УТВЕРЖДЕН

ЛКНВ.11100-01 31 03-ЛУ

ОПЕРАЦИОННАЯ СИСТЕМА АЛЬТ 8 СП

(ОС Альт 8 СП)

Описание применения

ЛКНВ.11100-01 31 03

Листов 50

2024

Литера О

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

АННОТАЦИЯ

Настоящий документ содержит основные сведения о применении программного изделия «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: 1.1.

Описание применения состоит из четырех основных частей, в которых раскрываются основные вопросы применения и функционирования ОС Альт СП. Также рассматривается организация входных и выходных данных в системе, и конфигурация технических средств, необходимых для применения операционной системы.

В первом разделе приводятся назначение, основные принципы организации, возможности операционной системы, ее основные характеристики, ограничения, накладываемые на область ее применения.

Во втором разделе указываются условия, необходимые для функционирования операционной системы, структура технических и программных средств и требования к ним, общие характеристики входной и выходной информации, а также требования и условия организационного, технического и технологического характера и т. п.

В третьем разделе указывается определение задачи и методы ее решения, приводится общая структура и алгоритмы функционирования ОС Альт СП.

В четвертом разделе приводятся сведения о входных и выходных данных. Указываются их характер и организация, частота обновления и пр.

Описание применения разработано в соответствии с ГОСТ 19.502–78 «Единая система программной документации. Описание применения. Требования к содержанию и оформлению».

СОДЕРЖАНИЕ

1. Назначение программы 4
1.1. Назначение 4
1.2. Возможности и основные характеристики 4
1.2.1. Специальные характеристики 9
2. Условия применения 10
2.1. Требования к техническим средствам 10
2.2. Требования и условия организационного и технологического характера 10
2.3. Ограничения на использование технического и программного характера 11
2.3.1. Ограничения на использование аппаратных платформ и базовых систем ввода-вывода 11
2.3.2. Ограничения на действия при обнаружении уязвимостей 11
2.3.3. Ограничения, накладываемые на использование механизмов КСЗ 11
3. Описание задачи 12
3.1. Определение задачи 12
3.2. Методы решения 13
3.2.1. Средства управления памятью 14
3.2.2. Средства управления процессами 15
3.2.3. Средства работы с файлами 23
3.2.4. Система ввода-вывода 25
3.2.5. Средства администрирования 29
3.2.6. Комплекс средств защиты 30
4. Входные и выходные данные 48
4.1. Входные данные 48
4.2. Выходные данные 48
Перечень сокращений 49

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Назначение

ОС Альт СП предназначена для группового и корпоративного использования в качестве средства автоматизации информационных, конструкторских и производственных процессов предприятий (организаций, учреждений).

1.2. Возможности и основные характеристики

ОС Альт 8 СП представляет собой комплекс программ, созданных на основе ОС Linux, и обеспечивает обработку, хранение, передачу информации, а также реализацию функций защиты от несанкционированного доступа к информации, обрабатываемой на средствах вычислительной техники, находящихся под управлением данного комплекса программ.

ОС Альт СП обладает следующими функциональными характеристиками:

- обеспечивает возможность обработки, хранения и передачи информации в защищенной программной среде;
- обеспечивает возможность запуска пользовательского программного обеспечения 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 поддержку виртуальной памяти;
- обеспечивает сетевую обработку данных, в том числе разграничение доступа к сетевым пакетам;
- поддерживает мультитерминальный режим для создания дополнительных рабочих мест на одном компьютере.

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) операционной системы (далее – ОС);
- администрирование;
- поддержка интерфейса прикладного программирования;
- поддержка пользовательского интерфейса.

ОС Альт СП поддерживает клиент-серверную архитектуру и может обслуживать процессы как в пределах одной компьютерной системы, так и процессы на других ПЭВМ через каналы передачи данных или сетевые соединения.

Вариант исполнения ОС Альт СП Рабочая станция включает офисные и клиентские приложения и обеспечивает выполнение следующих функций:

1) персональные средства информационного обмена:
   - получение и чтение электронной почты (по протоколам POP3, IMAP);
   - отправка почты, в том числе и напрямую на сервер получателя;
   - ведение адресной книги;
   - ведение коротких заметок;
   - планирование встреч и задач с уведомлением об их наступлении;

2) полезные возможности:
   - просмотр календаря;
   - арифметический калькулятор;
   - словарь (со встроенным англо-русским словарем);

3) работа с документами:
   - правка простых текстовых документов;

- правка документов со сложным форматированием;
- подсчет в электронных таблицах;
- подготовка и проведение презентаций;
- построение различных схем из предопределенных шаблонов;
- управление базами данных;
- сканирование;
- создание архивов, чтение из архивов (rar, arj, zip, tar.bz2, tar.gz, 7z);

4) средства работы в сети Интернет/Интранет:

- просмотр веб-страниц, включая гипертекстовые веб-страницы, аудио и видео;
- воспроизведение потокового аудио и видео;
- общение в сетях обмена немедленными сообщениями (с поддержкой XMPP);
- работа с файлами по протоколам FTP;

5) вывод информации:

- печать на принтере и МФУ;
- сохранение в формате PDF;

6) мультимедиа:

- просмотр изображений (форматы netpbm 8 и 16 бит, tiff 8 и 16 бит (в т. ч. многостраничный), geotiff, png (в т. ч. 16-бит), jpeg2000, djvu, jpeg, svg, bmp, gif с анимацией, ico;
- редактирование растровых изображений;
- редактирование векторных изображений;
- запись CD и DVD (создание нового проекта и копирование существующего диска);
- сохранение в файлах содержимого звуковых компакт-дисков и видео с DVD;
- запись звука с микрофона;
- запись видео с веб-камеры;

- просмотр видео (в форматах avi, mpg, ogg, divx, xvid, mkv, flv, .wmv) с субтитрами (.ssa, .srt, .ass);
- прослушивание звуковых файлов (в форматах wav, flac, cue, mp3, ogg, aac, ape);
- прослушивание звуковых компакт-дисков;
- возможность просмотра DVD;

7) ALT CSP КриптоПро – графический интерфейс для запуска команд криптопровайдера на проверку и создание электронной цифровой подписи (ЭЦП ГОСТ).

Вариант исполнения ОС Альт СП Сервер включает следующие серверные компоненты:

- систему управления базами данных (СУБД);
- веб-сервисы;
- почтовые сервисы;
- файловые сервера (Samba/NFS/FTP/TFTP);
- DNS сервер;
- DHCP сервер;
- сервер групповой работы SOGo;
- сервер контроллера домена Linux FreeIPA;
- LDAP сервер;
- сервер Kerberos;
- сервер печати CUPS;
- сервер времени;
- программные средства виртуализации;
- программные средства контейнеризации;
- программный комплекс Альт Домен.

ОС Альт СП реализует в соответствии с требованиями по безопасности информации к средствам виртуализации 4-го класса защиты[1] следующие функции безопасности:

- доверенная загрузка виртуальных машин;
- контроль целостности;
- регистрация событий безопасности;
- управление доступом;
- резервное копирование;
- управление потоками информации;
- защита памяти;
- ограничение программной среды;
- идентификация и аутентификация пользователей;
- централизованное управление образами виртуальных машин и виртуальными машинами.

ОС Альт СП реализует в соответствии с требованиями по безопасности информации к средствам контейнеризации 4-го класса защиты[2] следующие функции безопасности:

- изоляция контейнеров;
- выявление уязвимостей в образах контейнеров;
- проверка корректности конфигурации контейнеров;
- контроль целостности контейнеров и их образов;
- регистрация событий безопасности;
- управление доступом;
- идентификация и аутентификация пользователей;
- централизованное управление образами контейнеров и контейнерами.

---

[1] В соответствии с документом «Требования по безопасности информации к средствам виртуализации», утвержденным приказом ФСТЭК России от 27 октября 2022 г. №187.

[2] В соответствии с документом «Требования по безопасности информации к средствам контейнеризации», утвержденным приказом ФСТЭК России от 4 июля 2022 г. №118.

ОС Альт 8 СП реализует в соответствии с требованиями по безопасности информации к системам управления базами данных 4-го класса защиты[3] следующие функции безопасности:

- управление доступом;
- идентификация и аутентификация пользователей;
- контроль целостности;
- регистрация событий безопасности;
- резервное копирование и восстановление;
- обеспечение доступности;
- очистку памяти;
- производительность;
- ограничение программной среды.

ОС Альт 8 СП обеспечивает выполнение программ в защищенной среде. В состав ОС Альт 8 СП включены программные интерпретаторы (php, perl, lua, python, nodejs) и веб-сервер (nginx), прошедшие испытания по выявлению уязвимостей и недекларированных возможностей в соответствии с Методикой[4] ФСТЭК России в полном объеме.

1.2.1. Специальные характеристики

Средства разработки для ОС Альт СП предоставляются отдельно по запросу.

ПРЕДУПРЕЖДЕНИЕ

Программные компоненты компакт-диска со средствами разработки могут использоваться только для разработки специального (прикладного) программного обеспечения (СПО), предназначенного для функционирования в среде ОС Альт СП. В случае если необходимо применение программ из состава компакт-диска «Средства разработки» для обеспечения функционирования СПО, эти программы должны быть включены в состав разрабатываемого СПО, в том числе в состав загрузочного модуля (дистрибутива), и сертифицированы на соответствие требованиям безопасности информации в его составе.

[3] В соответствии с документом «Требования по безопасности информации к системам управления базами данных», утвержденным приказом ФСТЭК России от 14 апреля 2023 г. №64.

[4] Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении, утверждена ФСТЭК России 25.12.2020 г.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Требования к техническим средствам

Для функционирования ОС Альт СП необходима ПЭВМ, обладающая следующими характеристиками:

- процессор архитектуры: 64 бит (x86_64), AArch64 (ARMv8));
- объем оперативной памяти – от 1 Гбайт и более);
- объем доступного пространства накопителя на жестких магнитных дисках не менее 50 Гбайт (рекомендуется 200 Гбайт и более);
- периферийные устройства ввода/вывода – устройство чтения и записи компакт-дисков (опционально для инсталляции дистрибутива).

Рекомендуемые параметры для функционирования СУБД в ОС Альт СП необходима ПЭВМ, обладающая следующими характеристиками:

- процессор: 64 бит (x86_64)/AArch64 (ARMv8), 8 ядер;
- объем оперативной памяти – 16 Гбайт;
- объем доступного пространства накопителя на жестких магнитных дисках – от 100 Гбайт SSD;
- для построения кластера:
    а) минимальное количество хостов – 2;
    б) пропускная способность сетевого интерфейса – 10 Гбит/с.

2.2. Требования и условия организационного и технологического характера

Ко всем пользователям ОС Альт СП предъявляется следующее требование: базовые навыки работы с ОС семейства «Linux».

К администратору ОС Альт СП предъявляются следующие требования:

- знание принципов построения и функционирования современных вычислительных систем, механизмов защиты информации;
- навыки работы с ОС семейства «Linux»;

- навыки администрирования общесистемного и прикладного программного обеспечения;
- навыки настройки средств защиты и средств электронной подписи, используемых в составе ОС Альт СП.

2.3. Ограничения на использование технического и программного характера

2.3.1. Ограничения на использование аппаратных платформ и базовых систем ввода-вывода

Не допускается использование аппаратных платформ и версий базовых систем ввода-вывода и UEFI-драйверов, содержащих известные уязвимости, описанные в общедоступных источниках информации.

В случае если используемая аппаратная платформа, версия базовой системы ввода-вывода или версия UEFI-драйвера содержит уязвимость, то ее использование допускается только после применения патча, представленного разработчиком данной аппаратной платформы, версии базовой системы ввода-вывода или версии UEFI-драйвера (официального патча).

При отсутствии такого патча использование аппаратной платформы, версии базовой системы ввода вывода или версии UEFI-драйвера не допускается.

2.3.2. Ограничения на действия при обнаружении уязвимостей

В случае обнаружения уязвимостей в программных модулях ОС Альт СП необходимо устранить уязвимость путем установки сертифицированного обновления, либо путем принятия иных организационно-технических мер, направленных на исключение возможности уязвимости.

При этом сами меры носят временный характер, а их использование допустимо до момента выпуска соответствующего обновления.

2.3.3. Ограничения, накладываемые на использование механизмов КСЗ

Ограничения, накладываемые на использование механизмов КСЗ, приведены в документе «Руководство по комплексу средств защиты. ЛКНВ.11100-01 99 03».

3. ОПИСАНИЕ ЗАДАЧИ

3.1. Определение задачи

ОС Альт СП решает следующие основные задачи:

- организация дискреционного принципа контроля доступа к информации;
- идентификация и аутентификация субъектов;
- разграничение доступа к сетевому взаимодействию, фильтрация сетевых потоков и сбор статистики;
- управление информационными потоками;
- контроль создания и удаления процессов;
- синхронизация процессов;
- удаление объектов файловой системы путем многократной перезаписи уничтожаемых (стираемых) объектов файловой системы;
- распределение оперативной памяти между прикладными задачами;
- очистка (обнуление) освобождаемых областей оперативной памяти ПЭВМ;
- контроль распределения системных ресурсов;
- задание правил и контроль запуска компонентов ПО, реагирование на попытки запуска компонентов ПО, произведенные в нарушение установленных правил запуска компонентов ПО;
- изоляция программных модулей процессов в пределах оперативной памяти ПЭВМ;
- сопоставление пользователя с устройством;
- доступ к периферийным устройствам;
- защита ввода и вывода на отчуждаемый физический носитель информации;
- буферизация данных;
- взаимодействие с управляющими программами аппаратных средств;
- регистрация и журналирование событий, в том числе – событий безопасности;
- контроль целостности программных средств, КСЗ и обрабатываемой информации, в том числе реализация замкнутой программной среды;

- резервное копирование и восстановление объектов файловой системы, включая ассоциированные с ними атрибуты безопасности.

3.2. Методы решения

Для решения поставленных задач в ОС Альт СП используются:

1) средства управления процессами, в состав которых входят:
   - службы контроля создания и удаления процессов;
   - службы синхронизации процессов;
   - службы контроля распределения системных ресурсов;
   - подсистема межпроцессного взаимодействия;
2) средства управления памятью;
3) средства работы с файлами;
4) система ввода-вывода, в состав которых входят:
   - службы буферизации данных;
   - службы доступа к периферийным устройствам;
   - службы взаимодействия с управляющими программами аппаратных средств;
   - службы управления печатью;
5) средства администрирования;
6) КСЗ, который реализует следующие функции безопасности:
   - идентификация и аутентификация;
   - управление доступом;
   - регистрация событий безопасности;
   - ограничение программной среды;
   - изоляция процессов;
   - защита памяти;
   - контроль целостности;
   - обеспечение надежного функционирования;
   - фильтрация сетевого потока.

3.2.1. Средства управления памятью

Средства управления памятью обеспечивают выполнение функций распределения оперативной памяти между прикладными задачами. Оперативная память в ОС Альт СП имеет страничную организацию, в основе которой лежит принцип деления виртуального адресного пространства на части (страницы). Страницы всегда имеют фиксированный размер. Передача данных между оперативной памятью и дисковым накопителем всегда осуществляется в страницах. При этом процесс работает с виртуальными адресами, а не с физическими. Преобразование происходит посредством вычислений, используя таблицы дескрипторов и каталоги таблиц.

ОС Альт СП поддерживает три уровня таблиц:

- каталог таблиц первого уровня PGD (Page Table Directory);
- каталог таблиц второго уровня PMD (Medium Page Table Directory);
- таблица дескрипторов PTE (Page Table Entry).

Преобразование виртуального адреса в физический осуществляется в три этапа:

1) указатель PGD, имеющийся в структуре описывающий каждый процесс, преобразуется в указатель записи PMD;
2) указатель записи PMD преобразуется в указатель в таблице дескрипторов PTE;
3) к реальному адресу, указывающему на начало страницы прибавляется смещение от ее начала.

Все данные об используемой процессом памяти хранятся ядром ОС Альт СП в специальных структурах.

При открытии файла выполняется его отображение в память (часть файла, дочитанная до размера страницы; например, для процессоров Intel при чтении 10 байт будут прочитаны 4096) и добавление в страничный кэш. Реальный же запрос на отображение файла только возвращает адрес на уже кэшированные страницы.

На уровне процесса работа может вестись как со страницами напрямую, так и через специальные структуры ядра.

3.2.2. Средства управления процессами

Средства управления процессами ОС Альт СП обеспечивают выполнение следующих функций:

1) управление процессами:

- создание процессов;
- управление процессами;
- удаление процессов;
- планирование процессорного времени;

2) распределение системных ресурсов;

3) синхронизация процессов и организация межпроцессного взаимодействия:

- сокеты;
- сигналы;
- каналы;
- очереди сообщений;
- семафоры;
- разделяемая память.

3.2.2.1. Управление процессами

Процессом в ОС Альт СП называется любая выполняющаяся программа. ОС Альт СП, как многозадачная система, характеризуется тем, что одновременно может выполняться множество процессов, принадлежащих одному или нескольким пользователям.

Одновременно в оперативной памяти может находиться несколько процессов, при этом каждому работающему процессу система присваивает уникальный PID (process identificator). Каждый процесс выполняется в собственном виртуальном адресном пространстве.

ОС Альт СП управляет образом процесса в оперативной памяти или сегментами кода и данных, определяющих среду выполнения. Сегмент кода, в свою очередь, содержит реальные инструкции центральному процессору. Данные, связанные с процессом, также являются частью образа процесса, и хранятся в

регистрах. Для оперативного хранения рабочих данных существует область памяти, выделяемая динамически, и способы ее использования меняются от процесса к процессу.

Процессы разделяются на: функционирующие на уровне ядра операционной системы (kernel-space) и функционирующие вне ядра операционной системы (user-space). Процессы, функционирующие на уровне ядра, запускаются самим ядром ОС, либо в виде подгружаемых модулей ядра. Процессы, функционирующие в системном окружении, запускаются стандартным для приложений ОС Альт СП методом.

3.2.2.1.1. Создание процесса

Процесс порождается с помощью системного вызова. При создании нового процесса выполняется следующее:

1) выделяется память для описателя нового процесса в таблице процессов;
2) назначается уникальный идентификатор процесса PID;
3) создается логическая копия процесса, который выполняет полное копирование содержимого виртуальной памяти родительского процесса, копирование составляющих ядерного статического и динамического контекстов процесса-предка;
4) увеличиваются счетчики открытия файлов (порожденный процесс наследует все открытые файлы родительского процесса);
5) возвращается идентификатор процесса PID в точку возврата из системного вызова в родительском процессе и 0 – в процессе-потомке.

При порождении процесса, для него создается свой блок управления, который помещается в системную таблицу процессов, находящихся в ядре ОС. Эта таблица представляет собой массив структур блоков управления процессами.

В каждом блоке содержатся следующие данные, отслеживаемые ядром ОС:

- слово состояния процесса;
- приоритет;
- величина кванта времени, выделенного системным планировщиком;
- степень использования системным процессором;

- признак диспетчеризации;
- идентификатор пользователя, которому принадлежит процесс;
- эффективный идентификатор пользователя;
- реальный и эффективный идентификаторы группы;
- группа процесса;
- идентификатор процесса и идентификатор родительского процесса;
- размер образа, размещаемого в области подкачки;
- размер сегментов кода и данных;
- массив сигналов, ожидающих обработки.

3.2.2.1.2. Управление процессом

Для управления процессами ОС Альт СП использует два основных типа информационных структур:

- дескриптор процесса – содержит информацию о состоянии процесса, расположении образа процесса в оперативной памяти и на диске, о значении отдельных составляющих приоритета, а также его итоговое значение – глобальный приоритет, идентификатор пользователя, создавшего процесс, информация о родственных процессах, о событиях, осуществления которых ожидает данный процесс и другую информацию;
- контекст процесса – содержит информацию о процессе, необходимую для возобновления выполнения процесса с прерванного места: содержимое регистров процессора, коды ошибок, выполняемых процессором системных вызовов, информацию обо всех открытых данным процессом файлов и незавершенных операциях ввода-вывода и другие данные, характеризующие состояние вычислительной среды в момент прерывания.

3.2.2.1.3. Завершение процесса

Завершение процесса выполняется с помощью системного вызова, при котором освобождаются все используемые ресурсы, такие как память и структуры таблиц ядра. Кроме того, завершаются и дочерние процессы, порожденные данным процессом. Затем из памяти удаляются сегменты кода и данных, после этого родительский процесс очищает все ресурсы, занимаемые дочерними процессами.

3.2.2.1.4. Планирование

В ОС Альт СП реализована вытесняющая многозадачность, основанная на использовании приоритетов и квантования.

Все процессы разбиты на несколько групп, называемых классами приоритетов. Каждая группа имеет свои характеристики планирования процессов.

Дочерний процесс наследует характеристики планирования родительского процесса, которые включают класс приоритета и величину приоритета в этом классе. Процесс остается в данном классе до тех пор, пока не будет выполнен системный вызов, изменяющий его класс. Существует три приоритетных класса приоритетов: класс реального времени, класс системных процессов и класс процессов разделения времени. Приоритетность процесса тем выше, чем больше число, выражающее приоритет.

Процессы системного класса используют стратегию фиксированных приоритетов. Системный класс зарезервирован для процессов ядра. Уровень приоритета процессу назначается ядром и никогда не изменяется.

Процессы реального времени также используют стратегию фиксированных приоритетов, но пользователь может их изменять. При наличии готовых к выполнению процессов реального времени другие процессы не рассматриваются.

Характеристики планирования процессов реального времени включают две величины: уровень глобального приоритета и квант времени. Для каждого уровня приоритета устанавливается по умолчанию своя величина кванта времени. Процессу разрешается использовать ресурсы процессора в течение указанного кванта времени, по истечении которого планировщик снимает данный процесс с выполнения.

В классе процессов разделения времени для распределения времени процессора между процессами используется стратегия динамических приоритетов, которая адаптируется к операционным характеристикам процесса.

Величина приоритета, назначаемого процессам разделения времени, вычисляется пропорционально значениям двух составляющих: пользовательской части и системной части. Пользовательская часть приоритета может быть изменена

суперпользователем root и владельцем процесса, но в последнем случае только в сторону его снижения.

Системная составляющая позволяет планировщику управлять процессами в зависимости от длительности использования ими ресурсов процессора, не уходя в состояние ожидания.

3.2.2.2. Распределение системных ресурсов

Для запуска процесса, выполняемого в ОС Альт СП, необходимы системные ресурсы, такие как память, порты ввода-вывода, память ввода-вывода, линии прерывания, а также каналы памяти прямого обращения DMA (Direct Access Memory).

Средства управления ресурсами, реализованные в ОС Альт СП, могут управлять произвольными ресурсами, объединяя их в иерархическую структуру. Глобальные ресурсы системы (например, порты ввода-вывода) могут быть разделены на подмножества – например, относящиеся к какому-либо слоту аппаратной шины. Определенные драйверы также при желании могут подразделять захватываемые ресурсы на основе своей логической структуры.

Область памяти, принадлежащая периферийному устройству, называется памятью ввода-вывода, чтение и запись портов и памяти ввода-вывода – работа драйвера. Порты и память ввода-вывода объединены общим названием – регион (или область) ввода-вывода.

Для предотвращения коллизий между различными устройствами в ОС Альт СП реализован механизм запроса/высвобождения регионов ввода-вывода (порты и память ввода-вывода). Этот механизм представляет программную абстракцию и не распространяется на аппаратные возможности.

Информация о зарегистрированных ресурсах доступна в текстовой форме и содержится в файлах `/proc/ioports` и `/proc/iomem`. Каждая строка данного файла отображает в шестнадцатеричном виде диапазон портов, связанных с драйвером или владельцем устройства.

3.2.2.3. Синхронизация процессов и организация межпроцессного взаимодействия

К средствам для организации межпроцессного взаимодействия в ОС Альт СП относятся: сокеты, сигналы, коммуникационные и именованные каналы, сообщения (очереди сообщений), семафоры и разделяемая память.

3.2.2.3.1. Сокеты

Сокет домена UNIX (Unix domain socket, UDS) или IPC-сокет (сокет межпроцессного взаимодействия) – конечная точка обмена данными между процессами, работающими в одной и той же системе UNIX.

Доменные соединения UNIX являются, по сути, байтовыми потоками, схожими с сетевыми соединениями, но при этом все данные остаются внутри одного компьютера (то есть обмен данными происходит локально).

UDS используют файловую систему как адресное пространство имен, то есть они представляются процессами как иноды в файловой системе (системой создается специальный файл сокета по заданному пути). Это позволяет двум различным процессам открывать один и тот же сокет для взаимодействия между собой (через файл сокета любые локальные процессы смогут сообщаться путем чтения/записи из него). Однако конкретное взаимодействие, обмен данными, не использует файловую систему, а только буферы памяти ядра.

Несмотря на то, что другие процессы распознают файлы сокетов как элементы каталога, чтение и запись файлов сокета могут осуществлять только те процессы, между которыми установлено соответствующее соединение.

Взаимодействие, основанное на использовании сокетов, является основным механизмом межсистемной и межпроцессной связи. Сокеты представляют собой программный интерфейс для обеспечения двусторонней связи типа «точка-точка» между двумя процессами. Интерфейс сокетов позволяет явно разделить во взаимодействии двух процессов серверную и клиентскую часть.

Взаимодействие процессов посредством сокетов может быть представлено в общем виде следующим алгоритмом:

- серверный процесс инициализирует сокет и привязывает его к определенному адресу и (или) порту, после этого переключает сокет в режим ожидания подключения от клиентского процесса;
- клиентский процесс инициализирует сокет и привязывает его к определенному адресу и (или) порту;
- клиентский процесс инициирует подключение к сокету серверного процесса.

После установки соединения информационный обмен между процессами может быть осуществлен в двустороннем направлении.

3.2.2.3.2. Сигналы

ОС Альт СП также обеспечивает возможность организации межпроцессного взаимодействия с помощью сигналов.

Сигналы представляют собой программные прерывания и позволяют уведомлять процесс или группу процессов о наступлении некоторого события. Когда сигнал послан процессу, ОС прерывает его выполнение. Источником сигнала может выступать как другой процесс, так и сама ОС.

Сигналы, посылаемые ОС, уведомляют о наступлении некоторых строго предопределенных ситуаций (например, завершение дочернего процесса, попытка выполнить недопустимую машинную инструкцию, попытка недопустимой записи в канал и другие), при этом каждому событию сопоставлен свой сигнал. Существуют также зарезервированные номера сигналов, семантика которых определяется пользовательскими процессами по своему усмотрению (например, процессы могут посылать друг другу сигналы с целью синхронизации).

Сигналы являются механизмом асинхронного взаимодействия. При получении сигнала процессом возможны три варианта реакции на полученный сигнал:

- процесс реагирует на сигнал стандартным образом, установленным по умолчанию (для большинства сигналов действие по умолчанию – это завершение процесса);

- процесс может установить специальную обработку сигнала, в этом случае по приходу сигнала вызывается функция-обработчик, определенная процессом;
- процесс может проигнорировать сигнал.

3.2.2.3.3. Каналы

В ОС Альт СП взаимодействие между процессами осуществляется также с помощью неименованных и именованных каналов. Файлы данного типа подобны сокетам, поскольку тоже используются для взаимодействия между процессами, однако, в отличие от сокетов, в неименованных каналах данные передаются только в одном направлении.

Взаимодействие между родительским процессом и дочерним (процесс, порожденный родительским процессом) осуществляется по неименованному каналу, который представляет собой программный однонаправленный канал передачи данных между двумя родственными процессами (родителем и потомком). При необходимости двунаправленного информационного обмена родительский процесс создает два канала. Посторонний субъект вмешаться в обмен данными не может, так как обращение к неименованным каналам осуществляется только через механизм файловых дескрипторов, которые наследуются при порождении нового процесса.

Взаимодействие между независимыми процессами осуществляется по именованному каналу. Именованные каналы являются одним из способов обмена данными между изолированными процессами. Именованный канал обеспечивает возможность взаимодействия процессов, выполняющихся как на одной, так и на разных ПЭВМ, объединенных в локальную сеть.

Именованный канал создается явно с помощью команды `mkfifo`, и два различных процесса могут обратиться к нему по имени.

3.2.2.3.4. Очереди сообщений

Очередь сообщений представляет собой механизм, позволяющий процессам асинхронно посылать сообщения друг другу. Когда сообщение получено процессом, оно удаляется из очереди. Очередь сообщений существует независимо от процесса-источника и процесса-приемника: процесс-источник может отправить сообщение в

очередь и завершиться, а сообщение, тем не менее, будет получено процессом-приемником. Сообщениям могут быть назначены приоритеты. Высокоприоритетные сообщения всегда принимаются первыми, независимо от количества сообщений в очереди.

3.2.2.3.5. Семафоры

Для синхронизации процессов в ОС Альт СП применяются семафоры. Семафоры используются как блокирующий механизм, позволяющий разграничить доступ параллельно работающих процессов к критическим информационным ресурсами и исключить возможность использования сегмента памяти двумя процессами одновременно.

3.2.2.3.6. Разделяемая память

Разделяемая память используется для того, чтобы увеличить скорость обмена данными между процессами. В большинстве случаев обмен информацией между процессами осуществляется через ядро, в то время как механизм взаимодействия процессов посредством разделяемой памяти позволяет осуществить обмен информацией, используя некоторую часть виртуального адресного пространства, куда помещаются и откуда считываются данные. После добавления разделяемого сегмента памяти к собственному виртуальному пространству пользовательский процесс может работать с ним как с обычным сегментом памяти.

3.2.3. Средства работы с файлами

Средства работы с файлами ОС Альт СП обеспечивают возможность работы с файлами, ссылками, каталогами и разделами и поддерживает следующие файловые системы:

1) общий интерфейс к файловым системам VFS (Virtual File System);
2) файловые системы, поддерживающие дискреционный контроль доступа к информации:
   - сетевая файловая система NFS (Network File System);
   - файловая система ReiserFS;
   - файловая система ext2 (Second Extended File System);

- файловая система ext3 (Third Extended File System);
- файловая система ext4 (Fourth Extended File System);
- файловая система XFS;
- файловая система JFS (Journaled File System);
- распределенная сетевая файловая система CEPH;
- распределенная сетевая файловая система GlusterFS.

ОС Альт СП позволяет выполнять следующие операции с файлами:

- создание и просмотр файла;
- копирование файла;
- переименование и перемещение файлов;
- запуск исполняемых файлов;
- удаление файлов;
- поиск файлов;
- изменение прав доступа к файлам.

Примечание. Для каждого файла в ОС Альт СП устанавливаются права доступа.

Жесткая ссылка представляет собой дополнительное имя для исходного файла и ссылается на номер индексного дескриптора исходного файла, следовательно, такие ссылки могут указывать только на файлы, расположенные в той же файловой системе, что и жесткая ссылка. При изменении файла жесткой ссылки, автоматически изменяется и обычный файл. При удалении жесткой ссылки, файл удаляется только в том случае, если на него нет больше жестких ссылок, в противном случае удаляется только ссылка.

Символическая ссылка представляет собой файл, при обращении к которому ОС обращается к другому файлу. В отличие от жестких ссылок символические ссылки могут указывать на файлы, расположенные в другой файловой системе, например, на монтируемом носителе, или другом компьютере. В случае, если исходный файл удален, символическая ссылка не удаляется, но становится бесполезной. Символическая ссылка не имеет прав доступа, она наследует права доступа от файла, на который ссылается.

ОС Альт СП позволяет выполнять следующие операции с каталогами:

- просмотр содержимого каталога;
- вывод имени текущего каталога;
- создание и удаление каталога;
- смена каталога;
- изменение прав доступа к каталогу.

В случае, если дисковый накопитель из состава ПЭВМ разбит на разделы, на каждом разделе организуется отдельная файловая система с собственной структурой каталогов. Для пользователя файловая система представляет собой единое целое. В действительности, разные части файловой системы могут находиться на разных устройствах: разделах дискового накопителя, съемных носителях информации.

ОС Альт СП позволяет выполнять следующие операции с разделами:

- создание раздела;
- монтирование, размонтирование раздела;
- форматирование раздела;
- проверка файловой системы раздела.

3.2.4. Система ввода-вывода

Система ввода-вывода обеспечивает выполнение следующих функций:

- доступ к внешним устройствам;
- буферизация данных;
- взаимодействие с программами управления внешними устройствами ПЭВМ;
- службы управления печатью.

3.2.4.1. Доступ к внешним устройствам

В ОС Альт СП доступ к физическому устройству осуществляется с помощью специального файла устройства. При выполнении с файлом устройства операций открытия, чтения или записи осуществляется обмен данными с физическим устройством. Файлы устройств хранятся в каталоге `/dev`.

В ОС Альт СП используются стандартные имена устройств:

- ttyN – консоль;

- mouse – манипулятор типа «мышь»;
- audio – звуковая карта;
- modem – модем;
- ttySN – последовательный порт;
- lpN – параллельный порт;
- cuaN – могут обозначать последовательные порты;
- sdxN – накопитель на жестких магнитных дисках;
- fd0 – первый дисковод для гибких дисков;
- stN – стример с интерфейсом SCSI;
- nrtfN – запоминающее устройство на принципе магнитной записи на ленточном носителе, с последовательным доступом к данным с интерфейсом FDC;
- mdN – массив RAID;
- ethN – сетевая плата;
- null – пустое устройство.

П р и м е ч а н и е . N – номер устройства (например, tty1 – первая консоль).

3.2.4.2. Буферизация данных

Средства буферизации выполняет функцию кэш-памяти по отношению к дисковому накопителю. Кэширование дискового накопителя уменьшает среднее время доступа к данным, хранящимся на нем. Любой запрос на ввод/вывод к физическому устройству преобразуется в запрос к подсистеме буферизации, которая представляет собой буферный пул и комплекс программ управления пулом.

Буферный пул состоит из буферов, находящихся в области ядра. Размер отдельного буфера равен размеру блока данных на дисковом накопителе.

С каждым буфером связана специальная структура – заголовок буфера, в котором содержится следующая информация:

1) данные о состоянии буфера:

- занят/свободен;
- чтение/запись;

- признак отложенной записи;
- ошибка ввода-вывода;

2) данные об устройстве – источнике информации, находящейся в этом буфере:
   - тип устройства;
   - номер устройства;
   - номер блока на устройстве;
   - адрес буфера;
3) ссылка на следующий буфер в очереди свободных буферов, назначенных для ввода-вывода какому-либо устройству.

Запрос к подсистеме буферизации выполняется с помощью следующих основных функций:

- функции синхронной записи;
- функции асинхронной записи;
- функции отложенной записи;
- функций получения блока данных.

В результате выполнения функции синхронной записи немедленно инициируется физический обмен с внешним устройством, процесс, выдавший запрос, ожидает результат выполнения операции ввода-вывода. В данном случае в процессе может быть предусмотрена собственная реакция на ошибочную ситуацию. Такой тип записи используется, когда необходима гарантия правильного завершения операции ввода-вывода.

В результате выполнения функции асинхронной записи также немедленно инициируется физический обмен с устройством, однако завершения операции ввода-вывода процесс не дожидается. В этом случае возможные ошибки ввода-вывода не могут быть переданы в процесс, выдавший запрос. Такая операция записи целесообразна при поточной обработке файлов, когда ожидание завершения операции ввода-вывода не обязательно, но есть уверенность в повторении этой операции.

В результате выполнения функции отложенной записи передача данных из системного буфера не производится. В заголовке буфера создается отметка о том, что буфер заполнен и может быть выгружен, если потребуется его освободить.

Каждая из функций получения блока данных ищет в буферном пуле буфер, содержащий указанный блок данных. В случае, если такой блок в буферном пуле отсутствует, осуществляется поиск любого свободного буфера (при этом возможна выгрузка на дисковый накопитель буфера, содержащего в заголовке признак отложенной записи), либо организуется его загрузка в какой-нибудь свободный буфер. В случае, если свободные буферы отсутствуют, производится выгрузка буфера с отложенной записью.

3.2.4.3. Взаимодействие с программами управления внешними устройствами ПЭВМ

Программы управления внешними устройствами ПЭВМ предназначены для управления передачей данных между внешним устройством и оперативной памятью ПЭВМ.

Связь ядра ОС с такими программами обеспечивается с помощью двух системных таблиц:

- таблица блок-ориентированных устройств (устройства, например, дисковые накопители, информация на которых хранится в блоках фиксированного размера, имеющих свой собственный адрес);
- таблица байт-ориентированных устройств (устройства, например, терминалы, сетевое оборудование, генерирующие или потребляющие последовательность байтов).

Для связи используется следующая информация из индексных дескрипторов специальных файлов:

- класс устройства (байт-ориентированное или блок-ориентированное);
- тип устройства (ленточный носитель, накопитель на гибком магнитном диске, накопитель на жестком магнитном диске, устройство печати, дисплей, канал связи и другие);
- номер устройства.

Класс устройства определяет выбор таблицы блок- или байт-ориентированных устройств. Эти таблицы содержат адреса программных секций драйверов. Тип устройства определяет выбор драйвера.

3.2.4.4. Службы управления печатью

В ОС Альт СП основной системой печати является сервер печати Common UNIX Printing System (далее – CUPS).

Сервер печати CUPS функционирует в виде отдельной службы и может управляться администратором (предусмотрена возможность частично передавать права по управлению заданиями пользователя).

В состав сервера печати CUPS входят следующие компоненты:

- диспетчер очереди печати (планировщик);
- средства фильтрации;
- Back-end-система.

Сервер печати CUPS работает в соответствии со следующим алгоритмом:

- сервер печати принимает задание на печать от программы (активного процесса) и передает его диспетчеру очереди печати или планировщику;
- диспетчер очереди печати добавляет задание на печать в соответствующую очередь;
- диспетчер очереди печати передает задание на печать в соответствии с очередью системе фильтрации;
- средства фильтрации обрабатывают данные: осуществляет все необходимые преобразования данных в соответствии с применяемыми для этого задания фильтрами и переводит их в формат, понятный принтеру.

3.2.5. Средства администрирования

Средства администрирования обеспечивают возможность выполнения настройки конфигурации ОС, в частности:

- установка ОС Альт СП и назначение параметров системы;
- создание загрузочных дисков;
- конфигурирование параметров даты и времени, графической среды, средств ввода и вывода;

- настройка и управление системными сервисами и служебными программами;
- настройка и управление системой управления пакетами Advanced Packaging Tool (далее – APT);
- 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 и управление кэширующими прокси-серверами;
- настройка серверов электронной почты postfix;
- настройка серверного и клиентского ПО;
- настройка и управление базами данных;
- настройка и управление печатью;
- настройка подключаемых носителей;
- управление встроенным межсетевым экраном;
- настройка и управление виртуальными машинами;
- настройка и управление средствами контейнеризации;
- настройка и управление системой управления базами данных;
- настройка PHP;
- настройка и управление удаленным доступом по ssh;
- настройка и управление NTP.

Примечание. Защита от ошибочных действий администратора предусматривает их обнаружение и отображение компонентами операционной системы.

3.2.6. Комплекс средств защиты

КСЗ предназначен для обеспечения безопасности информации, хранящейся и обрабатываемой в ПЭВМ.

КСЗ обеспечивает выполнение следующих функции безопасности:

- идентификация и аутентификация;
- управление доступом;
- регистрация событий безопасности;
- ограничение программной среды;
- изоляция процессов;
- защита памяти;
- контроль целостности;
- обеспечение надежного функционирования;
- фильтрация сетевого потока.

3.2.6.1. Регистрация событий безопасности

Механизм аудита состоит из нескольких компонентов:

1) модуль ядра – перехватывает системные вызовы (syscalls) и выполняет регистрацию событий;
2) служба auditd – записывает зарегистрированное событие в файл;
3) служба audispd – осуществляет пересылку сообщений (выступает в роли диспетчера) к другому приложению;
4) ряд вспомогательных программ:
    - auditctl – программа, управляющая поведением системы аудита и позволяющая контролировать текущее состояние системы, создавать или удалять правила;
    - aureport – программа, генерирующая суммарные отчеты о работе системы аудита;
    - ausearch – программа, позволяющая производить поиск событий в журнальных файлах;
    - autrace – программа, выполняющая аудит событий, порождаемых указанным процессом.

Программы отсылают записи, предназначенные для протоколирования, системному демону auditd, который идентифицирует тип каждой пришедшей записи и обрабатывает запись способом, определенным для данного типа.

Для каждого из регистрируемых событий в журналах функции безопасности собирают следующую информацию:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то указываются объект и тип доступа);
- успешность осуществления события (обслужен запрос на доступ или нет).

ОС Альт СП обеспечивает:

- возможность просмотра журнала аудита только администратору системы;
- возможность поиска событий в журнале аудита;
- возможность выбора совокупности событий, подвергающихся аудиту;
- обеспечивает предотвращение потери данных аудита при переполнении журнала регистрации за счет записи событий поверх старых хранимых записей аудита, а также за счет передачи данных аудита для внешнего хранения.

Функции безопасности ОС Альт СП способны генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту:

- запуск и завершение выполнения функций аудита;
- действия, предпринимаемые в ответ на возможные нарушения безопасности;
- все модификации конфигурации аудита;
- чтение информации из записей аудита;
- неуспешные попытки читать информацию из записей аудита;
- предпринимаемые действия при сбое хранения журнала аудита;
- все запросы на выполнение операций на объекте, на который распространяются политики функций безопасности;
- все попытки экспортировать информацию;
- все решения по запросам на информационные потоки;
- достижение ограничения неуспешных попыток аутентификации и предпринятые действия, а также, при необходимости, последующее восстановление нормального состояния (блокирование учетной записи в

результате превышения максимального числа неуспешных попыток входа в систему);

- отклонение или принятие функции безопасности любого проверенного секрета;
- все случаи использования механизма аутентификации;
- результат действия каждого активизированного механизма аутентификации вместе с итоговым решением;
- все случаи использования механизма идентификации пользователя, включая представленный идентификатор пользователя;
- успешное или неуспешное связывание атрибутов безопасности пользователя с субъектом;
- все модификации режима выполнения функций из числа функции безопасности;
- все модификации значений атрибутов безопасности (включая все модификации значений атрибутов безопасности, используемых для смены начальной аутентификационной информации пользователя ОС после однократного использования);
- модификации настройки по умолчанию разрешающих или ограничительных правил;
- все модификации начальных значений атрибутов безопасности;
- все модификации значений данных функции безопасности (включая все модификации аутентификационной информации);
- все модификации ограничений данных функции безопасности;
- все модификации действий, предпринимаемых при нарушениях ограничений;
- назначение срока действия для атрибута;
- действия, предпринятые по истечении назначенного срока;
- запись аудита для событий, связанных с истечением установленного администратором срока действия пароля;

- запись аудита для событий, связанных с истечением установленного администратором срока действия идентификатора пользователя ОС;
- использование функций управления;
- модификация группы пользователей;
- выполнение и результаты самотестирования функции безопасности;
- тип сбоя или прерывания обслуживания;
- изменения внутреннего представления времени;
- все операции ОС Альт СП, прерванные из-за сбоя;
- все попытки использования функции распределения ресурсов с учетом приоритетности обслуживания;
- все обращения к функциям распределения ресурсов, управляемых функции безопасности;
- отклонение нового сеанса, основанное на ограничении числа параллельных сеансов;
- все попытки разблокирования интерактивного сеанса;
- завершение интерактивного сеанса механизмом блокирования сеанса;
- все попытки открытия сеанса пользователя;
- полнотекстовая запись привилегированных команд (команд, управляющих системными функциями);
- применение механизма восстановления информации;
- изменение настроек механизмов уничтожения (стирания) данных;
- сбои в работе механизма изоляции процессов;
- попытки установки внешних модулей уровня ядра, не проверенных разработчиком (производителем), или внешних модулей уровня ядра с нарушенной целостностью;
- попытки запуска компонентов программного обеспечения, произведенных в нарушение установленных правил запуска компонентов программного обеспечения.

При обнаружении потенциального нарушения безопасности ОС Альт СП имеет возможность информировать администратора системы.

ОС Альт СП способен передавать данные аудита по протоколу syslog и защищать от несанкционированного раскрытия, за счет передачи данных в нечитаемом виде.

3.2.6.2. Идентификация и аутентификация

В ОС Альт СП для предотвращения несанкционированного доступа субъекта доступа (пользователя) в программную среду используются механизмы идентификации (определение пользователя по имени – логину) и аутентификации (подтверждение подлинности имени пользователя с помощью пароля) пользователя. Процедуры идентификации и аутентификации пользователя выполняются при каждой попытке доступа в ОС.

Функции безопасности ОС Альт СП обеспечивают, чтобы все пользователи ОС были успешно идентифицированы и аутентифицированы до разрешения любого действия, выполняемого при посредничестве функции безопасности от имени этого пользователя ОС, требуют предъявления уникального идентификатора и пароля или аутентификационной информации из электронного идентификатора.

Администратор системы устанавливает:

- требования к сложности паролей, функции безопасности способны верифицировать, что пароль отвечает установленным требованиям;
- максимальное количество неуспешных попыток аутентификации, функции безопасности способны заблокировать учетную запись при превышении неуспешных попыток аутентификации.

ОС Альт СП хранит следующую информацию о пользователе:

- имя пользователя – регистрационное имя субъекта доступа;
- идентификатор пользователя – индивидуальный числовой идентификатор субъекта доступа, используемый при выполнении процедуры идентификации в ОС (задается из диапазона «0..65535», число «0» соответствует пользователю root);
- идентификатор группы – числовой идентификатор первичной группы пользователя (помимо первичной группы пользователь может входить в состав других групп, идентификатор группы 0 соответствует группе root);

- пароль – пароль пользователя;
- срок действия идентификаторов (учетных записей) пользователей ОС;
- домашний каталог пользователя – в качестве домашнего каталога используется каталог /home/<имя пользователя >;
- оболочка субъекта доступа – командный интерпретатор пользователя, который используется им по умолчанию (запускается при входе пользователя в ОС).

Информация о пользователе хранится в файле /etc/passwd, пароли в зашифрованном виде хранятся в файле /etc/tcb/<имя пользователя >/shadow.

Пользователю ОС предоставляются только условные знаки во время выполнения аутентификации. Функции безопасности ОС предотвращают хранение и чтение аутентификационной информации в открытом виде.

Процедура идентификации и аутентификации субъекта в ОС Альт СП выполняется в соответствии со следующим алгоритмом:

- пользователь посылает запрос на доступ в ОС Альт СП;
- автоматически системой вызывается программа login, (используется для запуска нового сеанса в системе), которая выводит приглашение login на терминал пользователя;
- пользователь предъявляет свое регистрационное имя (далее – логин) и пароль;
- модули переключателя служб имен Name Service Switch (далее – NSS) перехватывают логин пользователя и осуществляют его поиск в файлах виртуальной базы данных пользователей системы (для конфигурации источников виртуальной БД пользователей используется файл /etc/nsswitch.conf): в файлах /etc/passwd, /etc/shadow, /etc/group;
- если модули NSS находят логин пользователя в файлах /etc/passwd, /etc/shadow, /etc/group, система обращается к подключаемым модулям аутентификации, Pluggable Authentication Modules (далее – PAM) и запускается процесс аутентификации;

- модули PAM сравнивают логин и пароль, предъявленные пользователем со значениями, хранящимися в базе данных: в файлах `/etc/passwd`, `/etc/shadow`, `/etc/group`;
- если введенные имя и пароль субъекта соответствуют значениям, хранящимся в базе данных, КСЗ предоставляет доступ субъекту в ОС, информация о результате попытки доступа сохраняется в системном журнале `/var/log/`;
- если введенные имя и пароль субъекта не идентичны значениям, хранящимся в базе данных, КСЗ отклоняет запрос доступа субъекта в ОС (для выполнения повторной попытки аутентификации субъект должен инициировать новый запрос доступа), информация о результате попытки доступа сохраняется в системном журнале.

В конфигурации файла `/etc/nsswitch.conf` можно указать несколько источников файлов базы данных пользователей, например, в качестве источника указать дерево каталогов LDAP. В случае, если логин и пароль пользователя будут отсутствовать в файлах `/etc/passwd`, `/etc/shadow`, `/etc/group`, модули NSS осуществляют поиск в дереве каталогов LDAP, после чего соответствующие модули PAM выполняют аутентификацию пользователя (или оповещают об ошибке в случае несоответствия логина и пароля).

В случае необходимости реализации сетевой аутентификации пользователей в системе предусмотрена возможность аутентификации с помощью Kerberos с хранением информации о пользователях в дереве каталогов LDAP (Kerberos может использоваться и для осуществления локальной аутентификации пользователей).

3.2.6.3. Управление доступом

ОС Альт СП реализует дискреционное управление доступом.

Дискреционное разграничение доступа осуществляется для:

1) субъектов доступа (процессов, порождаемых пользователями ОС);

2) объектов доступа (файлов, каталогов, устройств);

3) операций субъектов доступа над объектами доступа (чтение, запись, выполнение), основываясь на:

- атрибутах субъектов доступа: GID, UID, SUID, SGID;
- атрибутах объектов доступа: GID владельца, UID владельца;
- атрибутах безопасности контроля доступа: список контроля доступа для определенных UID, список контроля доступа для определенных GID, права доступа для владельца объекта (если используется список контроля доступа ACL, то права доступа для владельца объекта, указанные в ACL), права доступа для группы владельца объекта (если используется список контроля доступа ACL, то права доступа для группы владельца объекта, указанные в ACL), эффективная маска, права доступа для пользователя «все остальные», права доступа, STICKY BIT, IMMUTABLE, APPEND.

Функции безопасности ОС предоставляют администратору системы возможность назначать начальные значения по умолчанию атрибутов объектов доступа при создании объекта.

В соответствии с дискреционным принципом управления доступом для каждого файла и каталога в ОС Альт СП устанавливаются права доступа, определяющие возможность доступа пользователя к объекту доступа (файл, каталог), а также возможные операции над ним.

Права доступа устанавливаются отдельно для различных категорий пользователей:

- владелец – пользователь, создавший файл (для того чтобы создать файл необходимо иметь право записи в каталог, в котором создается файл, при этом для владельца устанавливаются права на чтение и запись, для всех остальных пользователей – только на чтение);
- группа – набор пользователей, организованных, например, для работы с определенным набором файлов (владелец может разрешить или запретить доступ к файлам для членов группы);
- прочие – все остальные пользователи.

Основными операциями, выполняемыми над объектами доступа в ОС Альт СП, являются следующие:

- чтение (read, r);
- запись (write, w);
- исполнение (execution, x).

Чтение для файла означает право получать содержимое по индексному дескриптору. Для каталога – означает право получать список имен объектов, содержащихся в нем. В случае, если доступ на чтение к каталогу запрещен, процесс не сможет получить список имен, однако доступ непосредственно к файлу, находящемуся в каталоге, регулируется правом использования (исполнения) каталога, а не правом чтения.

Запись для файла означает право модифицировать содержимое по индексному дескриптору. Для каталога – означает право модифицировать список файлов. Без права на использование (исполнение) каталога право на запись практически неприменимо.

Использование для файла означает право запускать его в качестве программы. Различают бинарные исполняемые файлы, которые непосредственно загружаются в память в виде процесса (возможно, посредством динамической компоновки с разделяемыми библиотеками) и сценарии, для выполнения которых запускается процесс из другого файла, а текущий файл отдается ему в качестве параметра командной строки (следовательно, для работы запускаемого сценария требуется также доступ на чтение).

Для каталога доступ на использование (исполнение) означает право преобразовывать имена объектов, находящихся в каталоге, в индексные дескрипторы. Список имен файлов в каталоге, доступном процессу на чтение, но не на использование, будет виден, но сами файлы останутся недоступны.

Для работы с блочными и символьными устройствами в ОС при монтировании создаются специальные файлы, обеспечивающие произвольный или последовательный доступ соответственно типу устройства, которому они назначаются. Права доступа для учетных записей пользователя и вызываемых процессов назначаются на соответствующий созданный файл.

Права доступа к локальным сокетам назначаются на специальный файл сокета по заданному пути, через который к сокету будут сообщаться любые локальные процессы путем чтения/записи из него. При использовании сетевого сокета, создается абстрактный объект, привязанный к слушающему порту операционной системы и сетевому интерфейсу, затем ему присваивается INET-адрес, который имеет адрес интерфейса и слушающего порта, и далее обращение будет происходить к абстрактному объекту согласно назначенным правам.

Права доступа именованного канала аналогичны правам доступа к файлу. Обращение к именованному каналу осуществляется также, как и к обычному файлу. В связи с этим, для работы с именованными каналами процессам необходимо предоставлять права доступа для чтения (записи) из (в) канал. При создании канала необходимо учитывать, что каналы создаются с правами доступа «0666», модифицированными маской прав доступа umask(2) вызывающего процесса. Также, утилита создания канала требует право на запись в родительский каталог.

Права доступа к символьным ссылкам всегда выглядят как «rwxrwxrwx», поскольку при использовании ссылки драйвер файловой системы пересчитывает реальный путь к файлу и применяет права доступа, определенные для реального пути уже без учета самой символьной ссылки.

При вычислении прав доступа принимается во внимание уровень доступа процесса к файлу, который вычисляется следующим образом:

- если UID файла и актуальный UID процесса совпадают, процесс считается владельцем файла;
- в противном случае, если GID файла совпадает с актуальным GID процесса или входит в список групп, процесс считается членом группы;
- если оба условия не выполнены, процесс считается чужим по отношению к файлу.

Права доступа включают список из девяти атрибутов (битов) файла, записываемых в форме «rwxrwxrwx»: по три вида доступа (чтение – read, запись – write, исполнение – execute) для трех групп – пользователя-владельца (u), группы-владельца (g) и всех остальных (o) соответственно. Каждый пункт в этом списке может быть либо разрешен, либо запрещен (равен 1 или 0). В случае, если

некоторый доступ запрещен на некотором уровне, вместо символа пишется знак «-». Атрибуты неотторжимы от файла, так как хранятся в его метаданных (индексном дескрипторе), и не зависят от количества имен (ссылок на файл) и их расположения в дереве каталогов.

Права доступа файлового объекта могут быть изменены, если это разрешено текущими правилами (санкционировано). Модифицировать права доступа может только процесс-владелец (пользователь-владелец) файла, либо суперпользовательский (запущенный от имени пользователя root) процесс (UID процесса = 0).

Описанные выше права выставляются с помощью функции umask (user file creation mode mask). Umask одинаковым образом работает для всех объектов: каждый установленный бит umask запрещает выставление соответствующего бита прав. Исключением из этого запрета является бит исполняемости, который для обычных файлов зависит от создающей программы (трансляторы ставят бит исполняемости на создаваемые файлы, другие программы – нет), соответственно, исключением являются сокеты и каналы межпроцессного взаимодействия и монтируемые аппаратные устройства. В случае каталогов umask следует общему правилу.

При обращении процесса к объекту (с запросом доступа определенного вида) система проверяет совпадение идентификаторов владельцев процесса и владельцев файла в определенном порядке, и в зависимости от результата, применяет ту или иную группу прав.

В случае, если текущими правилами разрешено (санкционировано), права доступа файлового объекта могут быть изменены.

Кроме общей схемы разграничения доступа ОС Альт СП поддерживает также ACL, с помощью которых можно для каждого объекта задавать права всех субъектов на доступ к нему.

Механизм дискреционного разграничения доступа обеспечивает возможность санкционированного изменения списка пользователей и списка защищаемых файловых объектов.

При осуществлении резервного копирования файлов и каталогов функции безопасности ОС экспортируют данные пользователя с атрибутами безопасности.

Функции безопасности ОС запрещают пользователям модифицировать ядро и его драйверы/модули, журналы аудита безопасности, общие библиотеки, системные исполняемые файлы, файлы конфигурации системы, а также запрещают пользователям читать данные аудита событий безопасности ОС.

Функции безопасности ОС предоставляют возможность ограничить максимальное число параллельных сеансов, предоставляемых одному и тому же пользователю ОС.

Администратор имеет возможность установки интервала времени бездействия пользователя ОС, по истечение которого функции безопасности блокируют интерактивный сеанс пользователя ОС. При этом пользователю ОС также предоставлена возможность инициации блокирования своего собственного интерактивного сеанса.

При блокировании сеанса производится очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида, а также блокирование любых действий по доступу к данным пользователя (устройствам) отображения, кроме необходимых для разблокирования сеанса. Для разблокировки требуется повторная аутентификация пользователя ОС.

Функции безопасности ОС способны отказать в открытии сеанса, основываясь на идентификаторе пользователя ОС, сроке действия идентификатора пользователя ОС, аутентификационной информации, атрибутах, связанных с временем доступа в ОС.

Внешняя память, используемая ОС, располагается на отдельном разделе диска, представленном в файловой системе специальным файлом, доступ к которому непосредственно из программы контролируется дискреционными ПРД. По умолчанию доступ к разделам диска имеет только доверенный субъект или член группы «disk».

При первоначальном назначении или при перераспределении внешней памяти КСЗ может ограничивать доступ субъекта к остаточной HDD-информации через механизм «безопасного удаления» файлов (специальный атрибут файла,

указывающий на необходимость перезаписи физической области носителя диска после удаления файла). Еще одним способом является использование команды shred, обеспечивающей безопасное удаление файлов.

3.2.6.4. Ограничение программной среды

Функции безопасности ОС:

- предоставляют возможность установки ПО только администратору системы;
- обеспечивают возможность задания перечня компонентов программного обеспечения, разрешенных и запрещенных для автоматического запуска при загрузке ОС;
- обеспечивают возможность задания перечня компонентов программного обеспечения, разрешенных и запрещенных для запуска в процессе функционирования ОС за счет использования технологии NOT EXECUTE BIT (бит запрета исполнения). Установка бита исполнения позволена только администратору системы;
- контролирует запуск компонентов ПО и при обнаружении попытки запуска компонентов ПО, произведенных в нарушение установленных правил запуска компонентов ПО, обеспечивает блокирование попытки запуска, а также оповещение пользователя, выполняющего запуск, и администратора системы.

3.2.6.5. Изоляция процессов

ОС Альт СП предоставляет для каждого процесса в системе собственное изолированное адресное пространство. Каждый процесс работает со своими виртуальными адресами (в своем виртуальном адресном пространстве), трансляция которых в физические выполняется на аппаратном уровне с помощью ядра ОС.

Пользовательский процесс лишен возможности напрямую обратиться к страницам основной памяти, занятым информацией, относящейся к другим процессам. В результате процессы становятся изолированными друг от друга. Физическая память распределяется независимо от распределения виртуальной памяти отдельного процесса. Для всех процессов ОС выделяет случайные области оперативной памяти.

Функции безопасности ОС для изоляции параллельных процессов осуществляют управление временем использования процессами общих ресурсов, именование процессов, предоставление процессу виртуального адресного пространства, блокируют попытки удаления файлов, находящихся в специальных каталогах, на которые установлена функция блокирования, если в момент обращения к файлу процесса он используется другим процессом.

3.2.6.6. Защита памяти

По завершению работы активного процесса ОС Альт СП осуществляет очистку оперативной памяти (RAM-памяти), предоставляемой этому процессу. Очистка оперативной памяти осуществляется посредством записи нулей или маскирующей информации в память при ее освобождении (перераспределении).

Очистка освобождаемых областей оперативной памяти происходит в процессе перевода ядром ОС каждой страницы памяти в разряд «неиспользуемых» (free). Это означает, в числе прочего, что ни одна страница из числа неиспользуемых не будет содержать данных, которые там размещала ОС или приложения в процессе работы системы. Ядро высвобождает страницы, начинающиеся с указанной, размера [размер_страницы * (2 ^ кратность)]. Область возвращается в массив свободных областей в соответствующую позицию и после этого происходит попытка объединить несколько областей для создания одной большего размера.

В работающей системе информация об очистке освобождаемых областей памяти доступна в каталоге виртуальной служебной файловой системы `/sys/kernel/mm/sanitize_memory/`. Здесь файл `level` содержит значение параметра `smem`, а файл `count` – количество памяти в байтах, обработанной подсистемой очистки. Очистка освобождаемых областей памяти не распространяется на swap.

ОС Альт СП поддерживает механизм «безопасного удаления» файлов. Для надежного удаления информации используется утилита командной строки shred, которая способна многократно перезаписывать уничтожаемые объекты специальными битовыми последовательностями.

В ОС Альт СП реализована технология ASLR, которая обеспечивает защиту от выполнения произвольного кода вследствие переполнения буфера путем рандомизации размещения адресного пространства.

3.2.6.7. Контроль целостности

Под целостностью подразумевается свойство неизменности исполняемого программного кода и настроек. По перечню параметров, определяемому в конфигурационном файле, создается база данных, в которой содержится определенный набор параметров, описывающих состав и конфигурацию программного кода. Считается, что эти параметры должны оставаться неизменными в процессе функционирования системы, а любое изменение одного из них является сигналом о том, что была произведена попытка нелегального доступа. Также на основе различных алгоритмов создается контрольная сумма, которая должна оставаться неизменной. База данных, созданная в условиях, когда попытка нелегального доступа невозможна, считается эталонной. Выбранные объекты системы с параметрами, занесенными в эталонную базу данных, хранятся в их текущем состоянии в качестве эталонных.

Созданная в процессе работы база данных считается рабочей. Рабочая база данных сравнивается с эталонной во время загрузки ОС, далее периодически в процессе работы, а также по запросу администратора системы. Параметры сравнения определяются конфигурационным файлом. В случае совпадения баз данных считается, что целостность системы не нарушена. В случае возникновения события несоответствия рабочей и эталонной баз данных, информация о событии заносится в системный журнал при помощи средств протоколирования.

Функции безопасности контролируют целостность:

- компонентов ПО, разрешенного для запуска, и при обнаружении попытки запуска компонентов программного обеспечения, целостность которых была нарушена, обеспечивают оповещение администратора системы и блокируют попытки запуска;
- компонентов, критически важных для функционирования средств виртуализации, и данных средств виртуализации.

3.2.6.8. Обеспечение надежного функционирования

В ОС Альт СП реализована клиент-серверная система создания и управления резервными копиями данных, а также их резервного восстановления. В том числе резервное копирование виртуальных машин (контейнеров), данных средств виртуализации.

Функции безопасности ОС позволяют создавать отказоустойчивый кластер, обеспечивающий доступность сервисов и информации, при выходе из строя одного из технических средств.

При недоступности или повреждении файла аутентификационной информации функции безопасности ОС блокируют все попытки аутентификации.

Каждому субъекту доступа устанавливается приоритет доступа к процессору. Предусмотрена возможность реализации максимальных квот процессов и оперативной памяти, которые отдельные пользователи ОС могут использовать одновременно.

Генерирование временных меток и синхронизация системного времени в ОС обеспечиваются средствами openntpd. Предусмотрена возможность синхронизации локального системного времени с удаленными NTP серверами.

3.2.6.9. Фильтрация сетевого потока

ОС Альт СП осуществляет фильтрацию сетевого потока для отправителей информации, получателей информации, сетевого трафика и всех операций перемещения контролируемой ОС информации сетевого трафика к узлам информационной системы и от них, на которые распространяется фильтрация сетевого потока.

Разграничение доступа к сетевому взаимодействию в ОС выполняется посредством пакета iptables, в рамках выполнения следующих функций:

- сбор статистики по сетевому трафику (учета статистики пакетов);
- разграничения доступа к сети отдельным приложениям;
- разграничения доступа к сети для определенных пользователей системы (кроме ICMP-пакетов, для которых невозможно определить владельца);
- фильтрации пакетов для входящих и исходящих соединений;

- фильтрации пакетов по дате\времени;
- фильтрации протоколов прикладного уровня.

Функции безопасности ОС выполняют анализ атрибутов безопасности субъектов (отправителя, получателя) и информации (сетевого трафика). На атрибутах безопасности формируется набор правил фильтрации, основываясь на которых происходит явный запрет или разрешение информационного потока.

Отправитель и получатель имеют тип атрибута: сетевой адрес узла отправителя/получателя. Сетевой трафик имеет следующие типы атрибутов:

- сетевой протокол, который используется для взаимодействия;
- транспортный протокол, который используется для взаимодействия;
- порты источника и получателя в рамках сеанса (сессии);
- разрешенные/запрещенные протоколы прикладного уровня.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1. Входные данные

Обмен информацией между ОС Альт СП и внешними источниками осуществляется с помощью информационных сообщений по локальной вычислительной сети или сети Internet с использованием протоколов TCP/IP, ICMP, FTP, HTTP, POP, SMTP, IMAP, SLIP, PPP, RIP, IPX и NetBIOS.

Также входными данными являются управляющие команды пользователей и администраторов ПЭВМ, введенные с использованием клавиатуры и (или) манипулятора типа «мышь»:

- обращение субъектов доступа (процессов и команд СУБД) к защищаемым именованным объектам доступа – файлам (программам, библиотекам, файлам с пользовательской и служебной информацией), каталогам, специальным файлам (устройствам, ссылкам, каналам FIFO), базам данных и их элементам (таблицам, записям, полям записей, триггерам), а также средствам IPC (портам, сокетам, семафорам);
- атрибуты, определяющие полномочия субъектов доступа и правила разграничения доступа к объектам доступа.

4.2. Выходные данные

Выходными данными для ОС Альт СП являются результаты обработки управляющих команд со стороны пользователей, администратора и администратора безопасности, результаты обмена информацией между ОС Альт СП и внешними источниками по локальной вычислительной сети или сети Интернет с использованием протоколов TCP/IP, ICMP, FTP, HTTP, POP, SMTP, IMAP, SLIP, PPP, RIP, IPX и NetBIOS.

Также выходными данными являются результаты использования субъектом доступа защищаемого объекта, предоставленного ему в соответствии с установленными правилами разграничения доступа. К таким результатам могут относиться: запуск программы, редактирование файла, создание сокетов, добавление данных в базы данных и другие действия.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

КСЗ – комплекс средств защиты информации;

МФУ – многофункциональное устройство;

ОС – операционная средства;

ПО – программное обеспечение;

ПЭВМ – персональная электронная вычислительная машина;

СУБД – система управления базами данных.

Лист регистрации изменений									
Номера листов (страниц)					*Всего листов (страниц) в докум.*	*№ докумен-та*	*Входящий № сопро-водитель-ного докум. и дата*	*Подп.*	*Да-та*
Изм.	*изменен-ных*	*заменен-ных*	*новых*	*аннули-рован-ных*					