



## **Kaspersky Endpoint Security. Шифрование**

Код курса: KL 008.11.6

# Kaspersky Endpoint Security. Шифрование

Код курса: KL 008.11.6

<b>Длительность</b>	8 ак. часов
<b>Формат</b>	
<b>Разработчик курса</b>	Лаборатория Касперского
<b>Тип</b>	Учебный курс
<b>Способ обучения</b>	Под руководством тренера

## О курсе

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.

## Подробная информация

### Профиль аудитории:

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

### Предварительные требования:

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

### По окончании курса слушатели смогут:

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

## Программа курса

### Модуль 1. Полнодисковое шифрование

- Принципы работы полnodискового шифрования
- Использование утилиты FDE Test
- Лабораторная работа 1. Проверьте возможность шифрования на машине, используя FDE\_Precheck
- Включение полnodискового шифрования
- Особенности Агента аутентификации
- Управление учетными записями Агента аутентификации
- Лабораторная работа 2. Подготовка и включение шифрования
- Восстановление доступа к системе
- Восстановление данных
- Использование FDERT
- Обновление версии ПО
- Лабораторная работа 3. Восстановление доступа к компьютеру

## **Модуль 2. Шифрование средствами BitLocker**

- Что такое BitLocker
- Управление BitLocker средствами KSC
- Проверка состояния устройств
- Восстановление доступа
- Лабораторная работа 4. Шифрование диска средствами BitLocker

## **Модуль 3. Шифрование файлов и папок**

- Принципы работы шифрования файлов
- Включение шифрования файлов
- Лабораторная работа 5. Включение шифрования файлов и папок
- Обмен зашифрованными файлами
- Восстановление доступа, когда нет связи с KSC
- Лабораторная работа 6. Обмен данными с другими пользователями

## **Модуль 4. Шифрование съемных носителей**

- Обзор доступных решений
- Полное шифрование
- Шифрование отдельных файлов
- Портативный режим
- Восстановление доступа
- Лабораторная работа 7. Использование съемных дисков в портативном режиме

[Посмотреть расписание курса и записаться на обучение](#)

**Обращайтесь по любым вопросам**  
к менеджерам Учебного центра Softline

**8 (800) 505-05-07** | [edusales@softline.com](mailto:edusales@softline.com)

**Ждём вас на занятиях в Учебном центре Softline!**



## Почему Учебный центр Softline?

**Лидер** на рынке корпоративного обучения.

**Более 300 тысяч** подготовленных IT-специалистов.

**Гибкий индивидуальный подход** в обучении, скидки и акции.

**Широкая сеть представительств** в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

**Высокотехнологичное** оборудование

Более **18 лет** опыта работы

**Международные сертификаты** для IT-специалистов и пользователей в Центрах тестирования

**Сертифицированные тренеры** с богатым практическим опытом работы

**Авторизации от мировых производителей ПО** (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперского, Oracle, Autodesk, Код безопасности и других).

**Разработка курсов и тестов под заказ**, внедрение корпоративных систем обучения.

**Подробнее об Учебном центре Softline**

Вы можете узнать из [профайла](#).