Kaspersky Endpoint Security and Management. Расширенный курс (комплексный)

KL-302.10 (к)

Содержание

Краткая информация

Длительность:	5 дней (40 ак.часа)
Аудитория:	ИТ-специалисты
Автор/Вендор:	Лаборатория Касперского
Тип:	Учебный курс
Способ обучения:	Под руководством инструктора

Обзор/Аннотация*

Курс охватывает дополнительные вопросы по внедрению и обслуживанию построенных на основе Kaspersky Endpoint Security для платформы Microsoft Windows и Kaspersky Security Center систем информационной защиты от вирусов в крупных сетях. В ходе обучения слушатели получат теоретические знания и практические навыки развертывания и эксплуатации комплексной системы антивирусной защиты (КСАЗ) в крупных сетях, а также вопросы миграции КСАЗ с предыдущих версий антивируса Касперского и Kaspersky Administration Kit.

О курсе*

Курс предназначен для системных администраторов небольших сетей, которые планируют внедрение защиты в больших или географически распределенных сетях. Комплексный курс включает:

KL 302.10 Endpoint Security and Management. Расширенные возможности

KL 008.10 Endpoint Security and Management. Шифрование

KL 009.10 Endpoint Security and Management. Управление системами

KL 010.10 Endpoint Security and Management. Управление мобильными устройствами

Профиль аудитории*

Администраторы сетей Microsoft Windows с опытом работы с Kaspersky Security Center и Kaspersky Endpoint Security для Windows, или, прослушавшие базовый курс KL 002.10.

По окончании курса слушатели смогут:*

- спроектировать и внедрить оптимальную антивирусную защиту корпоративной сети предприятия с помощью Kaspersky Endpoint Security;
- поддерживать внедренную систему защиты;

- выполнять настройку параметров защиты;
- настраивать и использовать инструменты мониторинга Kaspersky Endpoint Security;
- выполнять резервное копирование и восстановление базы Kaspersky Security Center;

Детальная информация о курсе*

Часть I. Масштабирование.

1. Управление трафиком. Обсуждение. Способы ограничения трафика.
2. Агенты обновлений и шлюзы соединений. Агенты обновлений. Шлюзы соединений. Мониторинг агентов обновлений.
3. Использование нескольких Серверов Администрирования. Обсуждение. Независимые сервера. Иерархия серверов.
4. Управление администраторами. Обсуждение. Разграничение доступа. Виртуальные Сервера администрирования. Аудит.
5. Специальные функции. Проверка обновлений. Поддержка динамической VDI.

- Лабораторная работа №1 — Агенты обновлений
- Лабораторная работа №2 — Назначение шлюза соединений
- Лабораторная работа №3 — Перемещение компьютера к другому Серверу администрирования
- Лабораторная работа №4 — Автоматическое изменение настроек соединения
- Лабораторная работа №5 — Создание иерархии
- Лабораторная работа №6 — Наследование политик и задач
- Лабораторная работа №7 — Обновление в иерархии
- Лабораторная работа №8 — Удаленная установка в иерархии
- Лабораторная работа №9 — Настройка прав администратора группы
- Лабораторная работа №10 — Настройка тестирования обновлений

Часть II. Шифрование.

1. Ознакомление и начало работы.
2. Шифрование жестких дисков (Full Disk Encryption).
3. Шифрование файлов и папок (File Level Encryption).
4. Шифрование съемных дисков.

- Лабораторная работа №1 — Включение функций шифрования
- Лабораторная работа №2 — Включение Full Disk Encryption
- Лабораторная работа №3 — Восстановление доступа к компьютеру
- Лабораторная работа №4 — Включение шифрование файлов и папок
- Лабораторная работа №5 — Обмен данными с внешними пользователями
- Лабораторная работа №6 — Использование съемных дисков в портативном режиме

Часть III. Управление системами.

1. Введение.
2. Реестр программ и оборудования.
3. Управление уязвисостями и обновлениями.
4. Управление доступом в сеть (Network Access Control).
5. Захват и развертывание образов компьютеров.

- Лабораторная работа №1 — Управление лицензиями сторонних программ
- Лабораторная работа №2 — Установка обновлений Windows
- Лабораторная работа №3 — Устранение уязвимостей в программах
- Лабораторная работа №4 — Установка сторонних программ
- Лабораторная работа №5 — Запрет доступа в сеть любому устройству в ручном режиме
- Лабораторная работа №6 — Перенаправление компьютеров на страницу авторизации
- Лабораторная работа №7 — Ограничение доступа на основе статуса компьютера
- Лабораторная работа №8 — Захват образа операционной системы
- Лабораторная работа №9 — Развертывание операционной системы

Часть IV. Управление мобильными устройствами.

1. Kaspersky MDM для Exchange ActiveSync.
2. Kaspersky MDM для iOS.
3. Kaspersky Security для Mobile.

- Лабораторная работа №1 — Добавление Сервера мобильных устройств для Exchange ActiveSync

- Лабораторная работа №2 — Применение корпоративной политики безопасности через Exchange ActiveSync
- Лабораторная работа №3 — Подготовка к внедрению Kaspersky Security 10 для мобильных устройств
- Лабораторная работа №4 — Установка Kaspersky Security 10 для мобильных устройств
- Лабораторная работа №5 — Управление сторонними приложениями
- Лабораторная работа №6 — Удаленная блокировка мобильного устройства
- Лабораторная работа №7 — Удаленная очистка мобильного устройства

Предварительные требования

Для полноценного усвоения материала курса и эффективного выполнения лабораторных работ, слушатели должны обладать определенными знаниями и навыками в области информационных технологий:

Базовыми знаниями о функционировании сетей на основе TCP/IP, сети Интернет и электронной почте, сетях Microsoft Windows и Active Directory
Навыками работы с операционными системами семейства Microsoft Windows.

Дополнительная информация

По окончании курса все слушатели получают сертификат.

Если у вас возникли вопросы, воспользуйтесь следующими ссылками:

- Информации об учебных курсах и программах сертификации
- Расписание курсов