УТВЕРЖДАЮ
Генеральный директор
ООО «Мерион Нетворкс»
Тундайкина Т.Н.
«12» мая 2026 г.

Дополнительная профессиональная программа
повышения квалификации

«Этичный хакинг»

г. Москва
2026

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1. Общие сведения о программе

Дополнительная профессиональная программа повышения квалификации «Этичный хакинг и тестирование на проникновение (Penetration Testing)» (далее — Программа) разработана в соответствии с требованиями Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», приказа Министерства образования и науки Российской Федерации от 01 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», а также профессиональных стандартов в области информационной безопасности.

Программа ориентирована на специалистов в области информационных технологий, системных администраторов, сотрудников служб информационной безопасности и иных лиц, желающих освоить практические методы тестирования на проникновение (пентеста) и защиты информационных систем.

Наименование программы	Этичный хакинг и тестирование на проникновение (Penetration Testing)
Категория слушателей	Специалисты в области IT и ИБ, имеющие высшее или среднее профессиональное образование
Форма обучения	Заочная с применением дистанционных образовательных технологий (ДОТ)
Объём программы	290 академических часов
Срок освоения программы	Не менее 2 месяцев (доступ к платформе — 2 года)
Итоговый документ	Удостоверение о повышении квалификации установленного образца (для слушателей тарифа «Наставник»)
Разработчик	ООО «Мерион Нетворкс» (Merion Academy)

1.2. Цель программы

Цель Программы — формирование и совершенствование профессиональных компетенций в области выявления, анализа и устранения уязвимостей информационных систем методами этичного хакинга и тестирования на проникновение.

1.3. Задачи программы

Для достижения цели Программы решаются следующие задачи:

– ознакомить слушателей с методологиями и правовыми основами тестирования на проникновение;

– сформировать практические навыки работы с профессиональными инструментами пентеста (Nmap, Metasploit, Burp Suite, sqlmap, Mimikatz и др.);
– научить выявлять и эксплуатировать уязвимости сетевой инфраструктуры, веб-приложений, операционных систем Linux и Windows;
– освоить методы постэксплуатации и повышения привилегий в реальных сценариях атак;
– выработать навыки написания скриптов для автоматизации задач пентеста (Bash, Python);
– сформировать понимание мер защиты информационных систем и принципов безопасной архитектуры.

1.4. Требования к слушателям

К освоению Программы допускаются лица, имеющие высшее или среднее профессиональное образование. Рекомендуется наличие базовых знаний в области компьютерных сетей, операционных систем (Linux/Windows) и основ программирования.

1.5. Материально-техническое обеспечение

Реализация Программы осуществляется с применением дистанционных образовательных технологий на образовательной платформе Merion Academy (lms.merionet.ru). Для обучения слушателю необходимы:

– персональный компьютер или ноутбук (ОС: Windows 10/11, Ubuntu 20.04+, macOS 12+) с процессором не ниже Intel Core i5 / AMD Ryzen 5 и оперативной памятью не менее 8 ГБ (рекомендуется 16 ГБ);
– доступ к сети Интернет со скоростью не менее 10 Мбит/с;
– программное обеспечение: VirtualBox или VMware Workstation (для развёртывания учебной лаборатории), GNS3, Kali Linux (образ предоставляется платформой);
– веб-браузер актуальной версии (Google Chrome, Mozilla Firefox).

2. УЧЕБНЫЙ ПЛАН

№	Наименование раздела	Всего часов	Лекции/видео	Практика	Контроль
1	Введение в пентест. Методологии тестирования на проникновение. Работа с виртуальным полигоном.	21	8	10	3
2	Основы сетевого взаимодействия. Настройка стенда GNS3. Анализ трафика Wireshark. Атаки DHCP Starvation, ARP, MITM.	25	10	12	3
3	Веб-пентест. SQL-инъекции, Burp Suite, sqlmap. Серверные и клиентские уязвимости (Path Traversal, SSRF, XSS, CSRF). Основы WAF. Docker, DVWA, Juice Shop.	57	23	27	7
4	Эксплуатация и постэксплуатация Linux. Nmap, эскалация привилегий (sudo, capabilities, ядро, crontab). iptables. Metasploit, Searchsploit.	130	52	61	17
5	Windows и Active Directory. Компоненты AD. Эксплуатация Windows-систем. SMB Relay, Msfconsole, Mimikatz. Обеспечение безопасности Windows.	40	16	19	5
6	Программирование для хакинга. Bash. Python для пентеста: фаззинг, брутфорс, автоматизация Nmap. Решение задач на Hack The Box.	17	7	8	2
	ИТОГО	**290**	**116**	**136**	**38**

Примечание: лекции проводятся в формате видеоуроков с возможностью просмотра в удобное время. Практические занятия выполняются в виртуальной лаборатории (кибер-полигон). Промежуточный контроль — тестирование на платформе LMS.

3. РАБОЧАЯ ПРОГРАММА

Тема 1. Введение в пентест. Методологии тестирования на проникновение. Работа с виртуальным полигоном (21 ак. ч.)

Содержание. Понятие тестирования на проникновение (пентест). Виды пентеста: Black Box, White Box, Grey Box. Международные методологии: OSSTMM, PTES, OWASP Testing Guide, NIST SP 800-115. Этапы пентеста: разведка, сканирование, эксплуатация, постэксплуатация, отчётность. Правовые основы проведения пентеста в Российской Федерации. Развёртывание виртуальной лаборатории: установка VirtualBox/VMware, импорт образов Kali Linux и целевых машин, настройка изолированных сетевых сегментов.

Практические работы: настройка учебного стенда; знакомство с интерфейсом Kali Linux; создание отчётного шаблона по результатам пентеста.

Промежуточный контроль: тест (порог — 80%, неограниченное количество попыток).

Тема 2. Основы сетевого взаимодействия. Анализ трафика. Сетевые атаки (25 ак. ч.)

Содержание. Модели OSI и TCP/IP. Стек протоколов: Ethernet, IP, TCP/UDP, ARP, DHCP, DNS. Настройка эмулятора сетевого оборудования GNS3: создание топологий, интеграция с VirtualBox. Анализ сетевого трафика инструментом Wireshark: фильтры, диссекторы, статистика. Атака DHCP Starvation: исчерпание пула адресов с использованием Yersinia. Атаки на протокол ARP: ARP-спуфинг, построение таблицы ARP-кэша. Атаки Man-in-the-Middle (MITM): перехват трафика, SSL-stripping.

Практические работы: анализ захваченного трафика; проведение DHCP Starvation; выполнение ARP-спуфинга и MITM-атаки в учебной среде.

Промежуточный контроль: тест (порог — 80%).

Тема 3. Веб-пентест. SQL-инъекции, серверные и клиентские уязвимости (57 ак. ч.)

Содержание. Архитектура веб-приложений. OWASP Top 10. SQL-инъекции: классические, UNION-based, Blind, Time-based; автоматизация с sqlmap. Перехват и модификация HTTP-трафика с помощью Burp Suite (Proxy, Repeater, Intruder, Scanner). Серверные уязвимости: Path Traversal, Information Disclosure, SSRF, Command Injection, File Upload Vulnerability (FUV), XML External Entity (XXE) Injection. Клиентские уязвимости: Stored/Reflected/DOM-based XSS, CSRF. Основы Web Application Firewall (WAF):

принципы работы, обходы. Контейнеризация Docker: развёртывание уязвимых приложений DVWA и OWASP Juice Shop.

Практические работы: эксплуатация SQL-инъекции вручную и через sqlmap; обнаружение и эксплуатация XSS/CSRF; работа с DVWA и Juice Shop; написание скрипта-фаззера.

Промежуточный контроль: тест (порог — 80%).

Тема 4. Эксплуатация и постэксплуатация Linux (130 ак. ч.)

Содержание. Концепция Cyber Kill Chain. Разведка: пассивная (OSINT) и активная (Nmap). Техники сканирования Nmap: типы сканирований, NSE-скрипты, обход межсетевых экранов. Эскалация привилегий в Linux: через sudo (мисконфигурации), Linux Capabilities, уязвимости ядра (Dirty COW и аналоги), неправильно настроенный crontab. Фреймворк Metasploit: модули exploit, payload, post; работа с msfconsole. Searchsploit и Exploit-DB: поиск и адаптация публичных эксплойтов. Настройка межсетевого экрана iptables: цепочки, правила, NAT. Закрепление в системе, очистка следов.

Практические работы: полный цикл эксплуатации уязвимой Linux-машины; эскалация привилегий четырьмя методами; настройка iptables; работа с Metasploit.

Промежуточный контроль: тест (порог — 80%).

Тема 5. Windows и Active Directory. Эксплуатация корпоративной инфраструктуры (40 ак. ч.)

Содержание. Архитектура Microsoft Active Directory: домен, лес, доверительные отношения, контроллеры домена, групповые политики (GPO), Kerberos-аутентификация. Развёртывание учебного полигона AD: установка Windows Server, создание домена, ввод рабочих станций. Эксплуатация Windows: атака SMB Relay, получение оболочки через Msfconsole. Постэксплуатация: дамп учётных данных с Mimikatz (Pass-the-Hash, Pass-the-Ticket). Обеспечение безопасности Windows: харденинг, Windows Defender, политики аудита.

Практические работы: развёртывание стенда AD; проведение SMB Relay атаки; дамп паролей Mimikatz; настройка политик безопасности.

Промежуточный контроль: тест (порог — 80%).

Тема 6. Программирование для хакинга. Bash и Python (17 ак. ч.)

Содержание. Bash-скриптинг: переменные, условия, циклы, функции; автоматизация задач сканирования и сбора информации. Python для пентеста: работа с модулями socket, requests, subprocess; написание простого фаззера; реализация брутфорс-атаки; автоматизация Nmap через python-nmap. Решение практических задач на платформе Hack The Box.

Практические работы: написание Bash-скрипта для автоматической разведки; создание Python-фаззера и брутфорсера; решение задач Hack The Box.

Тема 7. Итоговая аттестация (10 ак. ч.)

Итоговая аттестация проводится в форме тестирования на платформе Merion Academy (lms.merionet.ru). Тест охватывает все разделы программы. Порог зачёта — 80% правильных ответов. Количество попыток — неограниченно. Оценивание: «зачёт» (80% и выше) / «незачёт» (до 79% включительно).

4. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ. ПОРЯДОК ПРОВЕДЕНИЯ АТТЕСТАЦИИ

Оценивание освоения Программы осуществляется в форме тестирования на образовательной платформе Merion Academy (lms.merionet.ru). Применяется система оценки «зачёт / незачёт» без промежуточных баллов.

4.1. Промежуточный контроль

По завершении каждого раздела (темы 1–6) слушатель проходит тематический тест. Параметры тестирования:

Параметр	Значение
Форма контроля	Тестирование в LMS (автоматизированная проверка)
Количество попыток	Неограниченно
Порог зачёта	≥ 80% правильных ответов
Результат «незачёт»	Менее 80% правильных ответов (до 79% включительно)
Система оценивания	Зачёт / Незачёт

4.2. Итоговая аттестация

Итоговая аттестация проводится в форме тестирования на платформе Merion Academy (lms.merionet.ru). К итоговой аттестации допускаются слушатели, успешно сдавшие все промежуточные тесты.

Параметр	Значение
Форма итоговой аттестации	Итоговое тестирование
Количество вопросов в тесте	60
Количество попыток	Неограниченно
Порог зачёта	≥ 80% правильных ответов
Результат «незачёт»	До 79% включительно — незачёт, пересдача без ограничений
Документ по итогам аттестации	Удостоверение о повышении квалификации — выдаётся слушателям тарифа «Наставник» при результате «зачёт»

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

5.1. Основная литература

18. Кейтс Д. Этичный хакер. Полное руководство по инструментам и методам взлома. — М.: БХВ-Петербург, 2022. — 832 с.
19. Орйяван Г., Харпер А. Penetration Testing: A Hands-On Introduction to Hacking. — No Starch Press, 2014. — 528 p.
20. Энн М., Харпер А. Этичный хакинг и тестирование на проникновение. — М.: ДМК Пресс, 2020. — 456 с.
21. Олифер В.Г., Олифер Н.А. Компьютерные сети: принципы, технологии, протоколы. — 6-е изд. — М.: Питер, 2021. — 1104 с.
22. Таненбаум Э., Уэзеролл Д. Компьютерные сети. — 5-е изд. — М.: Питер, 2012. — 960 с.
23. OWASP Testing Guide v4.2. — Open Web Application Security Project, 2021. — URL: https://owasp.org/www-project-web-security-testing-guide/
24. Seitz J. Black Hat Python: Python Programming for Hackers and Pentesters. — 2nd ed. — No Starch Press, 2021. — 216 p.
25. Скотт С. Metasploit: руководство по тестированию на проникновение. — М.: ДМК Пресс, 2013. — 326 с.

5.2. Нормативно-правовые акты и стандарты

26. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм.).
27. ГОСТ Р ИСО/МЭК 27001-2021. Информационные технологии. Методы и средства обеспечения безопасности. — М.: Стандартинформ, 2021.

5.3. Методические материалы

28. Merion Academy. Методические материалы курса «Этичный хакинг». — М.: Merion Networks LLC, 2024. — Электронный ресурс: https://merionet.ru

5.4. Интернет-ресурсы

29. OWASP Foundation — https://owasp.org
30. Hack The Box — https://www.hackthebox.com
31. Exploit Database (Exploit-DB) — https://www.exploit-db.com
32. Merion Academy — https://merionet.ru
33. LMS-платформа курса — https://lms.merionet.ru