



## **Kaspersky Endpoint Security and Management**

Код курса: KL 002.11.6

# Kaspersky Endpoint Security and Management

Код курса: KL 002.11.6

|                          |                          |
|--------------------------|--------------------------|
| <b>Длительность</b>      | 24 ак. часа              |
| <b>Формат</b>            | Очно; Дистанционно       |
| <b>Разработчик курса</b> | Лаборатория Касперского  |
| <b>Тип</b>               | Учебный курс             |
| <b>Способ обучения</b>   | Под руководством тренера |

## О курсе

Основная цель курса – предоставить слушателям необходимый набор знаний для успешного внедрения, настройки и управления решением. Курс готовит к проектированию, внедрению и обслуживанию систем защиты сетей Windows, построенных на Kaspersky Endpoint Security и централизованно управляемых через Kaspersky Security Center. Он рассказывает о продуктах, которые нужны, чтобы защитить сеть примерно до 1000 узлов, сосредоточенных в одном месте. Под узлами курс понимает серверы и рабочие станции под управлением Windows. Что нового Материалы курса и лабораторные работы обновлены в соответствии с функционалом версий Kaspersky Security Center 13 и Kaspersky Endpoint Security 11.6. В презентацию и учебник добавлена следующая информация: Описание Kaspersky Security Center Cloud Console, общей схемы взаимодействия ее компонентов и процесса подключения к Kaspersky Security Center Cloud Console. Как настроить и использовать слияние исключений в политиках. Как настроить и использовать локальные исключения. Описание настроек и работы задачи Wipe data.

## Подробная информация

### Предварительные требования:

- Понимание основ сетевых технологий: TCP/IP, DNS, электронной почты, web.
- Базовые навыки администрирования OS Windows.
- Базовые знания об информационной безопасности.

### По окончании курса слушатели смогут:

- Описать возможности Kaspersky Endpoint Security для Windows и Kaspersky Security Center
- Спроектировать и внедрить оптимальное решение для защиты сетей Windows, основанное на Kaspersky Endpoint Security и управляемое через Kaspersky Security Center
- Осуществлять обслуживание внедренной системы на всех стадиях эксплуатации
- Описать Kaspersky Security Center Cloud Console, общие схемы взаимодействия ее компонентов и процесс подключения к Kaspersky Security Center Cloud Console.
- Настроить и использовать слияние исключений в политиках.
- Настроить и использовать локальные исключения.
- Описать настройки и работу задачи Wipe data.

## Программа курса

### Модуль 1 «Введение»

- Основы Kaspersky Endpoint Security для бизнеса
- Как установить Kaspersky Endpoint Security для бизнеса
- Как установить Kaspersky Security Center
- Как установить Kaspersky Endpoint Security на компьютеры
- Как организовать компьютеры в группы
- Лабораторная работа 1 «Установить Kaspersky Security Center»
- Лабораторная работа 2 «Внедрить Kaspersky Endpoint Security»
- Лабораторная работа 3 «Создать структуру управляемых компьютеров»

### Модуль 2 «Управление защитой»

- Как Kaspersky Endpoint Security защищает компьютер
- Как настроить защиту файлов
- Как настроить защиту от угроз по сети
- Как настроить защиту от сложных угроз
- Как контролировать сетевые соединения
- Как защитить компьютеры за пределами сети
- Что еще есть в защите и зачем
- Лабораторная работа 4 «Проверить защиту от файловых угроз»
- Лабораторная работа 5 «Настроить защиту от почтовых угроз»
- Лабораторная работа 6 «Проверить защиту от веб-угроз»
- Лабораторная работа 7 «Как проверить защиту сетевых папок от программ-вымогателей»
- Лабораторная работа 8 «Проверить Защиту от эксплойтов»
- Лабораторная работа 9 «Проверить Защиту от бесфайловых угроз»
- Лабораторная работа 10 «Повысить меры по повышению безопасности рабочей станции для защиты от программ вымогателей»
- Лабораторная работа 11 «Как проверить Защиту от сетевых атак»
- Лабораторная работа 12 «Как настроить исключения из самозащиты»
- Лабораторная работа 13 «Настроить защиту паролем»

### Модуль 3 «Контроль»

- Общие сведения
- Контроль программ
- Контроль устройств
- Веб-Контроль
- Адаптивный контроль аномалий
- Лабораторная работа 14 «Настроить Контроль программ»
- Лабораторная работа 15 «Заблокировать запуск неизвестных файлов в сети»
- Лабораторная работа 16 «Запретить доступ к флешкам»
- Лабораторная работа 17 «Настроить права доступа к флешкам»
- Лабораторная работа 18 «Настроить контроль доступа к веб-ресурсам»
- Лабораторная работа 19 «Настроить Адаптивный Контроль Аномалий»

### Модуль 4 «Сопровождение»

- Как поддерживать защиту
- Что делать каждый день
- Что делать, если что-то случилось
- Что делать не каждый день
- Лабораторная работа 20 «Настроить дэшборд»
- Лабораторная работа 21 «Настроить инструменты для обслуживания»
- Лабораторная работа 22 «Собрать диагностическую информацию»

[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](#).