ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ АКАДЕМИЯ КИБЕРЁЖ

ООО "АКАДЕМИЯ КИБЕРЁЖ"

ОГРН: 1257700486702 ИНН: 7735212702 КПП: 773501001

Утверждаю
Генеральный директор

30 ноября 2025 г.

/ Денисенко Павел Андреевич

Дополнительная профессиональная программа повышения квалификации
«Active Directory. Пентест внутренней инфраструктуры»

Форма обучения: очная (с применением исключительно дистанционных образовательных технологий и электронного обучения)

Срок реализации: 20 недель (5. месяцев).

Режим занятий: 6,7. академических часов в неделю. Общая продолжительность: 20 недель (5. месяцев).

Объем программы: 134 академических часа

Авторы программы: Калинин Дмитрий, Патугин Евгений

г. Москва, 2026 г.

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1. Характеристики программы:

Дополнительная профессиональная программа повышения квалификации «**Active Directory. Пентест внутренней инфраструктуры**» (далее - Программа) разработана в соответствии стребованиями:

- Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказ Министерства образования и науки Российской Федерации от 1 декабря 2016 г. N 1515 - МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИКАЗ от 1 декабря 2016 г. N 1515 ОБ УТВЕРЖДЕНИИ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (УРОВЕНЬ БАКАЛАВРИАТА);
- Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей» (код 06.032) — утверждён Приказом Министерство труда и социальной защиты Российской Федерации РФ от 1 ноября 2016 г. № 598н;
- Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях» (код 06.030) — утверждён Приказом Минтруда РФ от 3 ноября 2016 г. № 608н;
- Профессиональный стандарт «Специалист по информационной безопасности в кредитно-финансовой сфере» — утверждён Приказом Минтруда РФ от 28 ноября 2022 г. № 739н (документ пока не полностью вступил в силу);
- Постановления Правительства Российской Федерации от 11.10.2023 № 1678 "Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ";
- с учетом требований приказа Минобрнауки РФ от 24.03.2025 N 266 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам".

1.2. Характеристика профессиональной деятельности слушателей: Основная цель вида профессиональной деятельности слушателей:

Программа ориентирована на совершенствование компетенций специалистов, чья профессиональная деятельность связана с обеспечением и оценкой защищённости корпоративных информационных систем, в первую очередь доменной инфраструктуры на базе Microsoft Active Directory, а также с выявлением уязвимостей, анализом рисков и разработкой мер защиты по результатам тестирования.

Профессиональная деятельность слушателей предполагает выполнение работ (в рамках согласованных и правомерных задач тестирования) по:

- анализу архитектуры доменной инфраструктуры и связанных сервисов;

- выявлению и оценке уязвимостей конфигураций, доменных политик и механизмов управления доступом;
- моделированию типовых и продвинутых сценариев атак на AD-инфраструктуру (разведка, первоначальный доступ, постэксплуатация, горизонтальное перемещение, атаки на Kerberos, ACL, ADCS, доверительные отношения);
- подготовке обоснованных рекомендаций по устранению выявленных уязвимостей и повышению уровня защищённости;
- документированию результатов тестирования и подготовке отчётов по стандартам OSSTMM, PTES, NIST 800-115.

Основная цель вида профессиональной деятельности слушателей: обеспечение и повышение уровня защищённости корпоративной доменной инфраструктуры Microsoft Active Directory путём проведения тестирования безопасности, выявления и анализа уязвимостей, моделирования сценариев компрометации и формирования приоритетных мер по их устранению, включая подготовку профессиональной отчётности по результатам проверки.

1.3. Категория слушателей: лица, имеющие среднее профессиональное и (или) высшее образование по направлению в области информационной безопасности; лица, получающие среднее профессиональное и (или) высшее образование по направлению в области информационной безопасности. Требования к слушателям: начинающие специалисты по информационной безопасности, системные администраторы, инженеры IT и DevOps, специалисты Red/Blue Team, интересующиеся безопасностью корпоративных сетей.

1.4. Объем программы (трудоемкость): общая трудоемкость 134 академических часов.

1.5. Срок освоения программы - 20 недель (5. месяцев).

1.6. Форма обучения: очная (с применением исключительно электронного обучения, дистанционных образовательных технологий).

1.7. Документ, выдаваемый после завершения обучения: по окончании обучения слушателям, выдается удостоверение о повышении квалификации установленного образца. Слушателям без оконченного высшего образования и (или) среднего профессионального образования удостоверение о повышении квалификации выдаётся одновременно с получением соответствующего документа об образовании и о квалификации.

2. ЦЕЛИ И ЗАДАЧИ ПРОГРАММЫ

2.1. Цель программы

Целью дополнительной профессиональной программы повышения квалификации «Active Directory. Пентест внутренней инфраструктуры» является формирование и совершенствование профессиональных компетенций слушателей в области тестирования безопасности доменной инфраструктуры Microsoft Active Directory, включая выявление и анализ уязвимостей, моделирование сценариев атак, проведение

постэксплуатационных действий в лабораторной среде и подготовку профессиональной отчётности по результатам тестирования в соответствии с подходами OSSTMM, PTES, NIST 800-115.

2.2. Задачи программы

Для достижения цели программы предусматривается решение следующих задач:

1. Сформировать системное понимание архитектуры и принципов функционирования Microsoft Active Directory и связанных сервисов, включая управление учётными записями, группами и групповыми политиками (GPO).
2. Обеспечить освоение практических навыков развёртывания базовой доменной инфраструктуры и оценки конфигурационных рисков и нарушений настроек безопасности.
3. Научить проводить разведку при тестировании безопасности доменной инфраструктуры, включая сбор информации по открытым источникам и активную разведку внешнего периметра, а также разведку внутри домена после компрометации.
4. Сформировать практические навыки получения первоначального доступа в рамках лабораторных сценариев и ведения доказательной базы действий.
5. Отработать методы постэксплуатации: локального повышения привилегий на узлах Windows, извлечения учётных данных (LSA/LSASS, DPAPI), обхода ограничений (в т.ч. UAC) и безопасного моделирования техник закрепления в системе.
6. Сформировать навыки горизонтального перемещения в сети и Pivoting, включая удалённое выполнение команд (PSRemoting/WinRM), использование SMB/PsExec, WMI, а также практику построения сетевых туннелей (SSH, Socat, Chisel, Ligolo, DNS-туннели).
7. Обучить выявлению и анализу уязвимостей и сценариев атак на механизмы аутентификации и делегирования Kerberos, включая техники Roasting, Pass-the-* и сценарии злоупотребления делегированием (неограниченное, ограниченное, RBCD).
8. Сформировать компетенции аудита и анализа прав доступа в домене Active Directory, включая поиск и эксплуатацию уязвимостей ACL (ошибочные ACE/ACL), оценку рисков и подготовку корректирующих мер.
9. Отработать понимание механизмов NTLM/NetNTLM и практические навыки моделирования Relay и Coerce-атак в контролируемой среде, а также разработку рекомендаций по снижению рисков.
10. Обеспечить освоение подходов к анализу инфраструктуры сертификации ADCS и практических сценариев атак на ADCS (ESC1–ESC16), включая аудит конфигураций и подготовку рекомендаций по усилению контроля.
11. Сформировать понимание доверительных отношений между доменами/лесами, методов их выявления и практических сценариев атак и передачи привилегий через междоменные связи, включая меры минимизации соответствующих угроз.
12. Систематизировать знания по часто встречающимся уязвимостям и типовым «низковисящим» сценариям компрометации (исторические CVE и распространённые векторы), с оценкой воздействия и выработкой мер предотвращения.

13. Сформировать навыки профессионального документирования результатов тестирования: структура отчёта, применение стандартов (OSSTMM, PTES, NIST 800-115), описание уязвимостей с учётом CVSS, подготовка рекомендаций для технической и управленческой аудитории, использование инструментов автоматизации отчётности (например, PwnDoc).
14. Подготовить слушателей к выполнению финального практического проекта, предусматривающего проведение полного цикла тестирования безопасности доменной инфраструктуры Active Directory в изолированной лабораторной среде — от разведки и получения доступа до анализа цепочек повышения привилегий и подготовки итогового отчёта с приоритизированными рекомендациями.

3. УЧЕБНЫЙ ПЛАН

№ п/п	Наменования модулей, тем, уроков	Всего, ауд. час.	Аудиторные учебные занятия		Внеауди т. сам. работа	Форма контроля	Трудоемкость
			Лекции	Практ. занятия			
1.1	**Введение, подготовка С2**	**1,18**	**0,18**	**1,00**	**0,00**	**-**	**1,18**
1.1.1	Инструкция по подключению к лаборатори	1,11	0,11	1,00	0,00	Практическое задание	1,11
1.1.2	Получение конфигурационного файла	0,07	0,07	0,00	0,00	Практическое задание	0,07
2.1	**2.1 Основы Active Directory**	**4,24**	**0,69**	**3,56**	**0,00**	**-**	**4,24**
2.1.1	2.1.1 Введение в Active Directory	0,89	0,33	0,56	0,00	Тест	0,89
2.1.2	2.1.2 Развертывание контроллера домена	1,09	0,09	1,00	0,00	Практическое задание	1,09
2.1.3	2.1.3 Управление пользователями и группами	1,13	0,13	1,00	0,00	Практическое задание	1,13
2.1.4	2.1.4 Групповые политики	0,13	0,13	0,00	0,00	-	0,13
2.1.	2.1.5 Создание и	1,00	0,00	1,00	0,00	Практич	1,00

5	настройка групповых политик					еское задание	
2.2	**2.2 Безопасность AD**	**4,60**	**0,60**	**4,00**	**1,33**	**-**	**5,93**
2.2.1	2.2.1 Ключевые моменты обеспечения безопасности AD	0,27	0,27	0,00	0,00	-	0,27
2.2.2	2.2.2 Настройка шаблонов безопасности	1,11	0,11	1,00	0,00	Практическое задание	1,11
2.2.3	2.2.3 Настройка политик безопасности через GPO	1,13	0,13	1,00	0,00	Практическое задание	1,13
2.2.4	2.2.4 Управление доступом через GPO	1,09	0,09	1,00	1,33	Практическое задание	2,42
2.2.5	2.2.5 Создание пользователей и групп, настройка GPO	1,00	0,00	1,00	0,00	Практическое задание	1,00
3.1	**3.1 Разведка и получение первоначального доступа**	**6,78**	**0,78**	**6,00**	**0,67**	**-**	**7,44**
3.1.1	3.1.1 Разведка при проведении пентеста	1,11	0,11	1,00	0,00	Практическое задание	1,11
3.1.2	3.1.2 Сбор информации о домене по открытым источникам	1,22	0,22	1,00	0,00	Практическое задание	1,22
3.1.3	3.1.3 Активная разведка внешнего периметра	1,24	0,24	1,00	0,00	Практическое задание	1,24
3.1.4	3.1.4 Получение первоначального доступа	1,13	0,13	1,00	0,00	Практическое задание	1,13
3.1.5	3.1.5 Сбор информации по внешним источникам, получение	2,07	0,07	2,00	0,67	Практическое задание	2,73

	перовначального доступа к домену						
3.2	**3.2 Разведка при постэксплуатации, разведка в домене**	**6,60**	**0,60**	**6,00**	**0,00**	**-**	**6,60**
3.2.1	3.2.1 Разведка в домене	1,20	0,20	1,00	0,00	Практическое задание	1,20
3.2.2	3.2.2 Локальная разведка на скомпрометированной машине	1,11	0,11	1,00	0,00	Практическое задание	1,11
3.2.3	3.2.3 Применение PowerView	1,09	0,09	1,00	0,00	Практическое задание	1,09
3.2.4	3.2.4 Применение BloodHound	1,13	0,13	1,00	0,00	Практическое задание	1,13
3.2.5	3.2.5 Разведка в домене	2,07	0,07	2,00	0,00	Практическое задание	2,07
4.1	**4.1 Локальное повышение привилегий**	**4,14**	**0,98**	**3,17**	**0,67**	**-**	**4,81**
4.1.1	4.1.1 Локальное повышение привилегий на узлах Windows	0,39	0,22	0,17	0,67	Практическое задание	1,06
4.1.2	4.1.2 Злоупотребление привилегиями пользователей	1,20	0,20	1,00	0,00	Практическое задание	1,20
4.1.3	4.1.3 Повышение привилегий за счет недостатков конфигураций	1,33	0,33	1,00	0,00	Практическое задание	1,33
4.1.4	4.1.4 DLL-Hijacking	1,22	0,22	1,00	0,00	Практическое задание	1,22
4.2	**4.2 Локальное повышение**	**6,14**	**0,98**	**5,17**	**0,67**	**-**	**6,81**

	привилегий часть 2, получение учетных данных						
4.2.1	4.2.1 Обход UAC	0,39	0,22	0,17	0,67	Практическое задание	1,06
4.2.2	4.2.2 Получение учетных данных	1,20	0,20	1,00	0,00	Практическое задание	1,20
4.2.3	4.2.3 LSA и LSASS, получение учетных данных	1,33	0,33	1,00	0,00	Практическое задание	1,33
4.2.4	4.2.4 DPAPI, получение учтеных данных	1,22	0,22	1,00	0,00	Практическое задание	1,22
4.2.5	4.2.5 Лабораторная работа по получению учетных данных	2,00	0,00	2,00	0,00	Практическое задание	2,00
4.3	**4.3 Закрепление в системе**	**6,14**	**0,98**	**5,17**	**0,67**	**-**	**6,81**
4.3.1	4.3.1 Методы закрепления в ОС Windows	0,39	0,22	0,17	0,67	Практическое задание	1,06
4.3.2	4.3.2 Закрепление через автозагрузку	1,20	0,20	1,00	0,00	Практическое задание	1,20
4.3.3	4.3.3 Закрепление через планировщик задач	1,33	0,33	1,00	0,00	Практическое задание	1,33
4.3.4	4.3.4 Закрепление через изменения реестра	1,22	0,22	1,00	0,00	Практическое задание	1,22
4.3.5	4.3.5 Итоговый кейс: закрепление в системе	2,00	0,00	2,00	0,00	Практическое задание	2,00
5.1	**5.1 Горизонтальное перемещение**	**6,14**	**0,98**	**5,17**	**0,67**	**-**	**6,81**
5.1.1	5.1.1 Методы и техники	0,39	0,22	0,17	0,67	Практическое	1,06

	горизонтального перемещения					задание	
5.1.2	5.1.2 Использование PSRemoting и WinRM для удаленного выполнения команд	1,20	0,20	1,00	0,00	Практическое задание	1,20
5.1.3	5.1.3 Протокол SMB для горизонтального перемещения, использование PsExec	1,33	0,33	1,00	0,00	Практическое задание	1,33
5.1.4	5.1.4 WMI для горизонтального перемещения	1,22	0,22	1,00	0,00	Практическое задание	1,22
5.1.5	5.1.5 Лабораторная работа по горизонтальному перемещению	2,00	0,00	2,00	0,00	Практическое задание	2,00
5.2	**5.2 Построение сетевых туннелей**	**6,14**	**0,98**	**5,17**	**0,67**	**-**	**6,81**
5.2.1	5.2.1 Построение сетевых туннелей	0,39	0,22	0,17	0,67	Практическое задание	1,06
5.2.2	5.2.2 SSH и Socat	1,20	0,20	1,00	0,00	Практическое задание	1,20
5.2.3	5.2.3 Chisel и Ligolo	1,33	0,33	1,00	0,00	Практическое задание	1,33
5.2.4	5.2.4 DNS-туннели	1,22	0,22	1,00	0,00	Практическое задание	1,22
5.2.5	5.2.5 Построение сетевых туннелей	2,00	0,00	2,00	0,00	Практическое задание	2,00
6.1	**6.1 Атаки на Kerberos**	**4,14**	**0,98**	**3,17**	**0,67**	**-**	**4,81**
6.1.1	6.1.1 Kerberos в AD	0,39	0,22	0,17	0,67	Практическое задание	1,06

6.1.2	6.1.2 Перебор пользователей, подбор паролей	1,20	0,20	1,00	0,00	Практическое задание	1,20
6.1.3	6.1.3 AS-REQ Roasting, AS-REP Roasting, Kerberoasting	1,33	0,33	1,00	0,00	Практическое задание	1,33
6.1.4	6.1.4 Pass-the-Key/Overpass-the-hash Pass-the-Ticket / Pass-the-Cache	1,22	0,22	1,00	0,00	Практическое задание	1,22
6.1.5	6.1.5 Классические атаки на Kerberos	2,00	0,00	2,00	0,00	Практическое задание	2,00
6.2	**6.2 Атаки на делегирование Kerberos**	**6,14**	**0,98**	**5,17**	**0,67**	**-**	**6,81**
6.2.1	6.2.1 Что такое делегирование Kerberos	0,39	0,22	0,17	0,67	Практическое задание	1,06
6.2.2	6.2.2 Неограниченное делегирование	1,20	0,20	1,00	0,00	Практическое задание	1,20
6.2.3	6.2.3 Ограниченное делегирование	1,33	0,33	1,00	0,00	Практическое задание	1,33
6.2.4	6.2.4 RBCD	1,22	0,22	1,00	0,00	Практическое задание	1,22
6.2.5	6.2.5 Атаки на делегирование	2,00	0,00	2,00	0,00	Практическое задание	2,00
7.1	**7.1 Уязвимости ACL**	**6,14**	**0,98**	**5,17**	**0,67**	**-**	**6,81**
7.1.1	7.1.1 Применение ACL в AD	0,39	0,22	0,17	0,67	Практическое задание	1,06
7.1.2	7.1.2 Поиск слабых ACL	1,20	0,20	1,00	0,00	Практическое задание	1,20

7.1.3	7.1.3 Эксплуатация уязвимостей ACL часть 1	1,33	0,33	1,00	0,00	Практическое задание	1,33
7.1.4	7.1.4 Эксплуатация уязвимостей ACL часть 2	1,22	0,22	1,00	0,00	Практическое задание	1,22
7.1.5	7.1.5 Атаки на ACL	2,00	0,00	2,00	0,00	Практическое задание	2,00
8.1	**8.1 Relay и Coerce атаки**	**6,14**	**0,98**	**5,17**	**0,67**	**-**	**6,81**
8.1.1	8.1.1 NetNTLM a AD	0,39	0,22	0,17	0,67	Практическое задание	1,06
8.1.2	8.1.2 NTLM-Relay часть 1	1,20	0,20	1,00	0,00	Практическое задание	1,20
8.1.3	8.1.3 NTLM-Relay часть 2	1,33	0,33	1,00	0,00	Практическое задание	1,33
8.1.4	8.1.4 Coerce-атаки	1,22	0,22	1,00	0,00	Практическое задание	1,22
8.1.5	8.1.5 Relay и Coerce атаки	2,00	0,00	2,00	0,00	Практическое задание	2,00
9.1	**9.1 Атаки на ADCS**	**6,14**	**0,98**	**5,17**	**0,67**	**-**	**6,81**
9.1.1	9.1.1 Центр сертификации ADCS	0,39	0,22	0,17	0,67	Практическое задание	1,06
9.1.2	9.1.2 ESC1-ESC5	1,20	0,20	1,00	0,00	Практическое задание	1,20
9.1.3	9.1.3 ESC6-ESC10	1,33	0,33	1,00	0,00	Практическое задание	1,33
9.1.4	9.1.4 ESC11-ESC16	1,22	0,22	1,00	0,00	Практическое задание	1,22

9.1.5	9.1.5 Атаки на ADCS	2,00	0,00	2,00	0,00	Практическое задание	2,00
10.1	**10.1.1 Доверительные отношения в домене**	**4,14**	**0,98**	**3,17**	**0,67**	**-**	**4,81**
10.1.1	10.1.2 Выявление доверительных отношений	0,39	0,22	0,17	0,67	Практическое задание	1,06
10.1.2	10.1.3 Эксплуатация уязвимостей доверительных отношений часть 1	1,20	0,20	1,00	0,00	Практическое задание	1,20
10.1.3	10.1.4 Эксплуатация уязвимостей доверительных отношений часть 2	1,33	0,33	1,00	0,00	Практическое задание	1,33
10.1.4	10.1.5 Атаки на доверительные отношения	1,22	0,22	1,00	0,00	Практическое задание	1,22
11.1	**11.1 «Низковисящие фрукты»**	**6,14**	**0,98**	**5,17**	**0,67**	**-**	**6,81**
11.1.1	11.1.1 Наиболее известные CVE в AD	0,39	0,22	0,17	0,67	Практическое задание	1,06
11.1.2	11.1.2 PrintNightMare, MS17-010, ZeroLogon	1,20	0,20	1,00	0,00	Практическое задание	1,20
11.1.3	11.1.3 NoPac	1,33	0,33	1,00	0,00	Практическое задание	1,33
11.1.4	11.1.4 PetitPotam	1,22	0,22	1,00	0,00	Практическое задание	1,22
11.1.5	11.1.5 Эксплуатация известных CVE	2,00	0,00	2,00	0,00	Практическое задание	2,00
12.1	**12.1 Постэксплуатация в домене**	**6,14**	**0,98**	**5,17**	**0,67**	**-**	**6,81**

12.1.1	12.1.1. Цели этапа пост эксплуатации	0,39	0,22	0,17	0,67	Практическое задание	1,06
12.1.2	12.1.2 Закрепление в домене: учетные записи, GPO	1,20	0,20	1,00	0,00	Практическое задание	1,20
12.1.3	12.1.3 Закрепление в домене: билеты Kerberos	1,33	0,33	1,00	0,00	Практическое задание	1,33
12.1.4	12.1.4 DCSync	1,22	0,22	1,00	0,00	Практическое задание	1,22
12.1.5	12.1.5 Постэксплуатация в домене	2,00	0,00	2,00	0,00	Практическое задание	2,00
13.1	**13.1 Основы документирования тестирования**	**7,37**	**1,20**	**6,17**	**0,67**	**-**	**8,03**
13.1.1	13.1.1 Зачем нужен отчет о пентесте и кому он предназначен, структура отчёта	0,39	0,22	0,17	0,67	Практическое задание	1,06
13.1.2	13.1.2 Стандарты: OSSTMM, PTES, NIST 800-115	1,20	0,20	1,00	0,00	Практическое задание	1,20
13.1.3	13.1.3 Документирование выявленных уязвимостей на основе CVSS	1,33	0,33	1,00	0,00	Практическое задание	1,33
13.1.4	13.1.4 Анализ примеров хороших и плохих отчетов, принципы написания четких и лаконичных рекомендаций	1,22	0,22	1,00	0,00	Практическое задание	1,22
13.1.5	13.1.5 Работа с PwnDoc: автоматизированная генерация отчетов	1,22	0,22	1,00	0,00	Практическое задание	1,22

13.1.6	13.1.6 Создание финального отчета по проведенному тестированию	2,00	0,00	2,00	0,00	Практическое задание	2,00
	Итоговый проект			13,33			13,33
	ИТОГО:	133,99 (134)	17,33	105,33	11,33		

4. СОДЕРЖАНИЕ УЧЕБНОГО ПЛАНА

Модуль 1: Введение
В этом модуле студенты получают общее представление о курсе, знакомятся с лабораторной средой, методами подключения к учебной инфраструктуре и конфигурацией инструментов. Отрабатывают правила безопасной работы в изолированной лаборатории и знакомятся с организационными и этическими аспектами проведения тестов.

Тема 1. Введение, подготовка С2
1.1.1 Инструкция по подключению к лаборатори
1.1.2 Получение конфигурационного файла

Итоговая практика:
Задание направлено на проверку навыков подготовки рабочего окружения: успешное подключение к учебной сети, получение и корректную загрузку конфигурационного файла, обеспечение безопасной работы в стенде и документирование настроек.

Модуль 2: Введение в Active Directory
В этом модуле студенты изучают архитектуру Active Directory, основные сервисы и принципы взаимодействия компонентов домена. Особое внимание уделяется ролям контроллеров домена, управлению учетными записями и принципам групповых политик.

Тема 1. Основы Active Directory
- 2.1.1 Введение в Active Directory
- 2.1.2 Развертывание контроллера домена
- 2.1.3 Управление пользователями и группами
- 2.1.4 Групповые политики
- 2.1.5 Создание и настройка групповых политик

Тема 2. Безопасность AD
- 2.2.1 Ключевые моменты обеспечения безопасности AD
- 2.2.2 Настройка шаблонов безопасности
- 2.2.3 Настройка политик безопасности через GPO
- 2.2.4 Управление доступом через GP
- 2.2.5 Создание пользователей и групп, настройка GPO

Итоговая практика:
Задание направлено на проверку умения моделировать базовую AD-инфраструктуру и оценивать её конфигурацию: развёртывание тестового контроллера, создание стандартных учетных записей и политик, анализ и документирование потенциальных конфигурационных рисков.

Модуль 3: Разведка и получение первоначального доступа
В этом модуле студенты изучают методы сбора информации о цели (исходная разведка), как с открытых источников, так и активными методами; учатся определять уязвимые точки внешнего периметра и моделировать сценарии первоначального доступа. Также рассматривается разведка внутри домена после компрометации.

Тема 1. Разведка и получение первоначального доступа
- 3.1.1 Разведка при проведении пентеста
- 3.1.2 Сбор информации о домене по открытым источникам
- 3.1.3 Активная разведка внешнего периметра
- 3.1.4 Получение первоначального доступа
- 3.1.5 Сбор информации по внешним источникам, получение перовначального доступа к домену

Тема 2. Разведка при постэксплуатации, разведка в домене
- 3.2.1 Разведка в домене
- 3.2.2 Локальная разведка на скомпрометированной машине
- 3.2.3 Применение PowerView
- 3.2.4 Применение BloodHound
- 3.2.5 Разведка в домене

Итоговая практика:
Задание направлено на отработку навыков систематического сбора и анализа информации: подготовка разведывательного отчёта по тестовому объекту, выявление критичных сервисов и учетных записей, формулировка возможных векторов первоначального доступа и документирование выводов.

Модуль 4: Постэксплуатация: локальное повышение привилегий получение учетных данных закрепление в системе
В этом модуле студенты изучают общие механизмы локального повышения привилегий, как конфигурационные слабости и злоупотребления прав позволяют получить расширенные доступы, а также методы устойчивого присутствия в системе. Рассматриваются ограничения и контрмеры.

Тема 1. Локальное повышение привилегий
- 4.1.1 Локальное повышение привилегий на узлах Windows
- 4.1.2 Злоупотребление привилегиями пользователей
- 4.1.3 Повышение привилегий за счет недостатков конфигураций
- 4.1.4 DLL-Hijacking

Тема 2. Локальное повышение привилегий. Часть 2. Получение учетных данных

- 4.2.1 Обход UAC
- 4.2.2 Получение учетных данных
- 4.2.3 LSA и LSASS, получение учетных данных
- 4.2.4 DPAPI, получение учтеных данных
- 4.2.5 Лабораторная работа по получению учетных данных

Тема 3. Закрепление в системе

- 4.3.1 Методы закрепления в ОС Windows
- 4.3.2 Закрепление через автозагрузку
- 4.3.3 Закрепление через планировщик задач
- 4.3.4 Закрепление через изменения реестра
- 4.3.5 Итоговый кейс: закрепление в системе

Итоговая практика:
Задание направлено на демонстрацию способности обнаруживать и использовать конфигурационные слабости для повышения привилегий и на безопасное моделирование техник закрепления в изолированной лаборатории с обязательной оценкой рисков и предложением мер защиты.

Модуль 5: Горизонтальное перемещение и Pivoting
В этом модуле студенты изучают методы перемещения внутри сети после получения доступа к узлу, способы удалённого выполнения команд и передачи управления между системами, а также практические подходы к обходу сетевых ограничений с помощью туннелирования.

Тема 1. Горизонтальное перемещение

- 5.1.1 Методы и техники горизонтального перемещения
- 5.1.2 Использование PSRemoting и WinRM для удаленного выполнения команд
- 5.1.3 Протокол SMB для горизонтального перемещения, использование PsExec
- 5.1.4 WMI для горизонтального перемещения
- 5.1.5 Лабораторная работа по горизонтальному перемещению

Тема 2. Построение сетевых туннелей

- 5.2.1 Построение сетевых туннелей
- 5.2.2 SSH и Socat
- 5.2.3 Chisel и Ligolo
- 5.2.4 DNS-туннели
- 5.2.5 Построение сетевых туннелей

Итоговая практика:
Задание направлено на отработку безопасных методов перемещения и связи: организация контролируемого горизонтального перемещения в стенде, настройка туннеля для обхода сетевых ограничений и документирование влияния на безопасность сети.

Модуль 6: Атаки на Kerberos

В этом модуле студенты изучают принципы аутентификации Kerberos в AD, уязвимости, связанные с билетами и делегированием, и современные техники атак на Kerberos. Разбираются принципы защиты и отчётности по подобным инцидентам.

Тема 1. Атаки на Kerberos

- 6.1.1 Kerberos в AD
- 6.1.2 Перебор пользователей, подбор паролей
- 6.1.3 AS-REQ Roasting, AS-REP Roasting, Kerberoasting
- 6.1.4 Pass-the-Key/Overpass-the-hash Pass-the-Ticket / Pass-the-Cache
- 6.1.5 Классические атаки на Kerberos

Тема 2. Атаки на делегирование Kerberos

- 6.2.1 Что такое делегирование Kerberos
- 6.2.2 Неограниченное делегирование
- 6.2.3 Ограниченное делегирование
- 6.2.4 RBCD
- 6.2.5 Атаки на делегирование

Итоговая практика:
Задание направлено на анализ конфигураций делегирования и Kerberos в тестовой среде: выявление рискованных настроек, моделирование сценариев компрометации на уровне билетов и формирование рекомендаций по смягчению рисков.

Модуль 7: Уязвимости ACL
В этом модуле студенты изучают роль ACL в контроле доступа Active Directory, методы поиска и анализа слабых ACL и подходы к оценке потенциала таких уязвимостей для эскалации прав.

Тема 1. Уязвимости ACL

- 7.1.1 Применение ACL в AD
- 7.1.2 Поиск слабых ACL
- 7.1.3 Эксплуатация уязвимостей ACL часть 1
- 7.1.4 Эксплуатация уязвимостей ACL часть 2
- 7.1.5 Атаки на ACL

Итоговая практика:
Задание направлено на проведение аудита прав доступа в тестовом домене: идентификация некорректных ACE/ACL, оценка риска их эксплуатации и разработка корректных политик и рекомендаций по исправлению.

Модуль 8: Relay и Coerce атаки
В этом модуле студенты получают представление о механизмах NTLM/NetNTLM, особенностях relay-атак и техниках принуждения аутентификации (coerce), а также изучают способы защиты от них.

Тема 1. Relay и Coerce атаки

- 8.1.1 NetNTLM a AD
- 8.1.2 NTLM-Relay часть 1

- 8.1.3 NTLM-Relay часть 2
- 8.1.4 Coerce-атаки
- 8.1.5 Relay и Coerce атаки

Итоговая практика:
Задание направлено на моделирование сценариев рискованной аутентификации в изолированной среде: обнаружение возможностей для relay/coerce-атак и формирование рекомендаций по защите и конфигурированию сервисов.

Модуль 9: Центр сертификации Active Directory
В этом модуле студенты изучают архитектуру ADCS, модель выдачи сертификатов и специфические векторы атак на инфраструктуру сертификации, а также методы её защиты.

Тема 1. Атаки на ADCS
- 9.1.1 Центр сертификации ADCS
- 9.1.2 ESC1-ESC5
- 9.1.3 ESC6-ESC10
- 9.1.4 ESC11-ESC16
- 9.1.5 Атаки на ADCS

Итоговая практика:
Задание направлено на аудит конфигурации ADCS в лабораторной среде: выявление рискованных шаблонов и ролей, оценка сценариев злоупотребления сертификатами и рекомендации по усилению контроля за выдачей сертификатов.

Модуль 10: Атаки на доверительные отношения в домене
В этом модуле студенты изучают концепцию доверительных отношений между доменами/лесами, способы их выявления и потенциальные векторы для передачи привилегий через междоменные связи.

Тема 1. Атаки на доверительные отношения
- 10.1.1 Доверительные отношения в домене
- 10.1.2 Выявление доверительных отношений
- 10.1.3 Эксплуатация уязвимостей доверительных отношений часть 1
- 10.1.4 Эксплуатация уязвимостей доверительных отношений часть 2
- 10.1.5 Атаки на доверительные отношения

Итоговая практика:
Задание направлено на анализ междоменных связей в тестовой инфраструктуре: выявление чрезмерных доверий, оценка риска и подготовку рекомендаций по минимизации угроз, связанных с доверительными отношениями.

Модуль 11: From Zero to Domain Admin. «Низковисящие фрукты»
В этом модуле студенты изучают часто встречающиеся слабости («низковисящие фрукты»), известные CVE и распространённые эксплойты, которые чаще всего приводят к быстрому повышению уровня доступа в домене.

Тема 1. «Низковисящие фрукты»

- 11.1.1 Наиболее известные CVE в AD
- 11.1.2 PrintNightMare, MS17-010, ZeroLogon
- 11.1.3 NoPac
- 11.1.4 PetitPotam
- 11.1.5 Эксплуатация известных CVE

Итоговая практика:
Задание направлено на систематизацию знаний по известным уязвимостям: проведение безопасного анализа риска по ряду исторических CVE, оценка воздействия и разработка практических рекомендаций по предотвращению повторной эксплойтации.

Модуль 12: Постэксплуатация и закрепление в домене
В этом модуле студенты обобщают методы постэксплуатации в масштабах домена: создание устойчивых точек доступа, работа с билетами Kerberos, техники эксфильтрации и способы минимизации следов присутствия.

Тема 1. Постэксплуатация в домене

- 12.1.1. Цели эатапа пост эксплуатации
- 12.1.2 Закрепление в домене: учетные записи, GPO
- 12.1.3 Закрепление в домене: билеты Kerberos
- 12.1.4 DCSync
- 12.1.5 Постэксплуатация в домене

Итоговая практика:
Задание направлено на комплексное моделирование постэксплуатационных сценариев в контролируемой среде: от создания устойчивого доступа до оценки последствий и выработки мер обнаружения и восстановления.

Модуль 13: Написание отчета
В этом модуле студенты осваивают принципы профессиональной документации результатов тестирования: структуру отчёта, стандарты, приоритизацию уязвимостей и формулирование понятных бизнесу рекомендаций.

Тема 1. Основы документирования тестирования

- 13.1.1 Зачем нужен отчет о пентесте и кому он предназначен, структура отчёта
- 13.1.2 Стандарты: OSSTMM, PTES, NIST 800-115
- 13.1.3 Документирование выявленных уязвимостей на основе CVSS
- 13.1.4 Анализ примеров хороших и плохих отчетов, принципы написания четких и лаконичных рекомендаций
- 13.1.5 Работа с PwnDoc: автоматизированная генерация отчетов
- 13.1.6 Создание финального отчета по проведенному тестированию

Итоговая практика:
Задание направлено на подготовку итогового отчёта по проведённому практическому аудиту: сбор доказательной базы, приоритизация находок, формулирование

рекомендаций для технической и управленческой аудитории, а также оформление презентации результатов.

Итоговый проект
Финальная практика — масштабная лабораторная работа, моделирующая реальный аудит безопасности корпоративного домена на базе Microsoft Active Directory. Проект объединяет все изученные модули: подготовку стенда, разведку (OSINT и активную), получение первоначального доступа, локальное и сетевое повышение привилегий, горизонтальное перемещение, атаки на Kerberos/ACL/ADCS/доверия, методы закрепления и пост-эксплуатации, а также подготовку профессионального отчёта. Работа выполняется в изолированной учебной среде под контролем преподавателя и имитирует заказ на пентест от «клиента».

Цель проекта:
отработать и продемонстрировать способность слушателя провести полный цикл тестирования безопасности доменной инфраструктуры: от сбора информации до подготовки обоснованных и приоритетных рекомендаций по устранению уязвимостей, при строгом соблюдении правил безопасности и этики пентестинга.

5. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Планируемые результаты обучения по дополнительной профессиональной программе повышения квалификации формируются через «совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации».

В результате освоения программы слушатели совершенствуют компетенции (без изменения нумерации), в том числе:

Общекультурные компетенции (ОК):

- «ОК-7 способностью к самоорганизации и самообразованию»
- «ОК-8 способностью использовать методы и средства выявления, идентификации и оценивания угроз безопасности информации, определения требований по защите информации»

Общепрофессиональные компетенции (ОПК):

- «ОПК-7 способностью определять виды и состав угроз информационной безопасности объекта»
- «ОПК-8 способностью разрабатывать модели угроз и нарушителя информационной безопасности объекта»
- «ОПК-9 способностью анализировать возможные последствия реализации угроз информационной безопасности объекта, рисков информационной безопасности»
- «ОПК-10 способностью применять методы и средства оценки уязвимостей объектов информатизации»

Профессиональные компетенции (ПК):

- «ПК-1 способностью собирать и проводить анализ исходных данных для проектирования систем защиты информации»
- «ПК-2 способностью разрабатывать и оформлять техническую документацию, связанную с профессиональной деятельностью»
- «ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты»
- «ПК-4 способностью устанавливать, настраивать и обслуживать технические и программно-аппаратные средства защиты информации»
- «ПК-5 способностью проводить мониторинг информационной безопасности средств и систем информатизации»
- «ПК-6 способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации»
- «ПК-7 способностью проводить аттестацию объекта информатизации по требованиям безопасности информации»
- «ПК-8 способностью оформлять необходимую техническую документацию, связанную с эксплуатацией системы защиты информации»
- «ПК-9 способностью осуществлять установку, настройку и эксплуатацию средств криптографической защиты информации»

Профессиональный стандарт (Приказ Минтруда России от 14.09.2022 № 533н)

Трудовая функция: «Проведение анализа безопасности компьютерных систем и сетей», код C/03.7.
Трудовые действия:

- «Оценка рисков, выявление и классификация уязвимостей компьютерных систем и сетей»
- «Подготовка аналитического отчета по результатам проведенного анализа безопасности компьютерных систем и сетей»
- «Формулирование предложений по устранению выявленных уязвимостей компьютерных систем и сетей»

Необходимые умения:

- «Прогнозировать возможные пути развития действий нарушителя в компьютерных системах и сетях»
- «Устанавливать причинно-следственные связи между действиями нарушителя и воздействием вредоносных программ на компьютерные системы и сети»
- «Моделировать и оценивать возможные вредоносные воздействия на компьютерные системы и сети»
- «Использовать регистрируемые события для выявления и классификации уязвимостей компьютерных систем и сетей»
- «Выполнять оценку рисков в компьютерных системах и сетях»

Трудовая функция: «Проведение инструментального мониторинга защищенности компьютерных систем и сетей», код C/05.7.
Трудовые действия:

- «Выполнение анализа защищенности компьютерных систем с использованием сканеров безопасности»
- «Выполнение анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей»
- «Составление отчетов по результатам проверок защищенности компьютерных систем»

Необходимые умения:

- «Формализовывать задачу управления безопасностью компьютерных систем»
- «Применять инструментальные средства проведения мониторинга защищенности компьютерных систем»
- «Применять методы анализа защищенности компьютерных систем и сетей»
- «Структурировать аналитическую информацию для включения в отчет»

Необходимые знания:

- «Принципы построения компьютерных систем и сетей»
- «Формальные модели безопасности компьютерных систем и сетей»
- «Принципы построения систем обнаружения компьютерных атак»
- «Методы обработки данных мониторинга безопасности компьютерных систем и сетей»
- «Порядок создания и структура отчета, создаваемого по результатам проверок»
- «Способы обнаружения и нейтрализации последствий вторжений в компьютерные системы»
- «Криптографические протоколы, применяемые в компьютерных сетях»
- «Нормативные правовые акты в области защиты информации»
- «Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры»
- «Организационные меры по защите информации»

Профессиональный стандарт (Приказ Минтруда России от 14.09.2022 № 525н)

Трудовая функция: «Тестирование автоматизированных систем и прикладного программного обеспечения на наличие уязвимостей», код C/01.7.
Трудовые действия:

- «Выявление угроз информационной безопасности автоматизированных систем и прикладного программного обеспечения»
- «Анализ возможных уязвимостей автоматизированных систем и прикладного программного обеспечения»
- «Подготовка отчета о выявленных угрозах информационной безопасности и возможных уязвимостях автоматизированных систем и прикладного программного обеспечения»

Необходимые умения:

- «Применять существующие методики выявления угроз информационной безопасности»
- «Классифицировать угрозы информационной безопасности»
- «Определять опасные значения параметров вычислительного процесса автоматизированных систем»
- «Составлять и оформлять аналитический отчет по выявленным угрозам и возможным уязвимостям автоматизированных систем и прикладного программного обеспечения»

Необходимые знания:

- «Нормативные правовые акты в области защиты информации»
- «Методики выявления угроз информационной безопасности»
- «Принципы построения автоматизированных систем и сетей»
- «Основные классы и типы атак на автоматизированные системы и прикладное программное обеспечение»
- «Основные методы и средства анализа уязвимостей автоматизированных систем и прикладного программного обеспечения»

Профессиональный стандарт (Приказ Минтруда России от 28.11.2022 № 739н)

Трудовая функция: «Реагирование на компьютерные инциденты», код B/04.7. Трудовые действия:

- «Определение приоритетов при реагировании на компьютерные инциденты»
- «Фиксация данных о компьютерных инцидентах»
- «Сбор и анализ информации о компьютерных инцидентах»
- «Определение причин и источников возникновения компьютерных инцидентов»
- «Разработка рекомендаций по устранению причин возникновения компьютерных инцидентов и недопущению их повторного возникновения»
- «Выполнение мероприятий по ликвидации последствий компьютерных инцидентов»

Необходимые умения:

- «Сопоставлять данные о компьютерных инцидентах»
- «Выявлять причинно-следственные связи по данным о компьютерных инцидентах»
- «Фиксировать данные о компьютерных инцидентах»
- «Разрабатывать рекомендации по реагированию на компьютерные инциденты»
- «Применять методы и инструменты анализа компьютерных инцидентов»

Необходимые знания:

- «Нормативные правовые акты в области информационной безопасности»
- «Методики и инструменты анализа компьютерных инцидентов»
- «Методы и средства выявления компьютерных атак»
- «Основные виды компьютерных атак и методы их реализации»
- «Технологии расследования компьютерных инцидентов»

6. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Обучение организуется согласно утвержденному календарному учебному графику, который формируется по мере набора учебной группы на соответствующий период обучения. Курс обучения не привязан к началу или окончанию учебного и календарного года. Прием заявок на курс происходит в течение всего календарного года. Календарный учебный график является примерным и утверждается отдельно для каждой учебной группы.

Срок освоения программы – 20 недель (5. месяцев) – 134 академ. часов. Начало обучения – по мере набора группы. Режим занятий – 6,7. академических часов в неделю. Общая продолжительность: 20 недель (5. месяцев). Для всех видов занятий академический час устанавливается продолжительностью 45 минут. Форма обучения – очная (с применением исключительно дистанционных образовательных технологий и электронного обучения).

Дата начала занятий	**Дата окончания занятий**	**Кол-во учебных недель**	**Кол-во учебных часов**	**Режим занятий**
По мере набора группы	По мере завершения обучения группы	20 недель (5. месяцев)	134	**6,7. академических часов в неделю. Общая продолжительность: 20 недель (5. месяцев).**[1]

7. ФОРМЫ АТТЕСТАЦИИ. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

7.1. Общие положения

Оценка качества освоения дополнительной профессиональной программы повышения квалификации «Active Directory. Пентест внутренней инфраструктуры» осуществляется для подтверждения достижения планируемых результатов обучения и сформированности профессиональных компетенций в области тестирования безопасности доменной инфраструктуры Microsoft Active Directory, выявления уязвимостей, моделирования атак, разработки рекомендаций по повышению защищенности, а также документирования результатов тестирования в соответствии с профессиональными стандартами (OSSTMM, PTES, NIST 800-115).

Оценка качества освоения Программы включает:

- текущий контроль по отдельным урокам и модулям;
- итоговую аттестацию в форме защиты финального проекта (итогового практического проекта).

[1]Для всех видов занятий академический час устанавливается продолжительностью 45 минут.

7.2. Формы текущего контроля

Текущий контроль осуществляется в течение всего периода обучения и проводится в формах, предусмотренных Программой:

- промежуточные тестирования после уроков;
- выполнение лабораторных и практических заданий по темам и модулям (в соответствии с учебно-тематическим планом);
- оценка практических результатов выполнения лабораторных и практических заданий, включая корректность выполненных действий, анализ рисков и качество документирования результатов теста.

Особое внимание при текущем контроле уделяется практическим результатам — корректности выполненных действий, анализу рисков и качеству документирования результатов теста. Выполнение лабораторных заданий предполагает получение обратной связи от эксперта или самопроверку по эталонному решению.

7.3. Итоговая аттестация

Итоговая аттестация проводится в форме защиты финального проекта (итогового практического проекта), представляющего собой масштабную лабораторную работу, моделирующую реальный аудит безопасности корпоративного домена на базе Microsoft Active Directory.

Финальный проект объединяет освоенные в рамках Программы модули и включает:

- подготовку стенда и организацию безопасной работы в изолированной учебной среде;
- разведку (OSINT и активную), выявление критичных сервисов и учетных записей, формирование возможных векторов первоначального доступа;
- получение первоначального доступа в тестовой среде;
- локальное и сетевое повышение привилегий, получение учетных данных;
- горизонтальное перемещение и Pivoting, построение туннелей в рамках стенда;
- моделирование атак на Kerberos, делегирование Kerberos, уязвимости ACL;
- моделирование Relay и Coerce-атак;
- аудит и моделирование атак на инфраструктуру сертификации Active Directory (ADCS);
- анализ и моделирование атак на доверительные отношения в домене;
- выполнение практик по наиболее распространенным слабостям и известным CVE в AD;
- постэксплуатацию и закрепление в домене в контролируемой среде;
- подготовку профессионального итогового отчета по проведенному тестированию.

Цель итогового проекта: отработать и продемонстрировать способность слушателя провести полный цикл тестирования безопасности доменной инфраструктуры — от сбора информации до подготовки обоснованных и приоритетных рекомендаций по устранению уязвимостей — при строгом соблюдении правил безопасности и этики пентестинга.

7.4. Критерии оценки качества освоения Программы

Оценка качества освоения Программы проводится по совокупности критериев, отражающих практическую применимость сформированных компетенций:

1. Корректность организации работы в лабораторной среде и соблюдение правил безопасной работы в изолированном стенде.
2. Логика и полнота выполнения этапов тестирования безопасности (последовательность работ, обоснованность выбранных действий и векторов).
3. Корректность выполнения практических действий в рамках лабораторных заданий и модулей Программы.
4. Обоснованность анализа рисков по выявленным уязвимостям и слабым конфигурациям.
5. Способность применять инструменты пентестинга и постэксплуатации, предусмотренные Программой (в лабораторной среде).
6. Полнота и качество фиксации результатов (доказательная база, описание шагов, найденные уязвимости, приоритизация, рекомендации).
7. Качество итогового отчета: структура, ясность формулировок, соответствие логике проведенного тестирования и требованиям стандартизированного документирования (OSSTMM, PTES, NIST 800-115).
8. Качество защиты финального проекта: обоснование решений, демонстрация результатов, аргументация выводов и предложенных мер по повышению защищенности.

7.5. Условия допуска к итоговой аттестации и выдачи удостоверения

К итоговой аттестации допускаются слушатели, которые:

- выполнили все лабораторные и практические задания, предусмотренные Программой;
- прошли промежуточные тестирования после уроков;
- подготовили материалы по практическим работам в составе, позволяющем оценить корректность выполненных действий, анализ рисков и качество документирования результатов.

Невыполнение хотя бы одного обязательного лабораторного или практического задания либо непрохождение предусмотренного тестирования образует академическую задолженность по Программе.

Удостоверение о повышении квалификации установленного образца выдается только при одновременном выполнении условий:

- отсутствие академической задолженности (выполнены все практические работы и тестирования, предусмотренные Программой);
- успешная защита финального проекта.

7.6. Фиксация результатов аттестации

Результаты текущего контроля и итоговой аттестации фиксируются в оценочных материалах Программы и подтверждаются материалами, предоставленными слушателем в рамках выполнения лабораторных и практических заданий, а также финального проекта.

Особое внимание уделяется практическим результатам — корректности выполненных действий, анализу рисков и качеству документирования результатов теста. Выполнение лабораторных заданий предполагает получение обратной связи от эксперта или самопроверку по эталонному решению.

8. ИТОГОВЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

По завершении дополнительной профессиональной программы повышения квалификации «Active Directory. Пентест внутренней инфраструктуры» слушатели будут готовы к практической работе в качестве специалистов по тестированию безопасности (Pentester), инженеров по защите Active Directory, специалистов Red Team / Blue Team, применяющих методы и инструменты оценки защищённости доменной инфраструктуры в корпоративных сетях.

Слушатели будут обладать следующими компетенциями:

- пониманием полного цикла тестирования безопасности доменной инфраструктуры Active Directory — от подготовки лабораторной среды и разведки до постэксплуатации и подготовки итогового отчёта;
- умением анализировать архитектуру и компоненты Active Directory, включая роли контроллеров домена, учетные записи, группы, политики и ключевые сервисы;
- навыками выявления и анализа уязвимостей конфигурации и доменных политик безопасности, включая управление доступом, GPO и настройки безопасности;
- способностью выполнять разведку (OSINT и активную) и формировать обоснованные гипотезы о возможных векторах первоначального доступа;
- умением моделировать сценарии первоначального доступа и выполнять разведку в домене после компрометации с применением PowerView и BloodHound;
- навыками локального повышения привилегий, получения учетных данных и применения техник постэксплуатации в контролируемой среде;
- умением выполнять горизонтальное перемещение в сети и применять техники Pivoting и туннелирования (в том числе PSRemoting/WinRM, SMB/PsExec, WMI, SSH/Socat, Chisel, Ligolo, DNS-туннели);
- навыками моделирования атак на Kerberos и делегирование Kerberos (AS-REQ/AS-REP Roasting, Kerberoasting, Pass-the-Ticket/Pass-the-Cache, RBCD и др.);
- способностью выявлять и оценивать уязвимости ACL и риски неправильно настроенных прав доступа в домене;
- умением анализировать и моделировать Relay и Coerce-атаки, понимать механизмы NetNTLM/NTLM-аутентификации и меры защиты;
- навыками аудита и оценки безопасности Active Directory Certificate Services (ADCS), включая сценарии ESC и формирование рекомендаций по усилению контроля выдачи сертификатов;

- умением выявлять и анализировать доверительные отношения между доменами/лесами и оценивать риски междоменных компрометаций;
- знанием распространённых уязвимостей и «низковисящих фруктов» в AD (включая PrintNightMare, MS17-010, ZeroLogon, NoPac, PetitPotam) и практических мер предотвращения повторной эксплуатации;
- умением документировать результаты тестирования и представлять выводы в форме профессионального отчёта, включая приоритизацию уязвимостей (на основе CVSS), доказательную базу и рекомендации, понятные технической и управленческой аудитории, в соответствии с OSSTMM, PTES, NIST 800-115.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Литература

- NIST SP 800-115 — Technical Guide to Information Security Testing and Assessment.
- PTES (Penetration Testing Execution Standard) — руководство по проведению пентестов.
- OSSTMM — методология оценки безопасности.
- MITRE ATT&CK — матрица поведения противника для моделирования атак.
- Mark E. Russinovich, David A. Solomon, Alex Ionescu — *Windows Internals* (разделы по безопасности и взаимодействию процессов/LSASS).

Дополнительная литература и руководства:

- Официальная документация Microsoft по Active Directory и ADCS (разделы по архитектуре, GPO и безопасности).
- Публикации и блоги экспертов по AD-безопасности (анкоры к специализированным статьям и анализам кейсов).
- Руководства по инструментам: BloodHound, PowerView, Mimikatz, Impacket — документация и практические мануалы.

Онлайн-ресурсы

- **Официальные ресурсы и стандарты:** Microsoft Docs (Active Directory, ADCS, GPO), NIST, MITRE.
- **Обучающие платформы и виртуальные лаборатории:** TryHackMe, Hack The Box, другие CTF/лаборатории для практики атак и защиты (использовать изолированные стенды).
- **Инструменты и репозитории:** GitHub-репозитории с утилитами (PowerView, BloodHound, Rubeus, Impacket и т.д.) — для изучения и тестирования в лаборатории.
- **Профессиональные сообщества и блоги:** блоги специалистов по AD-безопасности (обзоры CVE, разборы инцидентов), форумы и каналы с разбором практических кейсов.
- **Базы уязвимостей и CVE-трекеры:** NVD, CVE Details — для анализа известных проблем и мониторинга актуальных эксплойтов.

10. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Практические задания и кейсы

Подготовка среды и подключение

- Цель: уверенное развертывание и подключение к учебному стенду (AD, DC, клиентские узлы).

- Ожидаемый результат: рабочий профиль, документированная конфигурация, сохранённый конфиг C2.

Моделирование базовой AD-инфраструктуры и анализ конфигураций

- Цель: развёртывание контроллера домена, создание пользователей/GPO и оценка конфигурационных рисков.
- Ожидаемый результат: отчёт с уязвимыми настройками и предложениями исправления.

Разведка (OSINT и активная)

- Цель: собрать карту активов, сервисов и возможных векторов доступа.
- Ожидаемый результат: разведывательный отчёт с картой периметра и списком приоритетных целей.

Первоначальный доступ и локальное получение учетных данных

- Цель: безопасная отработка техник первоначального доступа и извлечения локальных учётных данных.
- Ожидаемый результат: журнал действий, доказательства успешных сценариев, рекомендации по защите.

Повышение привилегий и закрепление

- Цель: найти конфигурационные и программные векторы эскалации и отработать методы закрепления (в стенде).
- Ожидаемый результат: демонстрация цепочки привилегий, оценка риска, план устранения.

Горизонтальное перемещение и туннелирование

- Цель: реализовать контролируемое перемещение и настройку туннелей для обхода ограничений.
- Ожидаемый результат: отчёт о траектории движения, конфигурациях туннелей и рекомендациях.

Атаки на Kerberos, делегирование и ACL

- Цель: анализ и моделирование атак на Kerberos, оценка делегирования и прав доступа через ACL.
- Ожидаемый результат: выявленные уязвимости, сценарии эксплуатации и корректирующие меры.

ADCS/доверительные отношения/низковисящие фрукты

- Цель: оценить инфраструктуру сертификации, междоменные доверия и известные CVE.
- Ожидаемый результат: кейс-анализ по уязвимым элементам и рекомендации по конфигурации.

Итоговый практический проект (финальный кейс)

- Цель: провести полный цикл аудита тестовой доменной инфраструктуры и подготовить профессиональный отчёт.
- Ожидаемый результат: финальный отчёт, техническая карта угроз, бизнес-резюме, план корректирующих действий.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

- **Виртуализированная лаборатория** (желательно изолированная сеть): сервер виртуализации (ESXi/Proxmox/Hyper-V), возможность быстрого развёртывания шаблонов Windows Server и клиентских машин.
- **Образцы ОС и лицензии**: образы Windows Server (контроллеры домена), Windows Client, образы Kali или других тестовых дистрибутивов (использование trial/образов в учебных целях).

- **Стенд для C2/логирования**: отдельный сервер C2 (в учебной изоляции), система сбора логов и SIEM-эмулятор для отработки обнаружения.
- **Сетевое оборудование и сегментация**: виртуальные/физические коммутаторы с возможностью VLAN, NAT/маршрутизация для имитации внешнего периметра.
- **Инструменты и утилиты**: сборник инструментов для практик (PowerView, BloodHound, Mimikatz, Rubeus, Impacket, PsExec, Chisel/Socat и др.) — хранить на внутреннем репозитории.
- **Средства безопасности и мониторинга**: разделённый лабораторный SIEM/лог-сервер, инструменты для снятия дампов памяти (в учебных целях), антивирусы/EDR-эмуляция для кейсов обнаружения.
- **Средства резервного копирования**: шаблоны снимков/снэпшоты стендов для быстрого восстановления и повторного использования практик.
- **Инфраструктура доступа и управление пользователями**: система учётных записей преподавателей и студентов с разграничением прав в лаборатории.
- **Документация и каналы поддержки**: FAQ по развёртыванию стенда, чат/техническая поддержка для студентов во время практик.