



Безопасность в ОС Astra Linux Special Edition 1.8

Код курса: AL-1805

Безопасность в ОС Astra Linux Special Edition 1.8

Код курса: AL-1805

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

О курсе

Курс будет интересен администраторам безопасности, системным администраторам, которым требуется обеспечить комплексную безопасность сетевой инфраструктуры посредством ОС Astra Linux Special Edition 1.8 и тем, кто планирует освоить смежную компетенцию специалиста по информационной безопасности. На курсе вы научитесь производить настройку локальной политики безопасности, рассмотрите учетные записи пользователей и аудит операционной системы, узнаете как производить настройку программ для организации единого пространства, а также выполните настройку системы.

Подробная информация

Профиль аудитории:

- администраторы безопасности, системные администраторы

Предварительные требования:

- успешное окончание курса «AL-1802. Администрирование ОС Astra Linux Special Edition 1.8» или эквивалентная подготовка
- успешное окончание курса «AL-1803. Расширенное администрирование ОС Astra Linux Special Edition 1.8» или эквивалентная подготовка

Получаемые знания и умения:

- знание моделей безопасности
- знание нормативных документов ФСТЭК России
- знание принципов построения защищенной операционной системы
- понимание принципов мандатного контроля целостности и мандатного управления доступом
- умение работать с Astra Linux Special Edition при использовании различных режимов функционирования ее средств защиты информации (базовый, усиленный, максимальный)
- умение настраивать локальные политики безопасности
- умение настраивать учетные записи пользователей и групп в соответствии с политикой безопасности предприятия

- умение настраивать режим замкнутой программной среды
- умение настраивать режим киоска
- умение настраивать подсистему аудита
- умение администрировать подсистемы мандатного контроля целостности и мандатного управления доступом
- понимание особенностей работы сетевых служб при использовании мандатных уровней доступа
- понимание мандатного управления доступом в СУБД PostgreSQL
- умение настраивать Astra Linux Special Edition в соответствии с методическими рекомендациями
- умение настраивать печать документов с маркировкой
- умение настраивать защищенные каналы с помощью OpenVPN

Программа курса

Модуль 1. Компьютерная безопасность: общие сведения. Формальные модели и моделирование безопасности современных ОС

- История развития теории и практики обеспечения компьютерной безопасности. Основные понятия и определения.
- Основные модели безопасности.
- Принципы построения защищенной операционной системы.
- Подходы к построению защищенных операционных систем.
- Архитектура подсистемы защиты операционной системы.
- Основные функции подсистемы защиты операционной системы.
- Идентификация, аутентификация и авторизация субъектов доступа.
- Управление доступом к объектам операционной системы.
- Правила управления доступом.
- Основные модели управления доступом.
- Сравнительный анализ моделей управления доступом.

Модуль 2. Нормативные документы ФСТЭК России, регламентирующие требования безопасности информации

- основополагающие законы и подзаконные акты в области информационной безопасности.
- Обзор нормативно-правовых актов ФСТЭК России по вопросам защиты информации ограниченного доступа.
- Обзор нормативно-правовых актов, руководящих и методических документов ФСТЭК России по вопросам сертификации средств защиты информации.
- Требования ФСТЭК России к сертифицированным операционным системам.

Модуль 3. Архитектура и режимы функционирования средств защиты информации Astra Linux Special Edition

- Особенности и преимущества операционной системы Astra Linux Special Edition.
- Режимы функционирования (базовый, усиленный, максимальный) средств защиты информации операционной системы Astra Linux Special Edition.
- Архитектура подсистемы защиты PARSEC операционной системы Astra Linux Special Edition.

- Мандатная метка, мандатный контекст безопасности.

Практическая работа: Архитектура и режимы функционирования средств защиты информации Astra Linux Special Edition.

Модуль 4. Мандатный контроль целостности в Astra Linux

- Определение мандатного контроля целостности.
- Уровни целостности.
- Работа на низком и высоком уровне целостности.
- Управление мандатным контролем целостности.

Модуль 5. Мандатное управление доступом в Astra Linux Special Edition

- Дискреционное и мандатное управление доступом.
- Реализация мандатного управления доступом.
- Уровни конфиденциальности и неиерархические категории.
- Мандатные метки корневого и системных каталогов.
- Администрирование мандатного управления доступом.

Практическая работа: Организация файловой системы для работы пользователей в рамках мандатного управления доступом и мандатного контроля целостности.

Модуль 6. Настройка подсистемы аудита в Astra Linux Special Edition

- Архитектура аудита.
- Правила протоколирования.
- Утилиты управления протоколированием.
- Журнал аудита.

Практическая работа: Администрирование аудита в рамках реализации мандатного контроля целостности. Настройка аудита.

Модуль 7. Контроль целостности программной среды

- Возможности замкнутой программной среды.
- Механизм контроля целостности исполняемых файлов.
- Настройка модуля `digsig_verif`.
- Подписывание программного обеспечения.
- Регламентный контроль целостности.
- Назначение режима Киоск.
- Графический киоск.
- Запуск приложений в графическом киоске в разных режимах.
- Настройка ограничений пользователя по запуску программ.
- Системный киоск.

Практическая работа: Работа администратора и пользователей в режиме замкнутой программной среды. Настройка графического киоска. Работа в режиме киоска.

Модуль 8. Проверка функционирования подсистем, реализующих функции безопасности ОС

- Состав и назначение средств тестирования СЗИ.
- Порядок загрузки и настройки тестов.
- Запуск тестов и анализ результатов.

Практическая работа: Подготовка системы к тестированию, загрузка, настройка и запуск тестовых скриптов.

Модуль 9. Сетевое взаимодействие в Astra Linux Special Edition

- Внедрение меток безопасности в IPv4- и IPv6-пакеты.
- Особенности работы сетевых служб при использовании мандатного управления доступом. Механизм privsock.
- Создание защищенных каналов с помощью OpenVPN.
- Виды соединений и принципы работы OpenVPN.
- Установка и быстрая настройка сервера OpenVPN.
- Настройка клиента OpenVPN.
- Расширенные настройки OpenVPN и управление сертификатами.
- Диагностика работы OpenVPN.
- Настройка межсетевого экрана (ufw, gufw). Фильтрация сетевого трафика по меткам конфиденциальности.
- Маркировка документов, отправляемых на печать.
- Режим AstraMode в Apache2.
- Удаленный доступ к Astra Linux по протоколу RDP.

Практическая работа: Основные настройки системы и сетевых служб с точки зрения мандатного управления доступом. Настройка OpenVPN. Настройка межсетевого экрана.

Модуль 10. Дополнительные функции безопасности системы

- Монитор безопасности.
- Общие настройки безопасности.
- Установка квот на использование ресурсов.
- Блокировка системных параметров и действий пользователя.
- Управление безопасностью ядра и модулей.
- Дополнительные настройки безопасности для пользователей системы.

Практическая работа: Настройка дополнительных функций безопасности.

Модуль 11. Методические рекомендации по безопасной настройке ОС Astra Linux Special Edition

- Обеспечение безопасности среды функционирования ОС.
- Рекомендации по установке.
- Настройка ОС согласно указаниям по эксплуатации.
- Отключение неиспользуемых сервисов и аппаратных устройств.
- Конфигурирование наиболее уязвимых системных служб.
- Рекомендации по обновлению и резервному копированию.

Практическая работа: Настройка защищенного режима работы Astra Linux Special Edition в соответствии с методическими рекомендациями.

Модуль 12. Управление доступом в СУБД PostgreSQL (опциональный модуль)

- Установка экземпляра PostgreSQL.
- Автоматизированное тестирование функциональных возможностей по разграничению доступа в PostgreSQL.
- Основы работы PostgreSQL.
- Дискреционное управление доступом в СУБД PostgreSQL.
- Конфигурационные параметры для настройки дискреционного доступа.
- Мандатное управление доступом в СУБД PostgreSQL.
- Мандатные атрибуты сеанса пользователя.
- Применение мандатного управления доступом.
- Средства управления мандатным доступом к объектам БД.
- Целостность классификационных меток кластера БД.
- Особенности работы правил и триггеров с мандатным управлением доступом.

Практическая работа: Настройка дискреционного доступа. Работа пользователей с разными уровнями конфиденциальности с БД, в которой данные имеют различные классификационные метки.

[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](#).