Программа курса: ALTSEC. Информационная безопасность в ОС Альт

1.Законодательное регулирование IT-сферы в РФ

- Основы информационной безопасности.
- Лицензионность ПО.
- Реестр Российского ПО Минкомсвязи.
- Защита персональных данных.
- КИИ.

2. Основы обеспечения безопасности при использовании ОС Альт

- Механизмы разграничения доступа в Linux: (Дискреционный доступ; Мандатный доступ; Ролевой доступ).
- Отличия ОС Альт с точки зрения безопасности.
- Средства очистки оперативной и дисковой памяти.

3. Подсистема аутентификации ОС Альт

- Архитектура PAM.
- Настройка хэширования паролей (ГОСТ Р 34.11–2012).
- Настройка требований сложности паролей.
- Хранение истории паролей.
- Блокировка пользовательских УЗ.
- Ограничение возможности входа пользователей.

4. Контроль целости системы

- Возможности менеджера пакетов для контроля целостности системы
- Настройка контроля целостности средствами osec.
- Подсистема IMA/EVM.

5. Контроль ввода-вывода.

- Ограничения при помощи правил udev.
- Ограничение и контроль использования съемных носителей (usbguard, alterator-ports-access).
- Контроль ввода-вывода средствами библиотеки PolKit.

6. Управление протоколированием событий

- Система журналирования
- Система аудита.
- Централизация данных журналирования и аудита.

7. Шифрование данных

- Симметричные и ассиметричные алгоритмы шифрования.
- Шифрование отдельных файлов средствами openssl и gnupg.
- Использование зашифрованных разделов средствами LUKS.
- Использование криптоконтейнеров eCryptFS.
- Использование отечественных криптопровайдеров в ОС Альт (на примере Криптопро).

8. Инфраструктура публичных ключей и SSL/TLS

- Ассиметричная криптография и инфрастурктура публичных ключей.
- Использование openssl для генерации сертификатов.
- Инспользование EasyRSA для генерации сертифкатов

9. Использование технологий VPN для соединения удаленных офисов

- Основы технологии VPN.
- Развертывание OpenVPN-сервера средствами alterator-openvpn-server.
- Подключение к серверу OpenVPN.

•OpenVPN.

•Управление туннелированием трафика при помощи маршрутизации.

•Установка защищенных соединений с использованием WireGuard.

10. Обнаружение и предотвращение сетевых атак

•Обнаружение руткитов средствами Rkhunter/chkrootkit.

•Использование антивирусного ПО ClamAV.

•Настройка fail2ban.

•Использование сетевой СОВ suricata.