Kaspersky Secure Mail Gateway (036.3)

KL-036.3 **Длительность** 1 день

Кому следует посетить

Тренинг предназначен для администраторов, которые планируют защищать корпоративный почтовый трафик от вредоносных объектов и спама.

Предварительные требования

- Базовые знания протоколов электронной почты и принципов работы почтовых серверов.
- Базовое понимание сетевых технологий: TCP/IP, DNS.
- Базовые знания принципов защиты информации.

Содержание курса

Тренинг предназначен для администраторов, которые планируют защищать корпоративный почтовый трафик от вредоносных объектов и спама. Курс описывает основные сценарии интеграции продукта в существующую инфраструктуру и объясняет, как настроить защиту почты и аутентификацию входящей почты с помощью SPF, DKIM, DMARC.

Изучаемый продукт: Kaspersky Secure Mail Gateway 2.1.

Программа курса

Введение

- Принципы работы электронной почты
- Защита от почтовых угроз
- Принципы работы Kaspersky Secure Mail Gateway

Глава 1. Как развернуть Kaspersky Secure Mail Gateway

- Установка и настройка ОС (VA)
- Установка KSMG в виде rpm/deb пакета (SA)
- Настройка почтового релея (VA)
- Лабораторная работа 1. Установите Kaspersky Secure Mail Gateway

- Первоначальная настройка, активация
- Лабораторная работа 2. Установите лицензионный ключ
- Лабораторная работа 3. Настройте почтовый трафик
- Лабораторная работа 4. Проверьте работу Kaspersky Secure Mail Gateway
- Лабораторная работа 5. Настройте подключение к Active Directory

Глава 2. Управление защитой

- Списки
- Анти-Спам
- Антивирус и Проверка ссылок
- Лабораторная работа 6. Списки
- Лабораторная работа 7. Анализ заголовков и Анти-Спам
- Лабораторная работа 8. Настройте Антивирус
- Анти-Фишинг, Контентная фильтрация и Проверка подлинности
- Лабораторная работа 9. Контентная фильтрация
- Лабораторная работа 10. Настройте проверку подлинности для входящей почты

Глава 3. Обслуживание

- Панель мониторинга, журналы и отчёты
- Уведомления и Предупреждения
- Хранилище
- Лабораторная работа 11. Настройка дешборда

5. Глава 4. Расширенные настройки

- Шифрование и DKIM
- Учётные записи
- Лабораторная работа 12. Настройте доступ для сотрудника HelpDesk
- Масштабирование и обслуживание
- Интеграция с другими системами