KL 302.10 (к): Endpoint Security and Management. Расширенный курс (комплексный)

KL 302.10 (к): Endpoint Security and Management. Расширенный курс (комплексный)

Содержание

Краткая информация

Длительность:	5 дней (40 ак.часов)
Аудитория:	ИТ-профессионалы
Технология:	Kaspersky Endpoint Security
Тип:	Учебный курс
Способ обучения:	Под руководством инструктора
Подготовка к сертификации:	KLE 002.10 - Kaspersky Endpoint Security and Management. Базовый KLE 302.10 - Kaspersky Endpoint Security and Management. Расширенный KLE 008.10 - Kaspersky Endpoint Security and Management. Шифрование KLE 009.10 - Kaspersky Endpoint Security and Management. Управление системами KLE 010.10 - Kaspersky Endpoint Security and Management. Mobile Device Management

Обзор

О курсе

По окончании курса KL-302.10, рассчитанного на системных администраторов и специалистов по безопасности информации, вы научитесь внедрять комплексную систему антивирусной защиты Kaspersky Endpoint Security в распределенных сетях и больших организациях, управлять трафиком, обновлять систему администрирования и подготовиться к сдаче экзамена для получения статуса KL Certified System Engineer: Kaspersky Endpoint Security 10 для Windows.

Профиль аудитории

Курс рассчитан на системных администраторов и специалистов по безопасности информации, имеющих опыт работы с Kaspersky Security Center и Kaspersky Endpoint Security для Windows.

По окончании курса

По окончании курса слушатели смогут:

- использовать реализованные в клиенте Kaspersky Endpoint Security 10 возможности по шифрованию данных и дисков, по обеспечению безопасности мобильных устройств, по управлению системами;
- собирать информацию о программном и аппаратном обеспечении в сети;
- обнаруживать и автоматически закрывать уязвимости в программном обеспечении;
- управлять доступом к сети;
- создавать и распространять образы операционных систем.

Детальная информация о курсе

Модуль 1. Масштабирование

- Управление трафиком
- Агенты обновлений и шлюзы соединений
- Использование нескольких Серверов Администрирования
- Управление администраторами
- Специальные функции

- 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

Модуль 2. Шифрование

- Ознакомление и начало работы
- Шифрование жестких дисков (Full Disk Encryption)
- Шифрование файлов и папок (File Level Encryption)
- 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

Модуль 3. Управление системами

- Введение
- Реестр программ и оборудования
- Управление уязвимостями и обновлениями
- Управление доступом в сеть (Network Access Control)
- 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

Модуль 4. Управление мобильными устройствами

- Kaspersky MDM для Exchange ActiveSync
- Kaspersky MDM для iOS
- Kaspersky Security для Mobile

- Лабораторная работа №1 — Добавление Сервера мобильных устройств для Exhange 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

Рекомендуется прослушать курс KL-002.10 «Endpoint Security and Management. Базовый курс».

Дополнительная информация

Если у вас возникли вопросы, воспользуйтесь следующими ссылками:

- Информации об учебных курсах и программах сертификации
- Расписание курсов