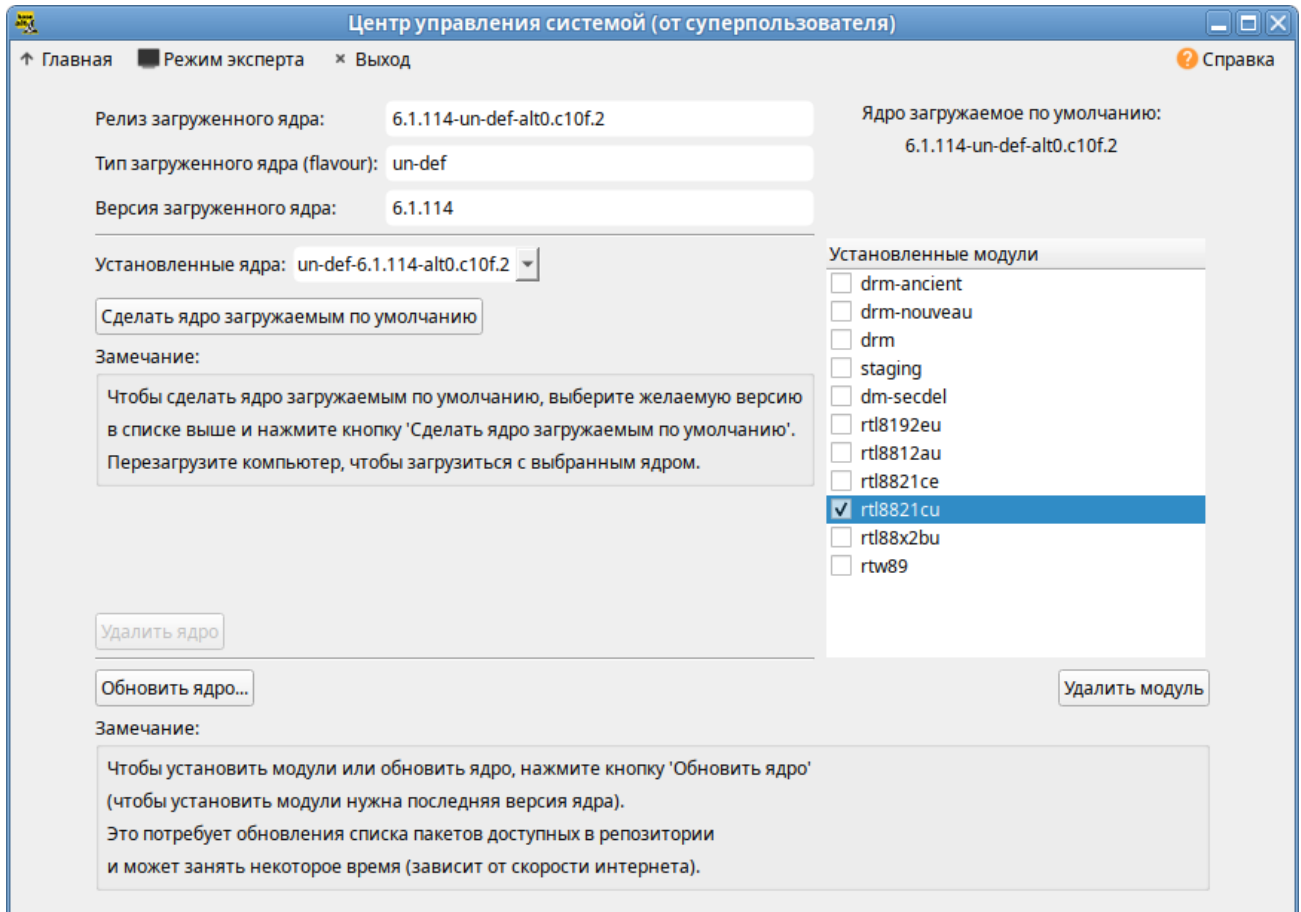


Рис. 590 – Выбор модуля в списке «Установленные модули»

18.11. Обновление изолированного окружения (chrooted environment)

Команда `update_chrooted --list` выводит список всех типов модулей для `update_chrooted`, которые установлены в системе:

```
# update_chrooted --list
List of registered types: all conf lib
```

С помощью команды `update_chrooted <имя_типа>` можно выполнить все модули указанного типа.

После изменения общесистемных конфигурационных файлов типа `/etc/resolv.conf`, для того чтобы синхронизировать эти изменения во всех многочисленных `chrooted environments` следует выполнить команду:

```
# update_chrooted conf
```

После изменения системных библиотек следует выполнить команду:

```
# update_chrooted lib
```

Для синхронизации изменений конфигурационных файлов и системных библиотек следует выполнить команду:

```
# update_chrooted all
```

18.12. Проверка подлинности пакетов

Подлинность пакетов при обновлении обеспечивается средствами кодирования, подтверждающих как целостность самих пакетов, так и целостность индексов, описывающих репозитории.

Ключевая информация для проверки подлинности распространяется вместе с дистрибутивом на сертифицированном носителе и защищена от потенциальной подмены при передаче по каналам связи.

Проверить подлинность и целостность пакета можно командой:

```
# rpm -vK имя_пакета
```

18.13. Получение уведомлений о выходе обновлений

Информирование потребителей о мерах, направленных на нейтрализацию выявленных уязвимостей ПИ ОС Альт СП, и выпускаемых обновлениях выполняется путем публикации информации на официальном сайте предприятия-разработчика (<https://altsp.su>) или по электронной почте.

18.14. Обновление систем, не имеющих выхода в Интернет

Обновление систем, не имеющих выхода в Интернет осуществляется в соответствии с п. 8.7.4.

18.15. Единая команда управления пакетами (epm)

epm – единая команда управления пакетами. Основное предназначение: унифицировать управление пакетами в дистрибутивах с разными пакетными менеджерами. epm упрощает процедуру управления пакетами, особенно полезна для тех, кто работает с множеством дистрибутивов, может использоваться в скриптах и установщиках, сервисных программах, в повседневном администрировании различных систем. Кроме того, в epm добавлены типовые операции, которые, например, в случае использования apt, потребовали бы ввода более одной команды.

Установка выполняется командой:

```
# apt-get install eepm
```

Включает в себя следующую функциональность:

- управление пакетами (установка – удаление – поиск);
- управление репозиториями (добавление – удаление – обновление – список);
- управление системными сервисами (включение – выключение – список).

Список поддерживаемых пакетных менеджеров: rpm, deb, tgz, tbz, tbz2, apk, pkg.gz.

Список команд rpm --help представлен в таблице 108.

Т а б л и ц а 108 – Список команд rpm --help

Описание операции	Команда rpm	Команда ОС Альт СП
Установка пакета по названию в систему	rpm -i (package)	apt-get install (package)
Установка файла пакета в систему	rpm -i (package file)	apt-get install (package file)
Удаление пакета из системы	rpm -e (package)	apt-get remove (package)
Поиск пакета в репозитории	rpm -s (text)	apt-cache search (text)
Проверка наличия пакета в системе	rpm -q (package)	rpm -qa (pipe) grep (package)
Список установленных пакетов	rpm -qa	rpm -qa
Поиск по названиям установленных пакетов	rpm -qp <word>	grep <word>
Принадлежность файла к (установленному) пакету	rpm -qf (file)	rpm -qf (file)
Поиск, в каком пакете есть указанный файл	rpm -sf <file>	
Список файлов в (установленном) пакете	rpm -ql (package)	rpm -ql (package)
Вывести информацию о пакете	rpm -qi (package)	apt-cache show (package)
Обновить дистрибутив	rpm upgrade	apt-get dist-upgrade

Примеры:

```
# epms name subtext – выполняет epms name | grep subtext
```

```
# epms name ^subtext – выполняет epms name | grep -v subtext
```

```
# epms "name1 name2" – выполняет поиск именно такого сочетания.
```

19. ОГРАНИЧЕНИЕ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ

19.1. Определение параметров уничтожения данных

Для пользователей нужно запретить использование команды `rm`.

Для этого нужно выполнить команду:

```
# chmod o-x /bin/rm
```

Команда `srm` предназначена для удаления данных без возможности их восстановления. `srm` выполняет безопасную перезапись/переименование/удаление целевого файла(ов). Использование команды `srm` аналогично использованию `rm`.

Команда `shred` переписывает несколько раз файл, скрывая его содержимое, для того, чтобы сделать более трудоемким процесс восстановления данных даже в случае использования специального оборудования для восстановления:

```
shred [ОПЦИЯ] ФАЙЛ [...]
```

Стандартные опции для запуска команды:

- 1) `-f`, `--force` – изменить права для разрешения записи, если нужно;
- 2) `-n`, `--iterations=N` – переписать `N` раз вместо указанных (25) по умолчанию;
- 3) `-s`, `--size=N` – очистить `N` байт (возможны суффиксы вида `K`, `M`, `G`);
- 4) `-u`, `--remove` – обрезать и удалить файл после перезаписи;
- 5) `-v`, `--verbose` – показывать индикатор прогресса;
- 6) `-x`, `--exact` – не округлять размеры файлов до следующего целого блока;
- 7) `-z`, `--zero` – перезаписать в конце с нулями, чтобы скрыть перемешивание.

Если файл задан как `-`, перемешивать стандартный вывод.

Удаляет ФАЙЛЫ если указан `--remove` (`-u`). По умолчанию файлы не удаляются, так как часто обрабатываются файлы-устройства вроде `/dev/hda`, а такие файлы нельзя удалять.

Команда `sfill` выполняет безопасную перезапись свободного пространства на разделе, в котором находится указанная директория и всех свободных индексных дескрипторов (`inode`) указанного каталога. Процесс удаления данных выглядит следующим образом:

- 1 проход с `0xff` (все данные затираются значением `0xff`);
- 5 случайных проходов с `/dev/urandom` используя RNG;
- 27 проходов со значениями Питера Гутмана;
- обрезает файл.

Стандартные опции для запуска команды:

- 1) `-d` – игнорировать специальные файлы `"."` и `".."`;
- 2) `-f` – быстрый (и небезопасный режим);
- 3) `-l` – выполнить только два прохода, с `0xff` и случайное заполнение;
- 4) `-l -l` – выполнить только случайное заполнение (один проход);
- 5) `-r` – выполнить в рекурсивном режиме, удалить все подкаталоги;
- 6) `-v` – подробный режим;
- 7) `-z` – последний проход заполняет нулями, а не случайными данными.

Пользователю запрещено определять параметры уничтожения данных. Эти параметры определяет администратор.

Для определения параметров уничтожения данных в системе созданы скрипты с предопределенными настройками уничтожения данных, для их переопределения администратор должен внести правки в файл `/etc/sysconfig/s_rm`.

П р и м е ч а н и е . Должен быть установлен пакет `altsp-test-scripts`.

Пользователи для удаления данных должны использовать команды `s_rm` и `s_fill`.

20. КОНТРОЛЬНЫЕ ХАРАКТЕРИСТИКИ РАЗВЕРНУТОЙ ОС АЛЬТ СП

После установки нужно проверить корректность развертывания ОС Альт СП путем подсчета и сличения контрольных характеристик установленных файлов. Подробнее см. в документе «Руководство по комплексу средств защиты. ЛКНВ.11100-01 99 03».

В качестве контрольной характеристики файла выступает контрольная сумма.

Подробнее об интегральных контрольных суммах ПИ, расположении пофайловых отчетов подсчета, алгоритме подсчета контрольных сумм приведено в документах «Формуляр. ЛКНВ.11100-01 30 01» и «Руководство по комплексу средств защиты. ЛКНВ.11100-01 99 03».

Информацию о применении критических обновлений ОС Альт СП нужно внести в раздел «Особые отметки» документа «Формуляр. ЛКНВ.11100-01 30 01».

21. ОСНОВЫ АДМИНИСТРИРОВАНИЯ LINUX

21.1. Общие принципы работы ОС

21.1.1. Процессы и файлы

ОС Альт СП является многопользовательской интегрированной системой. Это значит, что она разработана в расчете на одновременную работу нескольких пользователей.

Пользователь может либо сам работать в системе, выполняя некоторую последовательность команд, либо от его имени могут выполняться прикладные процессы.

Пользователь взаимодействует с системой через командный интерпретатор. Командный интерпретатор представляет собой прикладную программу, которая принимает от пользователя команды или набор команд и транслирует их в системные вызовы к ядру системы. Интерпретатор позволяет пользователю просматривать файлы, передвигаться по дереву файловой системы, запускать прикладные процессы. Все командные интерпретаторы UNIX имеют развитый командный язык и позволяют писать достаточно сложные программы, упрощающие процесс администрирования системы и работы с ней.

21.1.1.1. Процессы функционирования ОС

Все программы, которые выполняются в текущий момент времени, называются процессами. Процессы можно разделить на два основных класса: системные процессы и пользовательские процессы.

Системные процессы – программы, решающие внутренние задачи ОС, например, организацию виртуальной памяти на диске или предоставляющие пользователям те или иные сервисы (процессы-службы).

Пользовательские процессы – процессы, запускаемые пользователем из командного интерпретатора для решения задач пользователя или управления системными процессами. Linux изначально разрабатывался как многозадачная система.

Он использует технологии, опробованные и отработанные другими реализациями UNIX, которые существовали ранее.

Фоновый режим работы процесса – режим, когда программа может работать без взаимодействия с пользователем. В случае необходимости интерактивной работы с пользователем (в общем случае) процесс будет «остановлен» ядром, и работа его продолжается только после перевода его в «нормальный» режим работы.

21.1.1.2. Файловая система ОС

В ОС использована файловая система Linux, которая, в отличие от файловых систем DOS и Windows, является единым деревом. Корень этого дерева – каталог, называемый root и обозначаемый /.

Части дерева файловой системы могут физически располагаться в разных разделах разных дисков или вообще на других компьютерах – для пользователя это прозрачно. Процесс присоединения файловой системы раздела к дереву называется монтированием, удаление – размонтированием. Например, файловая система CD-ROM в дистрибутиве монтируется по умолчанию в каталог /media/cdrom (путь в дистрибутиве обозначается с использованием /, а не \, как в DOS/Windows).

Текущий каталог обозначается ./.

21.1.1.3. Структура каталогов

Корневой каталог /:

- /bin – командные оболочки (shell), основные утилиты;
- /boot – содержит ядро системы;
- /dev – псевдофайлы устройств, позволяющие работать с устройствами напрямую. Файлы в /dev создаются сервисом udev;
- /etc – общесистемные конфигурационные файлы для большинства программ в системе;
- /etc/rc?.d, /etc/init.d, /etc/rc.boot, /etc/rc.d – каталоги, где расположены командные файлы, выполняемые при запуске системы или при смене ее режима работы;

- /etc/passwd – база данных пользователей, в которой содержится информация об имени пользователя, его настоящем имени, личном каталоге, его зашифрованный пароль и другие данные;
- /etc/shadow – теневая база данных пользователей. При этом информация из файла /etc/passwd перемещается в /etc/shadow, который недоступен для чтения всем, кроме пользователя root. В случае использования альтернативной схемы управления теневыми паролями (ТСВ), все теневые пароли для каждого пользователя располагаются в каталоге /etc/tcb/имя пользователя/shadow;
- /home – домашние каталоги пользователей;
- /lib – содержит файлы динамических библиотек, которые нужны для работы большей части приложений, и подгружаемые модули ядра;
- /lost+found – восстановленные файлы;
- /media – подключаемые носители (каталоги для монтирования файловых систем сменных устройств);
- /mnt – точки временного монтирования;
- /opt – вспомогательные пакеты;
- /proc – виртуальная файловая система, хранящаяся в памяти компьютера при загруженной ОС. В данном каталоге расположены самые свежие сведения обо всех процессах, запущенных на компьютере;
- /root – домашний каталог администратора системы;
- /run – файлы состояния приложений;
- /sbin – набор программ для административной работы с системой (системные утилиты);
- /selinux – виртуальная файловая система SELinux;
- /srv – виртуальные данные сервисных служб;
- /sys – файловая система, содержащая информацию о текущем состоянии системы;
- /tmp – временные файлы;

- /usr – пользовательские двоичные файлы и данные, используемые только для чтения (программы и библиотеки);
- /var – файлы для хранения изменяющихся данных (рабочие файлы программ, очереди, журналы).

Каталог /usr:

- /usr/bin – дополнительные программы для всех учетных записей;
- /usr/sbin – команды, используемые при администрировании системы и не предназначенные для размещения в файловой системе root;
- /usr/local – место, где рекомендуется размещать файлы, установленные без использования пакетных менеджеров, внутренняя организация каталогов практически такая же, как и корневого каталога;
- /usr/man – каталог, где хранятся файлы справочного руководства man;
- /usr/share – каталог для размещения общедоступных файлов большей части приложений.

Каталог /var:

- /var/log – каталог для регистрации сообщений, системный журнал;
- /var/spool – каталог для хранения файлов, находящихся в очереди на обработку для того или иного процесса (очереди печати, непочитанные или не отправленные письма, задачи cron и т. д.).

21.1.1.4. Организация файловой структуры

Система домашних каталогов пользователей помогает организовывать безопасную работу пользователей в многопользовательской системе. Вне своего домашнего каталога пользователь обладает минимальными правами (обычно чтение и выполнение файлов) и не может нанести ущерб системе, например, удалив или изменив файл.

Кроме файлов, созданных пользователем, в его домашнем каталоге обычно содержатся персональные конфигурационные файлы некоторых программ.

Маршрут (путь) – это последовательность имен каталогов, представляющая собой путь в файловой системе к данному файлу, где каждое следующее имя отделяется от предыдущего наклонной чертой (слешем). Если название маршрута начинается со слеша, то путь в искомый файл начинается от корневого каталога всего дерева системы. В обратном случае, если название маршрута начинается непосредственно с имени файла, то путь к искомому файлу должен начаться от текущего каталога (рабочего каталога).

Имя файла может содержать любые символы за исключением косой черты (/). Однако следует избегать применения в именах файлов большинства знаков препинания и непечатаемых символов. При выборе имен файлов рекомендуется ограничиться следующими символами:

- строчные и ПРОПИСНЫЕ буквы. Следует обратить внимание на то, что регистр всегда имеет значение;
- символ подчеркивания (_);
- точка (.).

Для удобства работы точку можно использовать для отделения имени файла от расширения файла. Данная возможность может быть нужна пользователям или некоторым программам, но не имеет значение для shell.

21.1.1.5. Имена дисков и разделов

Все физические устройства компьютера отображаются в каталог `/dev` файловой системы дистрибутива. Диски (в том числе IDE/SATA/SCSI/SAS жесткие диски, USB-диски) имеют имена:

- `/dev/sda` – первый диск;
- `/dev/sdb` – второй диск;
- и т. д.

Диски обозначаются `/dev/sdX`, где X – a, b, c, d, e, ... в зависимости от порядкового номера диска на шине.

Раздел диска обозначается числом после его имени. Например, `/dev/sdb4` – четвертый раздел второго диска.

21.1.1.6. Разделы для работы ОС

Для работы ОС на жестком диске (дисках) должны быть созданы, по крайней мере, два раздела: корневой (то есть тот, который будет содержать каталог /) и раздел подкачки (swap). Размер последнего, как правило, составляет от однократной до двукратной величины оперативной памяти компьютера. Если на диске много свободного места, то можно создать отдельные разделы для каталогов /usr, /home, /var.

21.1.2. Командные оболочки (интерпретаторы)

Для управления ОС используются командные интерпретаторы (shell).

После входа в систему, увидите приглашение – строку, содержащую символ «\$» (далее этот символ будет обозначать командную строку). Программа ожидает ваших команд. Роль командного интерпретатора – передавать ваши команды операционной системе. По своим функциям он соответствует `command.com` в DOS, но несравненно мощнее. При помощи командных интерпретаторов можно писать небольшие программы – сценарии (скрипты). В Linux доступны следующие командные оболочки:

- `bash` – самая распространенная оболочка под linux. Она ведет историю команд и предоставляет возможность их редактирования;
- `pdksh` – клон `korn shell`, хорошо известной оболочки в UNIX системах.

Проверить, какая оболочка используется в данный момент можно, выполнив команду:

```
$ echo $SHELL
```

Оболочкой по умолчанию является Bash (Bourne Again Shell) – самая распространенная оболочка под Linux, которая ведет историю команд и предоставляет возможность их редактирования.

21.1.3. Командная оболочка Bash

В Bash имеется несколько приемов для работы со строкой команд. Например, можно использовать следующие сочетания клавиш:

- `<Ctrl>+<A>` – перейти на начало строки;

- <Ctrl>+<U> – удалить текущую строку;
- <Ctrl>+<C> – остановить текущую задачу.

Для ввода нескольких команд одной строкой можно использовать разделитель «;». По истории команд можно перемещаться с помощью клавиш ↑ («вверх») и ↓ («вниз»).

Чтобы найти конкретную команду в списке набранных, не пролистывая всю историю, можно нажать <Ctrl>+<R> и начать вводить символы ранее введенной команды.

Для просмотра истории команд можно воспользоваться командой `history`. Команды, присутствующие в истории, отображаются в списке пронумерованными. Чтобы запустить конкретную команду нужно набрать:

```
!номер команды
```

```
Если ввести:
```

```
!!
```

запустится последняя из набранных команд.

В Bash имеется возможность самостоятельного завершения имен команд из общего списка команд, что облегчает работу при вводе команд, в случае, если имена программ и команд слишком длинны. При нажатии клавиши <Tab> Bash завершает имя команды, программы или каталога, если не существует нескольких альтернативных вариантов. Например, чтобы использовать программу декомпрессии `gunzip`, можно набрать следующую команду:

```
gu
```

Затем нажать клавишу <Tab>. Так как в данном случае существует несколько возможных вариантов завершения команды, то нужно повторно нажать клавишу <Tab>, чтобы получить список имен, начинающихся с `gu`.

В предложенном примере можно получить следующий список:

```
$ gu  
guile gunzip gunnp-binding-tool
```

Если набрать: `n` (`gunzip` – это единственное имя, третьей буквой которого является «n»), а затем нажать клавишу <Tab>, то оболочка самостоятельно дополнит имя. Чтобы запустить команду нужно нажать <Enter>.

Программы, вызываемые из командной строки, Bash ищет в каталогах, определяемых в системной переменной `$PATH`. По умолчанию в этот перечень каталогов не входит текущий каталог, обозначаемый `./` (точка слеш) (если только не выбран один из двух самых слабых уровней защиты). Поэтому, для запуска программы из текущего каталога, нужно использовать команду (в примере запускается команда `prog`):

```
./prog
```

21.1.4. Стыкование команд в системе Linux

21.1.4.1. Стандартный ввод и стандартный вывод

Многие команды системы имеют так называемые стандартный ввод (`standard input`) и стандартный вывод (`standard output`), часто сокращаемые до `stdin` и `stdout`. Ввод и вывод здесь – это входная и выходная информация для данной команды. Программная оболочка делает так, что стандартным вводом является клавиатура, а стандартным выводом – экран монитора.

Пример с использованием команды `cat`. По умолчанию команда `cat` читает данные из всех файлов, которые указаны в командной строке, и посылает эту информацию непосредственно в стандартный вывод (`stdout`). Следовательно, команда:

```
cat history-final masters-thesis
```

выведет на экран сначала содержимое файла `history-final`, а затем – файла `masters-thesis`.

Если имя файла не указано, программа `cat` читает входные данные из `stdin` и возвращает их в `stdout`.

Пример:

```
cat
Hello there.
Hello there.
Bye.
Bye.
Ctrl-D
```

Каждую строку, вводимую с клавиатуры, программа `cat` немедленно возвращает на экран. При вводе информации со стандартного ввода конец текста сигнализируется вводом специальной комбинации клавиш, как правило, `<Ctrl>+<D>`. Сокращенное название сигнала конца текста – EOT (end of text).

21.1.4.2. Перенаправление ввода и вывода

При необходимости можно перенаправить стандартный вывод, используя символ `>`, и стандартный ввод, используя символ `<`.

Фильтр (`filter`) – программа, которая читает данные из стандартного ввода, некоторым образом их обрабатывает и результат направляет на стандартный вывод. Когда применяется перенаправление, в качестве стандартного ввода и вывода могут выступать файлы. Как указывалось выше, по умолчанию, `stdin` и `stdout` относятся к клавиатуре и к экрану соответственно. Программа `sort` является простым фильтром – она сортирует входные данные и посылает результат на стандартный вывод. Совсем простым фильтром является программа `cat` – она ничего не делает с входными данными, а просто пересылает их на выход.

21.1.4.3. Использование состыкованных команд

Стыковку команд (`pipelines`) осуществляет командная оболочка, которая `stdout` первой команды направляет на `stdin` второй команды. Для стыковки используется символ `|`. Направить `stdout` команды `ls` на `stdin` команды `sort`:

```
ls | sort -r
notes
masters-thesis
history-final
english-list
```

Вывод списка файлов частями:

```
ls /usr/bin | more
```

Если нужно вывести на экран последнее по алфавиту имя файла в текущем каталоге, можно использовать следующую команду:

```
ls | sort -r | head -1 notes
```

где команда `head -1` выводит на экран первую строку получаемого ей входного потока строк (в примере поток состоит из данных от команды `ls`), отсортированных в обратном алфавитном порядке.

21.1.4.4. Недеструктивное перенаправление вывода

Эффект от использования символа `>` для перенаправления вывода файла является деструктивным; т. е., команда `ls > file-list` уничтожит содержимое файла `file-list`, если этот файл ранее существовал, и создаст на его месте новый файл. Если вместо этого перенаправление будет сделано с помощью символов `>>`, то вывод будет приписан в конец указанного файла, при этом исходное содержимое файла не будет уничтожено.

Примечание. Перенаправление ввода и вывода и стыкование команд осуществляется командными оболочками, которые поддерживают использование символов `>`, `>>` и `|`. Сами команды не способны воспринимать и интерпретировать эти символы.

21.2. Режим суперпользователя

21.2.1. Пользователи ОС

Linux – система многопользовательская, а потому пользователь – ключевое понятие для организации всей системы доступа в Linux. Файлы всех пользователей в Linux хранятся отдельно, у каждого пользователя есть собственный домашний каталог, в котором он может хранить свои данные. Доступ других пользователей к домашнему каталогу пользователя может быть ограничен.

Суперпользователь в Linux – это выделенный пользователь системы, на которого не распространяются ограничения прав доступа. Именно суперпользователь имеет возможность произвольно изменять владельца и группу файла. Ему открыт доступ на чтение и запись к любому файлу или каталогу системы.

Среди учетных записей Linux всегда есть учетная запись суперпользователя – `root`. Поэтому вместо «суперпользователь» часто говорят «`root`». Множество системных файлов принадлежат `root`, множество файлов только ему доступны для чтения или записи. Пароль этой учетной записи – одна из самых больших драгоценностей системы. Именно с ее помощью системные администраторы выполняют самую ответственную работу.

21.2.2. Назначение режима суперпользователя

Системные утилиты, например, такие, как ЦУС или программа управления пакетами Synaptic, настройки КСЗ ОС требуют для своей работы привилегий суперпользователя, потому что они вносят изменения в системные файлы. При их запуске выводится запрос/диалоговое окно с запросом пароля системного администратора.

21.2.3. Получение прав суперпользователя

Существует два различных способа получить права суперпользователя.

Первый – это зарегистрироваться в системе под именем root в командной строке.

Второй способ – воспользоваться специальной утилитой `su` (shell of user), которая позволяет выполнить одну или несколько команд от лица другого пользователя. По умолчанию эта утилита выполняет команду `sh` от пользователя root, то есть запускает командный интерпретатор. Отличие от предыдущего способа в том, что всегда известно, кто именно запускал `su`, а значит, ясно, кто выполнил определенное административное действие.

В некоторых случаях удобнее использовать не `su`, а утилиту `sudo`, которая позволяет выполнять только заранее заданные команды.

Примечание. Для того чтобы воспользоваться командами `su` и `sudo`, нужно быть членом группы `wheel`. Пользователь, созданный при установке системы, по умолчанию уже включен в эту группу.

21.2.4. Переход в режим суперпользователя

Для перехода в режим суперпользователя наберите в терминале команду `su -`.

Синтаксис:

```
su [-] [name [arg...]]
```

Чтобы вернуться к правам пользователя, нужно ввести следующую команду:

```
exit
```

Если воспользоваться командой `su` без ключа, то происходит вызов командного интерпретатора с правами root. При этом значение переменных

окружения, в частности `$PATH`, остается таким же, как у пользователя: в переменной `$PATH` не окажется каталогов `/sbin`, `/usr/sbin`, без указания полного имени будут недоступны команды `route`, `shutdown`, `mkswap` и другие. Более того, переменная `$HOME` будет указывать на каталог пользователя, все программы, запущенные в режиме суперпользователя, сохранят свои настройки с правами `root` в каталоге пользователя, что в дальнейшем может вызвать проблемы.

Чтобы избежать этого, следует использовать `su -`. В этом режиме `su` запустит командный интерпретатор в качестве `login shell`, и он будет вести себя в точности так, как если бы в системе зарегистрировался `root`.

21.3. Управление пользователями

Подробнее о средствах управления учетными записями пользователей смотрите в документе «Руководство по комплексу средств защиты. ЛКНВ.11100-01 99 03».

21.4. Система инициализации `systemd` и `sysvinit`

21.4.1. Запуск операционной системы

21.4.1.1. Запуск системы

Алгоритм запуска компьютера:

- 1) BIOS (БСВВ) компьютера;
- 2) загрузчик системы (например, `LILO`, `GRUB` или другой). В загрузчике можно задать параметры запуска системы (см. п. 6.1);
- 3) загрузка ядра `Linux`;
- 4) запускается на выполнение первый процесс в системе – `init`.

Ядром запускается самая первая программа в системе `init`. Ее задачей является запуск новых процессов и повторный запуск завершившихся. Можно посмотреть, где расположился `init` в иерархии процессов системы, введите команду: `ps tree`.

От конфигурации `init` зависит, какая система инициализации будет использована.

21.4.1.2. Система инициализации

Система инициализации – это набор скриптов, которые будут выполнены при старте системы.

Существуют разные системы инициализации, наиболее популярной системой являются `sysvinit` и ее модификации. `systemd` разрабатывается как замена для `sysVinit`.

В ОС Альт СП используется `sysvinit` (от System V init).

System V – классическая схема инициализации, на которой базируются многие дистрибутивы. Привычна и довольно проста для понимания: `init` описывает весь процесс загрузки в своем конфигурационном файле `/etc/inittab`, откуда вызываются другие программы и скрипты на определенном этапе запуска.

21.4.2. Примеры команд управления службами, журнал в `systemd`

Обратите внимание, что команды `service` и `chkconfig` продолжают работать в `systemd` практически без изменений. Тем не менее, в таблице 109 показано как выполнить те же действия с помощью встроенных утилит `systemctl`.

Т а б л и ц а 109 – Команды управления службами

Команды <code>sysvinit</code>	Команды <code>systemd</code>	Примечания
<code>service frobozz start</code>	<code>systemctl start frobozz.service</code>	Используется для запуска службы (не перезагружает постоянные).
<code>service frobozz stop</code>	<code>systemctl stop frobozz.service</code>	Используется для остановки службы (не перезагружает постоянные).
<code>service frobozz restart</code>	<code>systemctl restart frobozz.service</code>	Используется для остановки и последующего запуска службы.
<code>service frobozz reload</code>	<code>systemctl reload frobozz.service</code>	Если поддерживается, перезагружает файлы конфигурации без прерывания незаконченных операций.

Окончание таблицы 109

Команды sysvinit	Команды systemd	Примечания
<code>service frobozz condrestart</code>	<code>systemctl condrestart frobozz.service</code>	Перезапускает службу, если она уже работает.
<code>service frobozz status</code>	<code>systemctl status frobozz.service</code>	Сообщает, запущена ли уже служба.
<code>ls /etc/rc.d/init.d/</code>	<code>systemctl list-unit-files --type=service (preferred)</code> <code>ls /lib/systemd/system/*.service</code> <code>/etc/systemd/system/*.service</code>	Используется для отображения списка служб, которые можно запустить или остановить. Используется для отображения списка всех служб.
<code>chkconfig frobozz on</code>	<code>systemctl enable frobozz.service</code>	Включает службу во время следующей перезагрузки, или любой другой триггер.
<code>chkconfig frobozz off</code>	<code>systemctl disable frobozz.service</code>	Выключает службу во время следующей перезагрузки, или любой другой триггер.
<code>chkconfig frobozz</code>	<code>systemctl is-enabled frobozz.service</code>	Используется для проверки, сконфигурирована ли служба для запуска в текущем окружении.
<code>chkconfig --list</code>	<code>systemctl list-unit-files --type=service (preferred)</code> <code>ls /etc/systemd/system/*.wants/</code>	Выводит таблицу служб. В ней видно, на каких уровнях загрузки они (не)запускаются.
<code>chkconfig frobozz --list</code>	<code>ls /etc/systemd/system/*.wants/frobozz.service</code>	Используется, для отображения на каких уровнях служба (не)запускается.
<code>chkconfig frobozz --add</code>	<code>systemctl daemon-reload</code>	Используется, когда создается новая служба или модифицируется любая конфигурация.

21.4.3. Журнал в systemd

В systemd включена возможность ведения системного журнала. Для чтения журнала следует использовать команду `journalctl`. По умолчанию, больше не требуется запуск службы `syslog`.

Можно запускать `journalctl` с разными ключами (таблица 110).

Для ознакомления с прочими возможностями, читайте руководство по `journalctl`. Для этого используйте команду `man journalctl`.

Т а б л и ц а 110 – Примеры запуска `journalctl`

Команда	Описание
<code>journalctl -b</code>	Покажет сообщения только с текущей загрузки.
<code>journalctl -f</code>	Покажет только последние сообщения.
<code>journalctl --since "2015-07-20 17:15:00"</code>	Просмотреть все сообщения начиная с 20 июля 2015 года 17:15.
<code>journalctl -k</code>	Просмотр сообщений ядра.
<code>journalctl /usr/lib/systemd/system</code>	Все сообщения конкретной утилиты <code>systemd</code> .
<code>journalctl _PID=1</code>	Просмотр сообщения определенного процесса, покажет сообщения первого процесса (<code>init</code>).
<code>journalctl -u netcfg</code>	Все сообщения конкретного приложения или службы.
<code>journalctl _UID=33</code>	Все сообщения процессов, запущенных от имени конкретного пользователя.

22. СООБЩЕНИЯ АДМИНИСТРАТОРУ

При возникновении проблем в процессе функционирования ОС Альт СП появляются диагностические сообщения трех типов: информационные, предупреждающие и сообщения об ошибках.

Администратор должен проанализировать диагностические сообщения и принять меры по устранению появившихся проблем.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД	– база данных;
БСВВ	– базовая система ввода-вывода;
ЕПП	– единое пользовательское пространство;
КСЗ	– комплекс средств защиты;
НЖМД	– накопитель на жестких магнитных дисках;
ОС	– операционная система;
ПИ	– программное изделие;
ПО	– программное обеспечение;
ПЭВМ	– персональная электронная вычислительная машина;
СВТ	– средство вычислительной техники;
СУБД	– система управления базами данных;
УЦ	– удостоверяющий центр;
ФС	– файловая система;
ЦУС	– центр управления системой;
AD	– Active Directory;
DC	– Domain Controller;
PDC	– Primary Domain Controller.

