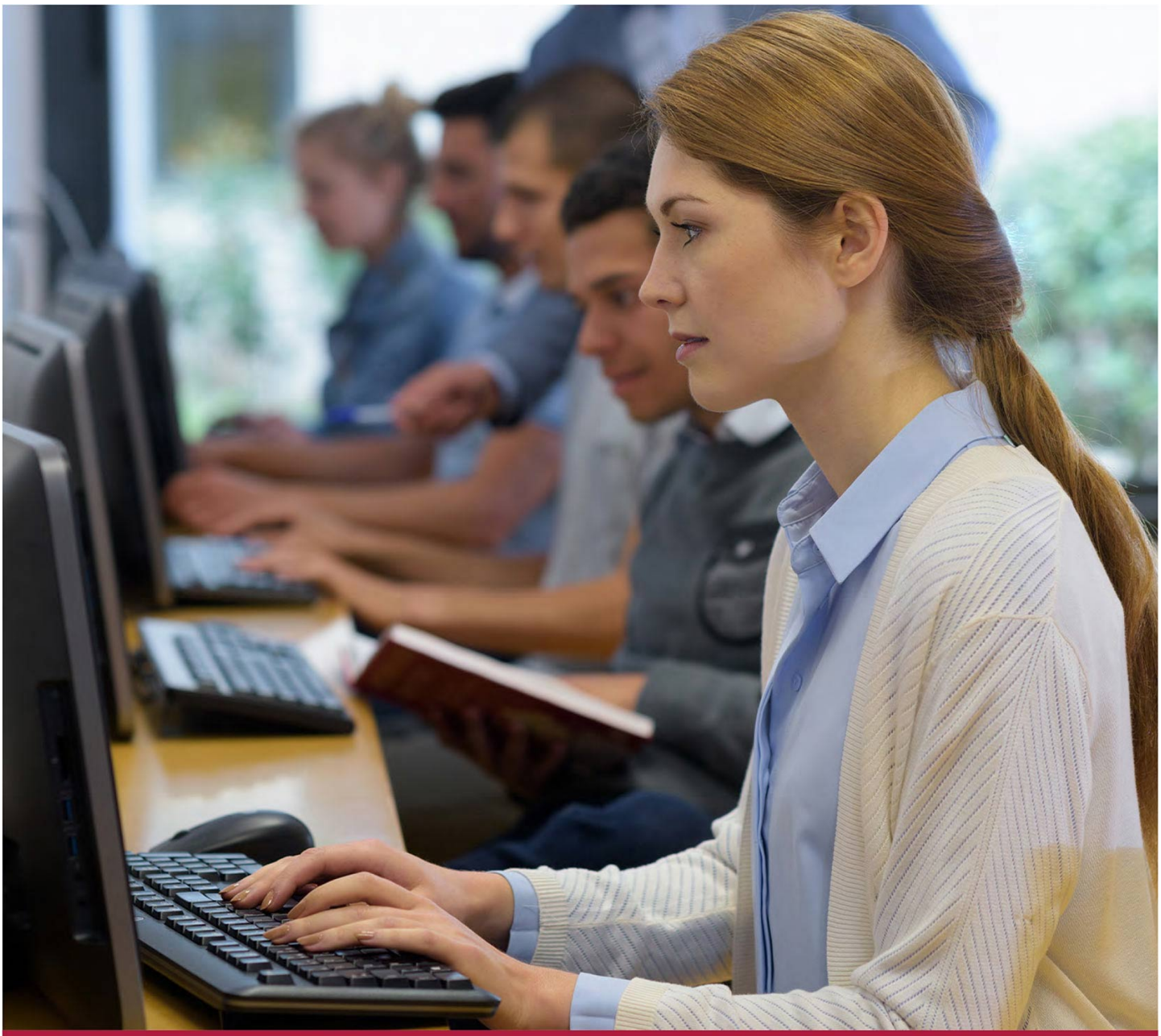
softline учебный центр



Информационная безопасность в ОС «Альт»

Код курса: ALTSEC

8 (800) 505-05-07 | edusales@softline.com | edu.softline.com

Информационная безопасность в ОС «Альт»

Код курса: ALTSEC

Длительность	40 ак. часов
Формат	
Разработчик курса	Базальт СПО
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Целью реализации нового курса «ALTSEC. Информационная безопасность в ОС "Альт"» является совершенствование имеющихся и (или) получение новых компетенций, необходимых для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации в области обеспечения информационной безопасности сетевых узлов при использовании ОС «Альт».

Подробная информация

Профиль аудитории:

Системные администраторы, IT специалисты

Предварительные требования:

Необходимы базовые знания архитектуры современных компьютеров и компьютерных сетей, понимание: клиент-серверной архитектуры, терминов «протокол передачи данных», «сокет», «аутентификация», «авторизация», «учётная запись», «база данных». Также потребуются знания дерева каталогов, иерархии пользователей системы, основных типов файлов Linux, понимание принципов базовой модели разграничения доступа в Linux, роли процесса в операционной системе, особенностей различных файловых систем. От слушателя ожидается уверенное владение интерфейсом командной строки, наличие базовых навыков создания сценариев на языке командного интерпретатора.

Получаемые знания и умения:

- настройки механизмов разграничения доступа в ОС «Альт»;
- настройки работы подсистемы аутентификации (PAM) ОС «Альт»;
- контроля целостности системы;
- ограничения возможности работы с устройствами ввода-вывода, в частности со съемными носителями;
- настройки аудита и журналирование системных событий;
- использовать механизмы шифрования данных для обеспечения безопасного хранения и

передачи данных по сети;
- настройки системы обнаружения и предотвращения атак.
- принципы построения системы защиты ОС «Альт» и назначение отдельных ее подсистем;
- основные требования, предъявляемые российским законодательством к обеспечению информационной безопасности;
- функции и характеристики операционной системы ОС «Альт», служащие для обеспечения информационной безопасности.
- использовать шифрование для обеспечения сетевой безопасности;
- настройки подсистемы аутентификации;
- настройки VPN для защищенного обмена данными в небезопасном сетевом окружении;
- настройки систем обнаружения вторжений.

Программа курса

Модуль 1. Законодательное регулирование IT-сферы в РФ

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

Модуль 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.

Модуль 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.

Модуль 4. Контроль целости системы

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

Модуль 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.

Модуль 6. Управление протоколированием событий

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

Модуль 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).

Модуль 8. Инфраструктура публичных ключей и SSL/TLS

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

Модуль 9. Использование технологий VPN для соединения удаленных офисов

- Основы технологии VPN.
- Развертывание OpenVPN-сервера средствами alterator-openvpnserver.
- Подключение к серверу OpenVPN.
- Управление туннелированием трафика при помощи маршрутизации.
- Установка защищенных соединений с использованием WireGuard.

Модуль 10. Обнаружение и предотвращение сетевых атак

- Обнаружение руткитов средствами Rkhunter/chkrootkit.
- Использование антивирусного ПО ClamAV.
- Настройка fail2ban.
- Использование сетевой СОВ suricata.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Учебного центра Softline

8 (800) 505-05-07 | edusales@softline.com

Ждём вас на занятиях в Учебном центре Softline!

Почему Учебный центр Softline?

Лидер на рынке корпоративного обучения.

Более 300 тысяч подготовленных IT-специалистов.

Гибкий индивидуальный подход в обучении, скидки и акции.

Широкая сеть представительств в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

Высокотехнологичное оборудование

Более **18 лет** опыта работы

Международные сертификаты для IT-специалистов и пользователей в Центрах тестирования

Сертифицированные тренеры с богатым практическим опытом работы

Авторизации от мировых производителей ПО (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперского, Oracle, Autodesk, Код безопасности и других).

Разработка курсов и тестов под заказ, внедрение корпоративных систем обучения.

Подробнее об Учебном центре Softline
Вы можете узнать из профайла.