

## KL 002.12.7:

# Kaspersky Endpoint Security and Management

## Изучаемые продукты

- Kaspersky Security Center Linux
- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux

## 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, 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. В данном курсе под узлами подразумеваются серверы и рабочие станции под управлением Windows и Linux.

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

- Описать возможности Kaspersky Endpoint Security и Kaspersky Security Center
- Спроектировать и внедрить оптимальное решение для защиты небольших сетей, основанное на Kaspersky Endpoint Security и управляемое через Kaspersky Security Center
- Осуществлять обслуживание внедренной системы на всех стадиях эксплуатации

## Длительность

4 дня

## Требования к участникам

Курс ориентирован на инженеров технической и предпродажной поддержки. От участников требуется:

- Понимание основ сетевых технологий: TCP/IP, DNS, электронной почты, web

- Базовые навыки администрирования ОС Windows и Linux
- Базовые знания об информационной безопасности

## Темы

1. Внедрение
2. Управление защитой Windows
3. Контроль безопасности Windows
4. EDR Optimum (Windows)
5. Защита Linux
6. Администрирование

## Лабораторные работы

- |                         |                                                                                 |
|-------------------------|---------------------------------------------------------------------------------|
| Лабораторная работа 1.  | Установить {ksc}                                                                |
| Лабораторная работа 2.  | Настроить {ksc}                                                                 |
| Лабораторная работа 3.  | Внедрить Kaspersky Endpoint Security Windows                                    |
| Лабораторная работа 4.  | Создать структуру групп управляемых компьютеров                                 |
| Лабораторная работа 5.  | Настроить защиту от файловых угроз                                              |
| Лабораторная работа 6.  | Настроить защиту от почтовых угроз                                              |
| Лабораторная работа 7.  | Проверить защиту от веб-угроз                                                   |
| Лабораторная работа 8.  | Проверить защиту сетевых папок от программ-вымогателей                          |
| Лабораторная работа 9.  | Проверить Защиту от бесфайловых угроз                                           |
| Лабораторная работа 10. | Проверить Защиту от эксплойтов                                                  |
| Лабораторная работа 11. | Настроить компонент Предотвращение вторжений для защиты от программ-вымогателей |
| Лабораторная работа 12. | Проверить Защиту от сетевых атак                                                |
| Лабораторная работа 13. | Настроить Контроль программ                                                     |
| Лабораторная работа 14. | Заблокировать запуск неизвестных файлов в сети                                  |
| Лабораторная работа 15. | Настроить контроль доступа к веб-ресурсам                                       |
| Лабораторная работа 16. | Настроить Адаптивный Контроль Аномалий                                          |
| Лабораторная работа 17. | Имитировать атаку на сеть предприятия                                           |
| Лабораторная работа 18. | Развернуть Kaspersky Endpoint Detection and Response                            |

- Лабораторная работа 19. Подготовить Kaspersky EDR к работе
- Лабораторная работа 20. Расследовать инцидент
- Лабораторная работа 21. Настроить защиту паролем
- Лабораторная работа 22. Настроить панель мониторинга
- Лабораторная работа 23. Настроить отчеты
- Лабораторная работа 24. Собрать диагностическую информацию
- Лабораторная работа 25. Установить {kesl} на управляемые устройства
- Лабораторная работа 26. Добавить компьютеры с ОС Linux в структуру групп управляемых компьютеров
- Лабораторная работа 27. Настроить базовую защиту сервера с операционной системой Linux
- Лабораторная работа 28. Настроить расширенную защиту сервера с операционной системой Linux
- Лабораторная работа 29. Работа с контролем безопасности на компьютере с ОС Linux
- Лабораторная работа 30. Управление защитой с помощью kesl-control
- Лабораторная работа 31. Управление учетными записями в Linux и администрирование устройств