

Обучение по программе **Безопасность в ОС Astra Linux Special Edition 1.7**

Вы научитесь:

Администрировать подсистемы мандатного контроля целостности и управления доступом

Настраивать защищённые каналы с помощью OpenVPN

Настраивать режим замкнутой программной среды

Разрабатывать локальные политики безопасности

По итогам обучения Вы получите:

- Свидетельство о повышении квалификации государственного образца
- Сертификат Astra Linux
- Сертификат МЦО НЦОТ "ROZUM"

Продолжительность: 40 академических часов
Стоимость: 2580 бел. рублей (НДС не облагается)
Форма обучения: очная (дневная)

Содержание программы:

1. Компьютерная безопасность, общие сведения. Построение защищенных операционных систем. Формальные модели управления доступом.

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

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

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

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

- 3.1. Особенности и преимущества операционной системы Astra Linux Special Edition.
- 3.2. Архитектура подсистемы защиты PARSEC операционной системы Astra Linux Special Edition.
- 3.3. Режимы функционирования (Базовый, Усиленный, Максимальный) средств защиты информации операционной системы Astra Linux Special Edition.
Практическая работа: Архитектура и режимы функционирования средств защиты информации Astra Linux Special Edition.

4. Мандатный контроль целостности в Astra Linux Special Edition.

- 4.1. Определение мандатного контроля целостности.
- 4.2. Уровни целостности.
- 4.3. Работа на низком и высоком уровне целостности.
- 4.4. Управление мандатным контролем целостности.
- 4.5. Администрирование ОС при включенном режиме мандатного контроля целостности.

5. Мандатное управление доступом в Astra Linux Special Edition.

- 5.1. Дискреционное и мандатное управление доступом.
- 5.2. Реализация мандатного управления доступом.
- 5.3. Уровни конфиденциальности и неиерархические категории.
- 5.4. Мандатные метки корневого и системных каталогов.
- 5.5. Администрирование мандатного управления доступом.
- 5.6. PARSEC-привилегии.

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

6. Настройка подсистемы аудита в Astra Linux Special Edition.

- 6.1. Архитектура аудита PARSEC.
- 6.2. Утилита просмотра журналов аудита.
- 6.3. Настройка политики аудита.

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

7. Реализация замкнутой программной среды. Проверка целостности подсистемы защиты.

- 7.1. Возможности замкнутой программной среды.
- 7.2. Механизм контроля целостности исполняемых файлов.
- 7.3. Настройка модуля `digsig_verif`.
- 7.4. Подписывание программного обеспечения.
- 7.5. Регламентный контроль целостности.
- 7.6. Практическая работа: Работа администратора и пользователей в режиме замкнутой программной среды.

8. Режим киоска.

- 8.1. Назначение режима киоск.
- 8.2. Графический киоск.
- 8.3. Запуск приложений в графическом киоске в разных режимах.
- 8.4. Настройка ограничений пользователя по запуску программ.
- 8.5. Системный киоск.

Практическая работа: Настройка графического киоска. Работа в режиме киоска.

9. Сетевое взаимодействие в Astra Linux Special Edition.

- 9.1. Внедрение меток безопасности в IPv4 и IPv6 пакеты.
- 9.2. Особенности работы сетевых служб при использовании мандатного управления доступом. Механизм `privsock`.
- 9.3. Создание защищенных каналов с помощью OpenVPN.
- 9.4. Виды соединений и принципы работы OpenVPN.
- 9.5. Установка и быстрая настройка сервера OpenVPN.
- 9.6. Настройка клиента OpenVPN.
- 9.7. Расширенные настройки OpenVPN и управление сертификатами.
- 9.8. Диагностика работы OpenVPN.
- 9.9. Маркировка документов, отправляемых на печать.

10. Настройка межсетевого экрана (ufw, gufw). Фильтрация сетевого трафика по меткам конфиденциальности.

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

10. Мандатное управление доступом в СУБД PostgreSQL..

10.1. Управление доступом к защищаемым ресурсам БД.

10.2. Конфигурационные параметры для настройки работы сервера СУБД с мандатным управлением доступом.

10.3. Средства управления мандатным доступом к объектам БД.

10.4. Целостность мандатных атрибутов кластера БД.

10.5. Особенности создания правил и триггеров.

10.6. Система привилегий СУБД.

Практическая работа: Работа пользователей с разными мандатными уровнями с БД, в которой данные имеют различные метки безопасности.

11. Дополнительные функции безопасности системы.

11.1. Монитор безопасности.

11.2. Общие настройки безопасности.

11.3. Установка квот на использование ресурсов.

11.4. Блокировка системных параметров и действий пользователя.

11.5. Управление безопасностью ядра и модулей.

11.6. Дополнительные настройки безопасности для пользователей системы

12. Red Book: настройка безопасной конфигурации для Astra Linux Special Edition 1.7.

12.1. Действия перед установкой Astra Linux Special Edition.

12.2. Действия во время установки Astra Linux Special Edition.

12.3. Действия после установки Astra Linux Special Edition.

12.4. Изменение настроек политики учетной записи пользователя.

12.5. Настройка межсетевого экрана.

12.6. Системные параметры.

12.7. Блокировка одновременной работы с разными уровнями конфиденциальности в пределах одной сессии.

12.8. Блокировка интерпретаторов и bash.

12.9. Режим замкнутой программной среды.

12.10. Политика очистки памяти.

12.11. Мандатный контроль целостности, защита файловой системы.

12.12. Действия в процессе эксплуатации Astra Linux Special Edition.

Практическая работа: Настройка защищенного режима работы Astra Linux Special Edition в соответствии с Astra Linux Red-Book.

Подать заявку на обучение:



pk@ncot.by



rozum.ntec.by



+ 375(17)327-14-29
+ 375(17)328-60-16



Бизнес-центр "Имперский",
ул. К. Цеткин, 24, 11 этаж

roz
um