

Описание курса «Основы сетевой безопасности. Часть 1: Межсетевые экраны»

Целевая аудитория

Курс «Основы сетевой безопасности. Часть 1: Межсетевые экраны» разработан совместно с факультетом вычислительной математики и кибернетики (ВМК) Московского государственного университета имени М. В. Ломоносова.

Курс предназначен для сетевых администраторов, желающих изучить теоретические основы сетевой безопасности и получить практические навыки по развертыванию и настройке **межсетевых экранов**, для студентов и аспирантов направлений ВПО 010400 «Прикладная математика и информатика» и 010300 «Фундаментальная информатика и информационные технологии», а также для всех, кто интересуется современными сетевыми технологиями и принципами обеспечения сетевой безопасности.

Предварительная подготовка

Данный курс требует прохождения курса «Основы сетевых технологий. Часть 1: Основы передачи и коммутации данных в компьютерных сетях», а также знания основ сетевого взаимодействия и стека протоколов TCP/IP.

Сертификаты

После прохождения курса, слушатель может получить сертификат ВМК МГУ им. Ломоносова, а после сдачи сертификационного экзамена – сертификат D-Link.

Сертификационный экзамен состоит из практической части, сдаваемой в [учебном центре ВМК МГУ им. Ломоносова](#), и теста на портале дистанционного обучения D-Link.

Теоретическая часть курса может быть самостоятельно изучена слушателем на [портале дистанционного обучения и сертификации D-Link](#). В этом случае для получения сертификата слушатель может сдать практический экзамен в учебном центре ВМК МГУ им. Ломоносова, и тест на портале дистанционного обучения D-Link. Также слушатель может изучить только практическую часть курса в учебном центре ВМК МГУ им. Ломоносова и сдать сертификационный экзамен.

Описание курса

Длительность курса – 72 академических часа. Курс включает лекционную (32 часа) и практическую (40 часов) части. Слушатели могут изучить теоретическую часть курса [в учебном центре ВМК МГУ им. Ломоносова](#) или самостоятельно на [портале дистанционного обучения и сертификации D-Link](#).

Целью курса является изучение принципов и получение практических навыков создания безопасной сетевой инфраструктуры с использованием межсетевых экранов D-Link DFL-860E (имеют сертификат ФСТЭК).

По окончании курса слушатели будут

- знать:
 - принципы создания надежной и безопасной ИТ-инфраструктуры;
 - классификацию межсетевых экранов;
 - классификацию систем обнаружения и предотвращения проникновений;
- иметь практические навыки:
 - основ администрирования и создания политик межсетевого экрана;

- использования различных способов приоритизации трафика и создания альтернативных маршрутов;
- совместного использования межсетевых экранов и систем обнаружения и предотвращения проникновений.

Оборудование

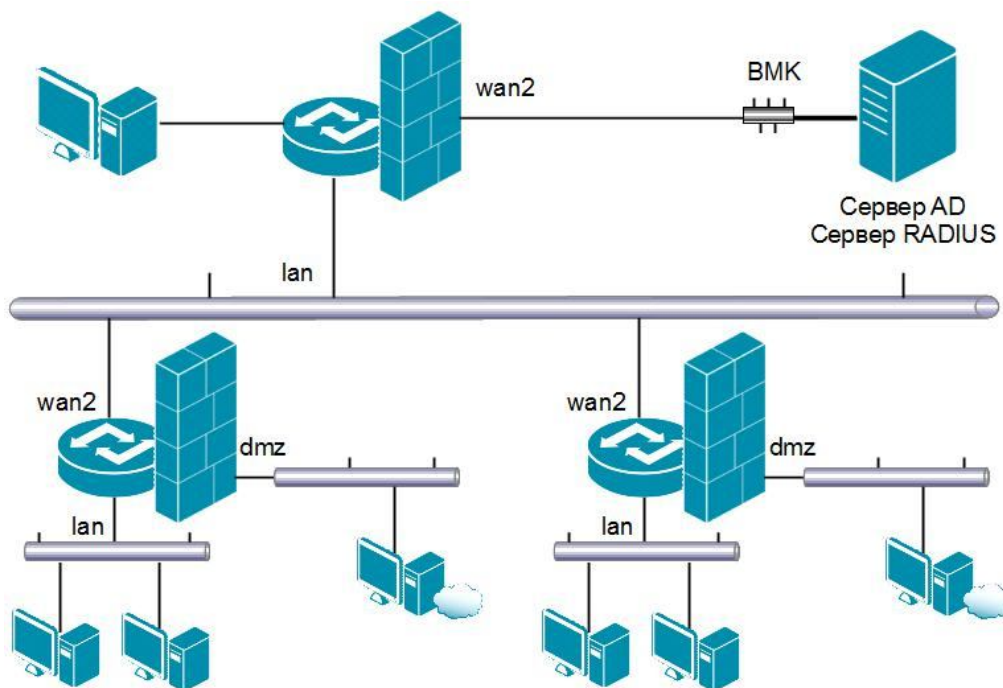
Для проведения лабораторных работ на 1 рабочее место требуется следующее оборудование:

- 3 компьютера, один из которых выступает в роли Web-сервера;
- 1 межсетевой экран DFL-860E;
- кабели Ethernet.

Дополнительно:

- 1 компьютер, выступающий в роли сервера, на котором установлен контроллер домена (сервер AD) и RADIUS-сервер.

Топология класса



Программа курса

Теория:

1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры

- Введение
- Классификация сетевых атак
 - Пассивная атака
 - Активная атака

- Определение расположения атакующего
- Соглашения по именованию атак
- **Триада безопасной ИТ-инфраструктуры – Конфиденциальность, Целостность, Доступность**
- **Гарантирование выполнения**
- **Анализ рисков**
- **Аутентификация и управление идентификациями**
- **Управление доступом**
- **Обеспечение отчетности**
- **Гарантирование доступности**
- **Управление конфигурациями**
- **Управление инцидентами**
- **Использование третьей доверенной стороны**
- **Криптографические механизмы безопасности**

2. Сегментирование сетей на канальном уровне

- **Использование технологии VLAN для создания подсетей**
- **Стандарт IEEE 802.1Q**
- **Типовая топология сети с использованием VLAN**
- **VLAN на основе портов**

3. Межсетевые экраны

- **Введение**
- **Технологии межсетевых экранов**
 - Стек протоколов
 - Состояния TCP-соединения
 - Классификация межсетевых экранов
 - Ограниченность анализа межсетевого экрана
- **Политика межсетевого экрана**
 - Политики, основанные на IP-адресах и протоколах
 - Политики, основанные на идентификации пользователя
 - Политики, основанные на сетевой активности
 - Основные рекомендации
- **Межсетевые экраны с возможностями NAT**
 - Используемая терминология и основные понятия
 - Статическое и динамическое назначение адресов
 - Варианты выполнения NAT
 - Сеть с частными адресами и туннели
 - Свойства NAT
 - Обсуждение безопасности
- **Топология сети при использовании межсетевых экранов**
 - Принципы построения окружения межсетевого экрана
 - Архитектура с несколькими уровнями межсетевых экранов
 - DMZ-сети
 - Конечные точки VPN
 - Интранет
 - Экстранет
 - Компоненты инфраструктуры: коммутаторы
 - Расположение серверов в DMZ-сетях

- **Планирование и внедрение межсетевого экрана**
 - Планирование
 - Конфигурирование
 - Развертывание
 - Управление

4. Системы обнаружения и предотвращения проникновений

- **Определение**
- **Основное назначение IDPS**
- **Способы классификации IDPS**
 - Архитектура IDPS
 - Каналы связи и распределенность управления и принятия решения
 - Скорость реакции
 - Информационные источники
 - Анализ, выполняемый IDPS
 - Возможные ответные действия IDPS
- **Дополнительные инструментальные средства**
 - Системы анализа и оценки уязвимостей
 - Разница между системами анализа уязвимостей и системами обнаружения проникновения
 - Проверка целостности файлов
- **Выбор IDPS**
 - Определение окружения IDPS
 - Цели использования IDPS
 - Существующая политика безопасности
- **Требования организации к функционированию IDPS**
 - Цели организации
 - Требования к ресурсам, необходимым для функционирования IDPS
- **Возможности IDPS**
 - Учет возможного роста организации
 - Предоставляемая поддержка программного продукта
- **Развертывание IDPS**
 - Стратегия развертывания IDPS
 - Развертывание network-based IDPS
 - Развертывание host-based IDPS
 - Стратегии оповещения о тревогах
- **Сильные стороны и ограниченность IDPS**
 - Сильные стороны IDPS
 - Ограничения IDPS
- **Выходные данные IDPS**
- **Будущие направления развития IDPS**

5. Приоритизация трафика и создание альтернативных маршрутов

- **Создание альтернативных маршрутов доступа в интернет**
 - Альтернативные таблицы маршрутизации
 - Правила выбора таблицы маршрутизации
- **Приоритизация трафика**
 - Ограничение (шейпинг) трафика
 - Шейпинг трафика с использованием IDP

- Гарантирование полосы пропускания вместо ограничения трафика
- Правила порога

Практика:

Основные принципы создания надежной и безопасной ИТ-инфраструктуры

- Лабораторная работа №1. Основы администрирования межсетевого экрана
Лабораторная работа №2. Соединение двух локальных сетей межсетевыми экранами

Сегментирование сетей на канальном уровне

- Лабораторная работа №3. Сегментирование подсетей с использованием управляемых коммутаторов
Лабораторная работа №4. Сегментирование подсетей на основе port-based VLAN

Межсетевые экраны

- Лабораторная работа №5. Создание политики без проверки состояния
Лабораторная работа №6. Создание политик для традиционного (или исходящего) NAT
Лабораторная работа №7. Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing

Системы обнаружения и предотвращения проникновений

- Лабораторная работа №8. Антивирусное сканирование
Лабораторная работа №9. Обнаружение и предотвращение вторжений

Приоритизация трафика и создание альтернативных маршрутов

- Лабораторная работа №10. Создание альтернативных маршрутов с использованием статической маршрутизации
Лабораторная работа №11. Ограничение полосы пропускания трафика
Лабораторная работа №12. Ограничение полосы пропускания P2P-трафика с использованием IDP