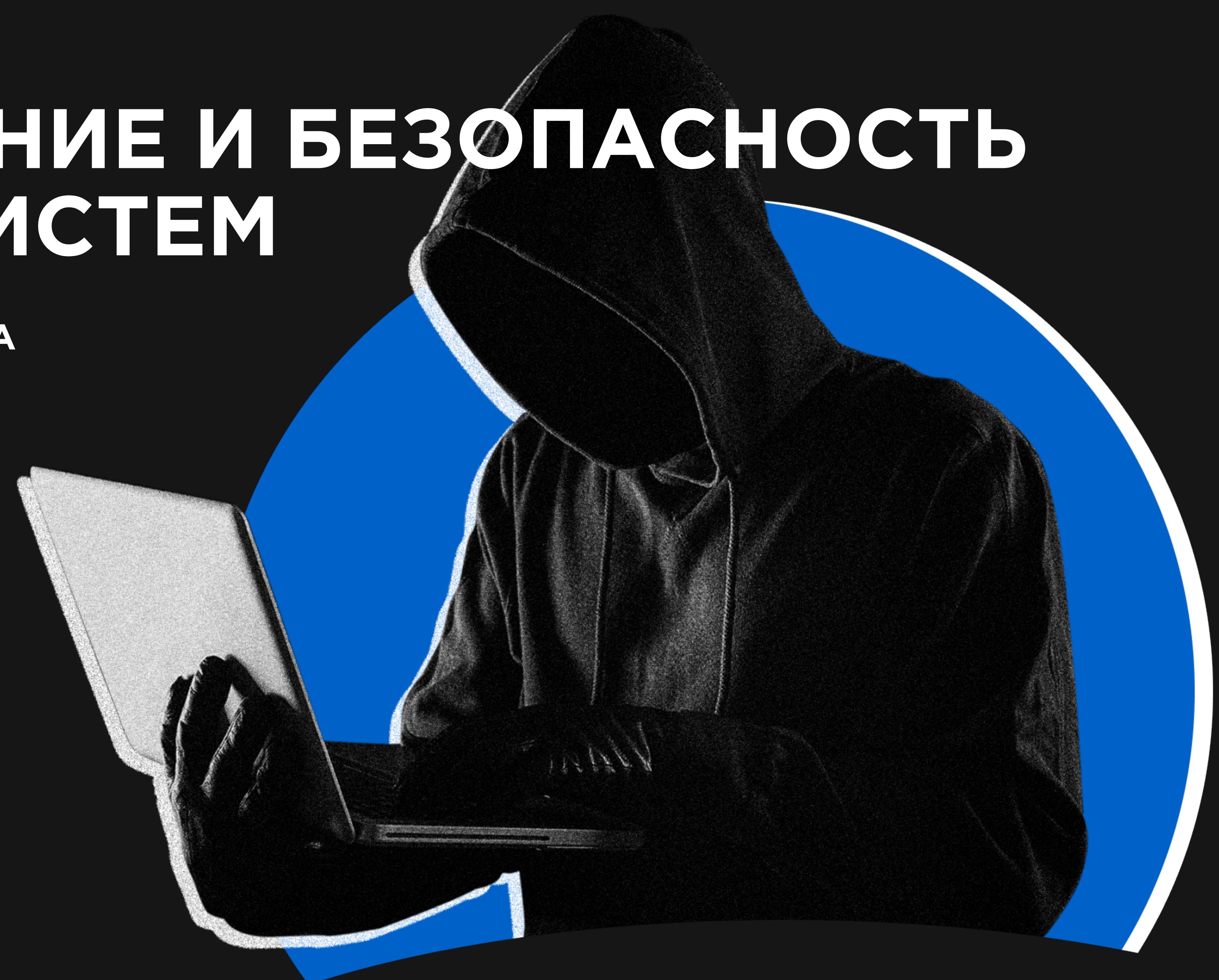


# ПРОГРАММА КУРСА

## АДМИНИСТРИРОВАНИЕ И БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ

12 НЕДЕЛЬ / 252 ЧАСА / ДИПЛОМ ГОС ОБРАЗЦА



# **Модуль 1. «Windows и базовый AD» (48 акад. час.)**

## **Занятие 1. Windows Server, Domain Services, Active Directory Management**

- Лекция «Обзор технологий и настроек Microsoft: Windows server»
- Практическая работа №1.1 (Подготовка стендса)
- Практическая работа №1.2 (Первоначальная настройка Windows)

## **Занятие 2. Администрирование Windows и Active Directory**

- Лекция «Как устроен Windows»
- Лекция «Что такое домен, Active Directory и как это работает»
- Практическая работа №2 (Настройка Windows сервера как контроллера домена)

## **Занятие 3. AAA в Windows**

- Лекция «Типы и протоколы аутентификации в Windows»
- Практическая работа №3 (Анализ памяти процесса lsass.exe)

## **Занятие 4. Инфраструктурные сервисы в домене**

- Лекция «DNS, DHCP, групповые политики»
- Практическая работа №4.1 (Настройка сервиса DNS)
- Практическая работа №4.2 (Настройка сервиса DHCP)
- Практическая работа №4.3 (Настройка отказоустойчивости DHCP)
- Практическая работа №4.4 (Настройка групповых политик)

## **Занятие 5. Обмен данными в домене и средства мониторинга Windows**

- Лекция «Обмен данными в домене»
- Лекция «Средства мониторинга Windows»
- Практическая работа №5.1 (Настроить инстанс обмена данными)
- Практическая работа №5.2 (Настроить журналирование событий, сборку и отправку журналов)

## **Занятие 6. Базовые атаки и компрометация доменной Windows-инфраструктуры**

- a) Лекция «Основные протоколы в Windows-инфраструктуре»
- b) Практическая работа №6.1 (Базовые атаки на Windows-инфраструктуру)
- c) Практическая работа №6.2 (Компрометация доменной Windows-инфраструктуры)

# **Модуль 2. «ОС Linux» (48 акад. час.)**

## **Занятие 1. Основы Linux**

- Лекция «Основы ОС Linux»
- Практическая работа №1.1 (Основы работы в терминале Linux)
- Практическая работа №1.2 (Основы работы с GREP)
- Практическая работа №1.3 (Основы работы с Vim)

## **Занятие 2. Администрирование Linux**

- Лекция «Администрирование и мониторинг в ОС Linux»
- Практическая работа №2.1 (Основы мониторинга ОС Linux с помощью утилит)
- Практическая работа №2.2 (Установка и настройка сервера SSH в Linux)
- Практическая работа №2.3 (Установка и настройка SSH-authorized\_keys)
- Практическая работа №2.4 (Сбор информации о Linux и WGET)
- Практическая работа №2.5 (Переменные окружения)

## **Занятие 3. Сервисы Linux**

- Лекция «Основы работы с сервисами ОС Linux»
- Практическая работа №3.1 (Написание скриптов для Cron)
- Практическая работа №3.2 (Настройка SFTP и FileZilla)
- Практическая работа №3.3 (Apache, Telnet, FTP, SMB)

## **Занятие 4. Безопасность Linux серверов**

- Лекция «Linux Firewall, Iptables.»
- Практическая работа №4.1 (Настройка файлового сервера в корпоративной инфраструктуре)
- Практическая работа №4.2 (Fail2Ban-SSH и Brute-force attack)
- Практическая работа №4.3 ("Fail2Ban и Dos/DDoS attack" на примере nginx)

## **Занятие 5. Работа с файловой системой Linux**

- Лекция «Файловые системы native для ОС семейства \*nix»
- Практическая работа №5 (Настройка и конфигурация файловых систем Linux и прав доступа на базе Debian 11)

## **Модуль 3. «Сети и протоколы» (96 акад. час.)**

### **Занятие 1. Введение в сетевые технологии**

- Лекция «Введение в сетевые технологии»
- Практическая работа №1.1 (Развертывание виртуальной лаборатории PNET)
- Практическая работа №1.2 (Базовая работа с виртуальной лабораторией PNET)

### **Занятие 2. Модель OSI. Канальный уровень - L2**

- Лекция «Топологии сети. Spanning Tree Protocol. Сегментация сети (VLAN).»
- Практическая работа №2.1 (Переполнение таблицы коммутации)
- Практическая работа №2.2 (Arp-Spoofing)
- Практическая работа №2.3 (VLAN hopping)

### **Занятие 3. Модель OSI. Сетевой уровень - L3**

- Лекция «Сетевой уровень OSI»
- Практическая работа №3.1 (Статическая маршрутизация)
- Практическая работа №3.2 (OSPF)
- Практическая работа №3.3 (BGP)

### **Занятие 4. Модель OSI. Транспортный уровень - L4**

- Лекция «Транспортный уровень OSI»
- Практическая работа №4 (MITM, SPAN)

### **Занятие 5. Безопасность локальной сети**

- Лекция «Защита сегментов сети, Port Security, базовые списки контроля доступа, защита коммутаторов»
- Практическая работа №5 (Безопасность локальной сети)

### **Занятие 6. Протоколы верхних уровней**

- Лекция «Протоколы верхних уровней»
- Практическая работа №6 (Протоколы верхних уровней)

## **Модуль 4. «WEB» (48 акад. час.)**

### **Занятие 1. Введение в Web технологии**

- Лекция «Введение в Web технологии»
- Практическая работа №1 (Развертывание Web-сервера с помощью docker)

### **Занятие 2. Архитектура WEB**

- Лекция «Архитектура WEB»
- Практическая работа №2 (Базовые принципы разведки)

### **Занятие 3. Основные атаки и паттерны**

- Лекция «XXS, CSRF, SQL-Injection, RCE и многое другое»
- Практическая работа №3 (Основные атаки и паттерны)

### **Занятие 4. Web Application Firewall**

- Лекция «Что такое WAF, разновидности и принципы работы»
- Практическая работа №4 (Развертывание и настройка Web Application Firewall)

## **Итоговая аттестация (Демо-экзамен) (10 акад. час.)**

После окончания обучения вы будете проходить экзамен, направленный на оценку полученных знаний. Вам будет дано несколько практических заданий.

### **Примерный набор задач к демо-экзамену:**

- Установка Windows Server 2016, Windows 10, Kali Linux
- Развертывание домена
- Настройка групповых политик
- Настройка логирования
- Проведение атак
- Работа с основными командами Linux
- Установка и настройка ssh сервера и клиента
- Ограничение доступов в Linux
- Настройка автоматического запуска скрипта
- Установка и настройка SFTP
- Построение топологии сети в PNET
- Настройка VLAN
- Построение топологии сети, визуализирующую атаку типа MITM
- Настройка SPAN
- Определение почтовых серверов домена
- Определение имени сервера по ip адресу
- Развертывание WEB сервера с помощью Docker