

**KL 002.12.1:**

# **Kaspersky Endpoint Security and Management**

## **Изучаемые продукты**

- Kaspersky Security Center
- Kaspersky Endpoint Security for Windows

## **Цель курса**

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.

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

- 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

## **Длительность**

3 дня.

## **Требования к участникам**

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

# Содержание

## 1. Внедрение

- 1.1. Общие сведения
- 1.2. Установка Kaspersky Security Center
  - [Лабораторная работа 1.](#) Установить Kaspersky Security Center
- 1.3. Установка Kaspersky Endpoint Security на компьютеры
  - [Лабораторная работа 2.](#) Внедрить Kaspersky Endpoint Security
- 1.4. Работа с группами управляемых устройств
  - [Лабораторная работа 3.](#) Создать структуру управляемых компьютеров
- 1.5. Kaspersky Security Center Cloud Console

## 2. Управление защитой

- 2.1. Как Kaspersky Endpoint Security защищает компьютер
- 2.2. Как настроить защиту файлов
- 2.3. Как настроить защиту от угроз по сети
  - [Лабораторная работа 4.](#) Настроить защиту от файловых угроз
  - [Лабораторная работа 5.](#) Настроить защиту от почтовых угроз
  - [Лабораторная работа 6.](#) Проверить защиту от веб-угроз
- 2.4. Как настроить защиту от сложных угроз
  - [Лабораторная работа 7.](#) Проверить защиту сетевых папок от программ-вымогателей
  - [Лабораторная работа 8.](#) Проверить защиту от бесфайловых угроз
  - [Лабораторная работа 9.](#) Проверить защиту от эксплойтов
  - [Лабораторная работа 10.](#) Настроить Предотвращение вторжений для защиты от программ-вымогателей
- 2.5. Как контролировать сетевые соединения
  - [Лабораторная работа 11.](#) Проверить Защиту от сетевых атак

## 3. Контроль

- 3.1. Общие сведения
- 3.2. Контроль приложений
  - [Лабораторная работа 12.](#) Настроить Контроль приложений
  - [Лабораторная работа 13.](#) Заблокировать запуск неизвестных файлов в сети
- 3.3. Контроль устройств
- 3.4. Веб-Контроль
  - [Лабораторная работа 14.](#) Настроить контроль доступа к веб-ресурсам
- 3.5. Адаптивный контроль аномалий
  - [Лабораторная работа 15.](#) Настроить Адаптивный контроль аномалий

## 4. Kaspersky Endpoint Detection and Response Optimum

- 4.1. Введение
- 4.2. Развертывание Kaspersky Endpoint Detection and Response Optimum
- 4.3. Реагирование на событие обнаружения
  - [Лабораторная работа 16.](#) Имитировать атаку на сеть предприятия
  - [Лабораторная работа 17.](#) Развернуть Kaspersky Endpoint Detection and Response Optimum
  - [Лабораторная работа 18.](#) Подготовить Endpoint Detection and Response Optimum к работе
  - [Лабораторная работа 19.](#) Расследование инцидента

## 5. Администрирование

- 5.1. Усиление защиты Сервера администрирования
- 5.2. Аварийное восстановление
- 5.3. Настройка политик и задач

[Лабораторная работа 20.](#) Настроить защиту паролем

- 5.4. Хранение событий и интеграция с SIEM
- 5.5. Управление уязвимостями
- 5.6. Панели мониторинга и отчеты

[Лабораторная работа 21.](#) Настроить панель мониторинга

[Лабораторная работа 22.](#) Настроить отчеты

- 5.7. Чеклисты
- 5.8. Техническая поддержка

[Лабораторная работа 23.](#) Собрать диагностическую информацию

## Что нового

Материалы курса и лабораторные работы обновлены в соответствии с функционалом версий Kaspersky Security Center 14.1 и Kaspersky Endpoint Security 12.1.

В презентацию и учебник добавлена следующая информация:

- Новый модуль Kaspersky Endpoint Detection and Response Optimum
- Советы по усилению защиты Сервера администрирования во избежание компрометации
- Особенности развертывания защиты в Kaspersky Security Center Cloud Console
- Управление уязвимостями
- Интеграция с SIEM