



Исх. №10 от 23 сентября 2026 года

Руководителю

26 – 30 октября 2026 года
ДИСТАНЦИОННЫЙ КУРС ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ПО ПРОГРАММЕ

«ОСНОВЫ ПЕНТЕСТА - ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ»
с выдачей удостоверения о повышении квалификации в **объеме 40 часов**

Цель курса повышения квалификации: рассмотрение методологии и инструментария хакерских атак, поиск и анализ уязвимостей системы, практическая отработка возможных сценариев проникновения и имитация атак на систему.

Приглашаем: руководителей, начальников отделов и специалистов, ответственных за обеспечение информационной безопасности в организации, специалистам, желающим изучить основы пентеста.

Программа курса:

1. Методология и инструментарий хакерских атак

Классификация программного обеспечения, которое использует злоумышленник при взломе компьютерных систем.

Запуск Kali Linux знакомство с инструментами для пентеста.

Этапы взлома системы.

Знакомство с Metasploit Framework. Лабораторная работа: Запуск, знакомство с основными командами и модулями.

Изучение и сканирование сети с использованием модулей Metasploit Framework.

Лабораторная работа: Определение ip-адресов, портов, название операционных систем с использованием Metasploit Framework.

2. Активный анализ сервисов внутри сети, сбор информации о сети

Знакомство с основными сетевыми службами.

Сканирование портов и определение версий сетевых служб операционных систем с использованием Nmap.

Проблемы, связанные со сканированием внутри сети. Сканирование при включенном файрволле.

Проведение скрытого (Stealth) сканирования. Сканирование при включенном файрволле.

Атака "Brute-force" что это и чем опасна.

Перебор логинов и паролей к ssh, ftp, telnet с использованием модулей Metasploit Framework.

Получение доступа при слабом пароле.

Типы соединения со взломанной системой. Основные проблемы и опасности.

Лабораторная работа: Создание прямого и обратного соединения с использованием разных протоколов. Создание программы для удаленного подключения к взломанной системе.

3. Базовые атаки на систему

Социальная инженерия, как эффективный способ получения логинов и паролей.

Лабораторная работа: Использование социальной инженерии для получения логинов и паролей.

Создание фейкового сайта для кражи логина и пароля.

Вирусы, троянские программы что это и для чего нужны.

Лабораторная работа: Генерирование троянских программ их склеивание с другими программами запуск в систему.

Что такое эксплойты, виды эксплойтов для чего используются.

Лабораторная работа: Использование эксплойтов для проникновения в систему.

Поиск и использование эксплойтов.

Лабораторная работа: Интегрирование эксплойта в систему Metasploit Framework. Использование эксплойта для повышения привилегий в системе.

4. Изучение модуля Meterpreter в Metasploit Framework

Изучение основных команд, модулей для работы на взломанной системе с использованием Meterpreter.

Лабораторная работа: Использование основных команд и модулей Meterpreter для работы с взломанной системой.

Изучение дополнительных модулей Meterpreter.

Лабораторная работа: Использование различных дополнительных модулей Meterpreter для кражи снимков экрана, снимков с Web - камер, хешей, паролей на взломанной системе, настроек системы.

Кража информации с использованием кейлогеров.

Лабораторная работа: Настройка и использование кейлогера для кражи информации в взломанной системе.

Изменение различных настроек в системе для последующего проникновения.

Лабораторная работа: Отключение файрволов открытие определённых портов, создание пользователей, изменение прав доступа.

5. Методы закрепления в системе для последующего подключения

Создание бэкдоров в операционной системе Windows.

Лабораторная работа: Настройка бэкдора в системе на примере Meterpreter в Metasploit Framework
Установка и настройка сервисов для удаленного администрирования операционной системы Windows.

Лабораторная работа: Настройка сервисов telnet, RDP для удаленного подключения к системе.

Создание бэкдоров в операционной системе Debian Linux

Лабораторная работа: Настройка бэкдора в системе на примере netcat.

Установка и настройка сервисов для удаленного администрирования операционной системы Linux.

Лабораторная работа: Настройка сервисов ssh, VNC x11vnc для удаленного подключения к системе

Преподаватель курса

Мурзинцев С.В., преподаватель Института МОИБ, специалист – практик, читает курс по тестированию на проникновение.

Условия и стоимость участия

обучение с применением дистанционных технологий

Даты обучения (вебинар)

26 - 30 октября 2026 г. (5 дней)

Время обучения

по расписанию курса

Место обучения

удаленное место слушателя

В стоимость обучения входит

методические материалы, тестовый стенд
видеозапись, презентации лектора

СТОИМОСТЬ ОБУЧЕНИЯ для юридических лиц
с выдачей удостоверения в объеме 40 часов

19 990 руб.

СТОИМОСТЬ ОБУЧЕНИЯ для физических лиц
(предоплата 100%) с выдачей удостоверения в
объеме 40 часов

15 990 руб.

Лицензии:

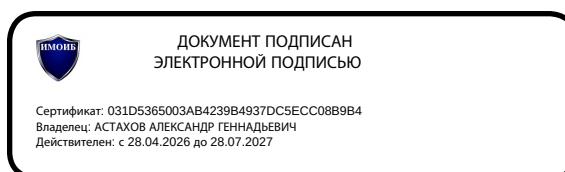
- Лицензия на право осуществления образовательной деятельности № Л035-01298-77/00184290 от 24.07.17 Департамента образования города Москвы.
- Лицензия ФСТЭК России (Л024-00107-77/01648168 от 17.12.24) на деятельность по технической защите конфиденциальной информации.

ПРЕДВАРИТЕЛЬНАЯ РЕГИСТРАЦИЯ ОБЯЗАТЕЛЬНА

тел. 8 (906) 055-28-55, тел. 8 (495) 268-13-42, e-mail: info@imoib.ru, сайт: www.imoib.ru

ЭЛЕКТРОННАЯ РЕГИСТРАЦИЯ НА САЙТЕ: <https://imoib.ru/training/course/2041>

Руководитель Института МОИБ



А.Г. Астахов