

KL 013.11.4:

Kaspersky Endpoint Security для Linux

Изучаемые продукты

- Kaspersky Endpoint Security для Linux 11.4
- Kaspersky Security Center Linux 14.2

Описание курса

Kaspersky Endpoint Security для Linux совместно с Kaspersky Security Center Linux представляет собой решение класса EPP (Endpoint Protection Platform) и помогает защитить устройства под управлением ОС Linux от широкого спектра угроз.

Теоретический материал и лабораторные работы дают слушателям необходимые знания и навыки, благодаря которым слушатель сможет выполнить развертывание и настройку решения, будет понимать принципы использования решения и сможет выполнять задачи по его обслуживанию.

Длительность

1 день.

Требования к участникам

Понимание основ сетевых технологий, базовые навыки администрирования Linux. Представление о современных угрозах и тенденциях развития информационных технологий.

Содержание

1. Как и зачем защищать Linux

- 1.1. Зачем защищать Linux?
- 1.2. Чем защищать Linux

2. Как установить защиту

- 2.1. Сценарий установки
- 2.2. Установка и настройка MariaDB
- 2.3. Установка и настройка PostgreSQL

- 2.4. Установка Сервера администрирования
- 2.5. Установка веб консоли

Лабораторная работа 1. Как установить Kaspersky Security Center Linux

- 2.6. Что делать после установки KSC
- 2.7. Первоначальная настройка сервера
- 2.8. Как обнаружить устройства в сети

Лабораторная работа 2. Как настроить Kaspersky Security Center Linux

- 2.9. Установка Агента администрирования
- 2.10. Установка KESL

Лабораторная работа 3. Установите Kaspersky Endpoint Security на управляемые устройства

3. Как настроить защиту

- 3.1. Как управлять устройствами
- 3.2. Как объединять устройства
- 3.3. Как присваивать тэги
- 3.4. Как применять политики

Лабораторная работа 4. Как управлять устройствами

4. Как защитить устройства

- 4.1. Как защититься от вредоносных файлов на устройстве
- 4.2. Как предотвратить попадание вредоносных файлов на устройство
- 4.3. Как защитить устройство от сетевых угроз
- 4.4. Как защититься от шифровальщиков
- 4.5. Как защититься от новых угроз

Лабораторная работа 5. Настройка защиты сервера

5. Как укрепить систему

- 5.1. Зачем контролировать систему?
- 5.2. Контроль приложений
- 5.3. Инвентаризация
- 5.4. Управление сетевым экраном
- 5.5. Контроль устройств

Лабораторная работа 6. Как собрать информацию об исполняемых файлах

Лабораторная работа 7. Проверить защиту от эксплуатации уязвимости

6. Управление KESL через командную строку

- 6.1. Зачем использовать командную строку
- 6.2. Как управлять задачами

Лабораторная работа 8. Как управлять защитой с помощью kesi-control