

# Безопасность в ОС ASTRA LINUX SPECIAL EDITION 1.7 (AL-1705)

ID AX-AL-1705 Цена 60 000,- руб. Длительность 5 дней

## Предварительные требования

Предварительные требования к уровню подготовки слушателей:

- Успешное окончание курса [Администрирование ОС ASTRA LINUX SPECIAL EDITION 1.7 \(AL-1702\)](#) или эквивалентная подготовка;
- Успешное окончание курса [Расширенное администрирование ОС ASTRA LINUX SPECIAL EDITION 1.7 \(AL-1703\)](#) или эквивалентная подготовка.

## Цели курса

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 рекомендациями, изложенными в Red Book;

- Умение настраивать печать документов с маркировкой;
- умение настраивать защищенные каналы с помощью OpenVPN.

## Программа курса

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

- История развития теории и практики обеспечения компьютерной безопасности. Основные понятия и определения;
- 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;
- основные стандарты 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;
- Архитектура подсистемы защиты PARSEC операционной системы Astra Linux Special Edition;
- Режимы функционирования (Базовый, Усиленный, Максимальный) средств защиты информации операционной системы Astra Linux Special Edition.

## МОДУЛЬ 4. Мандатный контроль целостности в Astra Linux Special Edition

- Определение мандатного контроля целостности;
- Уровни целостности;
- Работа на низком и высоком уровне целостности;
- Управление мандатным контролем целостности;
- Администрирование ОС при включенном режиме мандатного контроля 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;
- PARSEC-привилегии.

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 PARSEC;
- Утилита просмотра журналов аудита;
- Настройка политики аудита.

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

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

- Возможности замкнутой программной среды;
- Механизм контроля целостности исполняемых файлов;
- Настройка модуля `digsig_verif`;
- Подписывание программного обеспечения;
- Регламентный контроль целостности.

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

## МОДУЛЬ 8. Режим киоска

- Назначение режима киоск;
- Графический киоск;
- Запуск приложений в графическом киоске в разных режимах;
- Настройка ограничений пользователя по запуску программ;
- Системный киоск.

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

## 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;
- Маркировка документов, отправляемых на печать;
- Настройка межсетевых экранов (`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.

Special Edition.

МОДУЛЬ 10. Мандатное управление доступом в СУБД PostgreSQL

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

- Управление доступом к защищаемым ресурсам БД;
- Конфигурационные параметры для настройки работы сервера СУБД с мандатным управлением доступа;
- Средства управления мандатным доступом к объектам БД;
- Целостность мандатных атрибутов кластера БД;
- Особенности создания правил и триггеров;
- Система привилегий СУБД.

ИТОГОВОЕ ТЕСТИРОВАНИЕ

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

МОДУЛЬ 11. 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.

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

- Действия перед установкой Astra Linux Special Edition;
- Действия во время установки Astra Linux Special Edition;
- Действия после установки Astra Linux Special Edition:
  - Изменение настроек политики учетной записи пользователя;
  - Настройка межсетевого экрана;
  - Системные параметры;
  - Блокировка одновременной работы с разными уровнями конфиденциальности в пределах одной сессии
  - Блокировка интерпретаторов и bash;
  - Режим замкнутой программной среды;
  - Политика очистки памяти;
  - Мандатный контроль целостности, защита файловой системы;
  - Действия в процессе эксплуатации Astra Linux