

**KL 008.11.6:**

# **Kaspersky Endpoint Security and Management.**

## **Шифрование**

### **Изучаемые продукты**

- Kaspersky Endpoint Security
- Kaspersky Security Center

### **Описание курса**

Слушатели этого курса узнают, как защитить данные средствами шифрования, реализованными в Kaspersky Security Center 13 и Kaspersky Endpoint Security 11.6. Курс состоит из презентаций и упражнений. По окончании обучения слушатели смогут планировать внедрение шифрования, проверять его результаты и поддерживать корректную работу с зашифрованными данными.

Теоретический материал и лабораторные работы дают слушателям необходимые знания и навыки, благодаря которым слушатель сможет:

- Включать шифрование на рабочих станциях
- Управлять шифрованием на рабочих станциях и съемных накопителях
- Восстанавливать доступ к данным на зашифрованных носителях

### **Длительность**

1 день.

### **Требования к участникам**

- Базовые навыки администрирования ОС Windows
- Знание Kaspersky Security Center и Kaspersky Endpoint Security на уровне курса KL 002. Kaspersky Endpoint Security and Management

Курс ориентирован на системных администраторов Microsoft Windows, специалистов и администраторов безопасности, инженеров технической и предпродажной поддержки.

# Что нового по сравнению с предыдущей версией 008.104

- Добавлены изменения с учетом появившихся нововведений, рассматриваются вспомогательные утилиты
- В презентации и лабораторных работах функционал Шифрование теперь рассматривается на примере Web Console

## Содержание

### 1. Введение

### 2. Полнодисковое шифрование

- 2.1. Принципы работы полнодискового шифрования
- 2.2. Использование утилиты FDE Test

**Лабораторная работа 1.** Проверьте возможность шифрования на машине, используя FDE\_Precheck

- 2.3. Включение полнодискового шифрования
- 2.4. Особенности Агента аутентификации
- 2.5. Управление учетными записями Агента аутентификации

**Лабораторная работа 2.** Подготовка и включение шифрования

- 2.6. Восстановление доступа к системе
- 2.7. Восстановление данных
- 2.8. Использование FDERT
- 2.9. Обновление версии ПО

**Лабораторная работа 3.** Восстановление доступа к компьютеру

### 3. Шифрование средствами BitLocker

- 3.1. Что такое BitLocker
- 3.2. Управление BitLocker средствами KSC
- 3.3. Проверка состояния устройств
- 3.4. Восстановление доступа

**Лабораторная работа 4.** Шифрование диска средствами BitLocker

### 4. Шифрование файлов и папок

- 4.1. Принципы работы шифрования файлов
- 4.2. Включение шифрования файлов

**Лабораторная работа 5.** Включение шифрования файлов и папок

- 4.3. Обмен зашифрованными файлами
- 4.4. Восстановление доступа, когда нет связи с KSC

**Лабораторная работа 6.** Обмен данными с другими пользователями

### 5. Шифрование съемных носителей

- 5.1. Обзор доступных решений
- 5.2. Полное шифрование
- 5.3. Шифрование отдельных файлов
- 5.4. Портативный режим
- 5.5. Восстановление доступа

**Лабораторная работа 7.** Использование съемных дисков в портативном режиме