Описание курса «Основы информационной безопасности»

Целевая аудитория

Курс «Основы информационной безопасности» предназначен для студентов среднего профессионального образования, студентов высших учебных заведений, обучающихся по направлению подготовки «Информационная безопасность» (код 10.00.00), для слушателей программ профессиональной переподготовки и повышения квалификации, а также для специалистов служб информационной безопасности, сетевых и системных администраторов, желающих систематизировать свои знания и получить практические навыки работы с современными средствами защиты информации.

Предварительная подготовка

При отсутствии базовой подготовки рекомендуется прохождение курсов «Основы сетевых технологий. Часть 1: Передача и коммутация данных в компьютерных сетях», «Основы сетевых технологий. Часть 3: Технологии TCP/IP».

Сертификаты

После прохождения курса, слушатель может сдать сертификационный экзамен в авторизованном учебном центре или ближайшем офисе и получить сертификат D-Link. Экзамен состоит из теста на портале дистанционного обучения D-Link.

Описание курса

Длительность курса – 72 академических часа. Курс включает лекционную и практическую части.

Целью курса является формирование у слушателей целостного понимания принципов обеспечения информационной безопасности, изучение современных методов и средств защиты корпоративных сетей, а также получение практических навыков настройки оборудования и программного обеспечения для противодействия киберугрозам. В курсе рассматриваются ключевые концепции безопасности (конфиденциальность, целостность, доступность), архитектурные подходы (Defense in Depth, Zero Trust), криптографические механизмы, а также широкий спектр технологий защиты: от сетевой сегментации и межсетевого экранирования до систем обнаружения сложных атак (EDR, XDR, SIEM) и современных VPN-протоколов (IPSec, WireGuard).

Курс может использоваться как самостоятельная дисциплина или как практико-ориентированная часть образовательных программ в средних специальных и высших учебных заведениях, готовящих специалистов по защите информации.

После прохождения курса слушатели смогут:

- ориентироваться в современном ландшафте киберугроз и российской нормативной базе в области ИБ;
- применять принципы управления рисками, идентификации, аутентификации и авторизации для контроля доступа к информационным активам;
- использовать криптографические методы для обеспечения конфиденциальности, целостности и аутентичности данных;
- проектировать и настраивать сегментированную сетевую инфраструктуру с использованием VLAN и межсетевых экранов, включая организацию DMZ;
- организовывать защищённые удалённые подключения (VPN) с использованием протоколов L2TP, IPSec, SSL/TLS и WireGuard;

- реализовывать базовые элементы архитектуры Zero Trust, такие как явная проверка и микросегментация;
- настраивать политики качества обслуживания (QoS) и маршрутизации на основе политик (PBR) для обеспечения доступности критичных сервисов.

Оборудование

Минимальные требования (из расчета для одного рабочего места):

Оборудование	**Количество**
Маршрутизатор DSA-2108S (или DSA-2003)	2 шт.
Коммутатор DGS-1210-28/FL2A	2 шт.
Рабочая станция с ОС Linux (Ubuntu 20.04 LTS или выше)	4 шт.
Кабель Ethernet	7 шт.
Кабель USB-COM (RS-232)*	1 шт.

*Кабель USB-COM (RS-232) необходим в том случае, если на рабочей станции отсутствует COM-порт для подключения консольного кабеля.

Содержание курса

1. **Понятие информационной безопасности**

   1.1 Модель информационной безопасности (триада CIA, сервисы безопасности)
   1.2 Сетевые атаки (пассивные, активные, классификация)
   1.3 Оценка и обработка рисков. Модель нарушителя
   1.4 Менеджмент инцидентов информационной безопасности
   1.5 Оборона в глубину (Defense in Depth)
   1.6 Архитектура Zero Trust
   1.7 Киберугрозы и тенденции в защите (APT, Ransomware, угрозы ИИ)
   1.8 Российская нормативная база в области ИТ (ФСТЭК, ФСБ, Банк России, Роскомнадзор)

2. **Идентификация и аутентификация**

   2.1 Идентификация
   2.2 Аутентификация (факторы, методы, протоколы)
   2.3 Современные тенденции (беспарольная, SSO, адаптивная, Zero Trust)

3. **Авторизация**

   3.1 Списки управления доступом (ACL)
   3.2 Модели управления доступом (DAC, MAC, RBAC, ABAC)
   3.3 Авторизация в корпоративных сетях (RADIUS, LDAP, SAML, OAuth 2.0)

4. **Обеспечение отчетности и аудит**

   4.1 Активная оценка состояния компьютерной системы и сети (оценка уязвимостей, тестирование на проникновение)

5. **Криптографические механизмы безопасности**

   5.1 Типы криптографических механизмов
   5.2 Криптография с симметричным ключом
   5.3 Криптография с асимметричным ключом
   5.4 Хеш-функции

5.5 Общее руководство по управлению ключами
5.6 Внедрение криптографии в корпоративных системах

6. **Гарантирование доступности**
7. **Сегментация сетей на канальном уровне**
8. **Межсетевые экраны**

8.1 Технологии межсетевых экранов (Stateless, Stateful, NGFW, WAF)
8.2 Политика межсетевого экрана
8.3 Межсетевые экраны с возможностями NAT
8.4 Традиционная топология сети при использовании межсетевых экранов
8.5 Принципы построения окружения межсетевого экрана

9. **Технологии удаленного доступа**

9.1 Архитектуры удаленного доступа (Client-to-Site, Site-to-Site)
9.2 Протокол GRE
9.3 Протокол L2TP
9.4 Протокол IPSec
9.5 Протокол WireGuard
9.6 Протоколы SSL/TLS
9.7 Технологии удаленного доступа для мобильных устройств
9.8 Zero Trust Network Access (ZTNA)

10. **Маршрутизация на основе политик (PBR)**
11. **Качество обслуживания (QoS)**

11.1 Понятие класса обслуживания
11.2 Per-Hop Behavior (PHB)
11.3 Приоритизация пакетов
11.4 Классификация пакетов
11.5 Маркировка пакетов
11.6 Организация очередей и диспетчеризация
11.7 Механизм Traffic Shaping
11.8 Качество обслуживания (QoS) как элемент информационной безопасности

12. **Современные подходы к безопасности корпоративных сетей**

12.1 Межсетевой экран нового поколения (NGFW)
12.2 Системы обнаружения и реагирования на угрозы (EDR, XDR, SIEM, SOAR)

Приложение: Практические примеры и разбор инцидентов

Лабораторные работы

№	Название
1	Настройка прав доступа для групп пользователей
2	Сегментация сети с использованием VLAN
3	Настройка защиты сервера от сканирования портов и проникновений с помощью nftables
4	Настройка защиты сервера от сканирования портов и проникновений с помощью iptables
5	Настройка защиты SSH-сервера от атак полного перебора
6	Практическая реализация модели Zero Trust: явная проверка, микросегментация и взаимная аутентификация
7	Настройка NAT
8	Организация удаленного доступа к серверам, расположенным в DMZ
9	Организация удаленного доступа с помощью протокола GRE
10	Организация удаленного доступа с помощью протокола L2TPv2
11	Организация удаленного доступа с помощью протокола L2TPv3
12	Организация удаленного доступа с помощью протокола IPSec
13	Реализация принципов Zero Trust при построении защищённой сети на базе WireGuard
14	Настройка маршрутизации на основе политик
15	Обеспечение доступности служебного трафика в условиях DoS-атаки с помощью алгоритма HTB
16	Централизованный сбор логов и обнаружение атак с помощью syslog