

KL 036.3:

Kaspersky Secure Mail Gateway

Изучаемые продукты

- Kaspersky Secure Mail Gateway 3.0

Описание курса

Тренинг предназначен для администраторов, которые планируют защищать корпоративный почтовый трафик от вредоносных объектов, спама и утечек конфиденциальных данных. Курс описывает основные сценарии интеграции Kaspersky Secure Mail Gateway в существующую инфраструктуру и объясняет, как настроить защиту почты и аутентификацию входящей почты с помощью SPF, DKIM и DMARC. В программу включены новые технологии: анализ QR-кодов в письмах и вложениях, обезвреживание содержимого (CDR) для нейтрализации zero-day-угроз, а также проверка зашифрованных архивов с использованием паролей из тела письма.

Длительность

1 день

Требования к участникам

Базовые знания протоколов электронной почты и принципов работы почтовых серверов.

Базовое понимание сетевых технологий: TCP/IP, DNS. Базовые знания принципов защиты информации.

Содержание

Введение

- 1.1. Как работает почта
- 1.2. Защита от почтовых угроз
- 1.3. Новые вызовы для почтовых шлюзов
- 1.4. Стандарты SMTP
- 1.5. Проверка подлинности
- 1.6. Принципы работы Kaspersky Secure Mail Gateway

2. Глава 2. Как развернуть Kaspersky Secure Mail Gateway

- 2.1. Установка и настройка ОС в виде Virtual Appliance
- 2.2. Установка KSMG в виде rpm/deb пакета (Standalone)
- 2.3. Интеграция с системой фильтрации
- 2.4. Настройка почтового релея для Virtual Appliance

Лабораторная работа 1. Установите Kaspersky Secure Mail Gateway

- 2.5. Первоначальная настройка, активация

Лабораторная работа 2. Проверьте работу Kaspersky Secure Mail Gateway

Лабораторная работа 3. Настройте подключение к Active Directory

Лабораторная работа 4. Настройте доступ в веб консоль KSMG через SSO

3. Глава 3. Управление защитой

- 3.1. Списки
- 3.2. Анти-Спам
- 3.3. Антивирус
- 3.4. Проверка зашифрованных вложений

Лабораторная работа 5. Списки

Лабораторная работа 6. Анализ заголовков и Анти-Спам

Лабораторная работа 7. Антивирус

Лабораторная работа 8. Анализ зашифрованных вложений

- 3.5. Анти-Фишинг
- 3.6. Контентная фильтрация
- 3.7. Проверка подлинности
- 3.8. Анализ QR-кодов

Лабораторная работа 9. Контентная фильтрация

Лабораторная работа 10. Анти-фишинг

Лабораторная работа 11. Настройте проверку подлинности для входящей почты

- 3.9. Обезвреживание и восстановление содержимого

Лабораторная работа 12. Настройка Content Disarm & Reconstruction

4. Глава 4. Обслуживание

- 4.1. Панель мониторинга, журналы и отчёты
- 4.2. Уведомления и Предупреждения
- 4.3. Очередь сообщений
- 4.4. Хранилище

Лабораторная работа 13. Настройка панели мониторинга

5. Глава 5. Лицензирование

6. Глава 6. Расширенные настройки

- 6.1. Шифрование и DKIM
- 6.2. Учётные записи
- 6.3. Масштабирование и обслуживание
- 6.4. Интеграция с другими системами