



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
«Б1.В.09 ТЕХНОЛОГИЯ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ»**

Уровень высшего образования: бакалавриат

Направление подготовки: 10.03.01 Информационная безопасность

Направленность(профиль) подготовки: Организация и технология защиты информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 4 года

Объем:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Москва, 2024

Разработчики:

Преподаватель кафедры Информационно-измерительных систем
Сутягин Д. Д.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Минобрнауки от 17.11.2020 № 1427

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.12.2023, № 7-23

Содержание

1. Цель и задачи освоения дисциплины (модуля)
2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы
3. Место дисциплины в структуре ОП
4. Объем дисциплины и виды учебной работы
5. Содержание дисциплины
 - 5.1. Разделы, темы дисциплины и виды занятий
 - 5.2. Содержание разделов, тем дисциплины и формы текущего контроля
6. Оценочные материалы текущего контроля
7. Оценочные материалы промежуточной аттестации
8. Порядок проведения промежуточной аттестации
9. Материально-техническое и учебно-методическое обеспечение дисциплины
 - 9.1. Перечень основной и дополнительной учебной литературы
 - 9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся
 - 9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине
 - 9.4. Оборудование и технические средства обучения
10. Методические указания по освоению дисциплины (модуля)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - приобретение обучающимися знаний в области методологии, правовых основ и практических аспектов проведения тестирования на проникновение, а также формирование способности выявлять и использовать уязвимости автоматизированных систем для оценки реального уровня их защищенности.

Задачи изучения дисциплины:

- изучение нормативно-правовой базы, этических норм и стандартов, регламентирующих проведение работ по тестированию на проникновение;
- формирование у обучающихся системного понимания этапов проведения пентеста: от сбора информации и моделирования угроз до пост-эксплуатации и подготовки отчетной документации;
- приобретение практических навыков работы с современным программным обеспечением и инструментальными средствами для сканирования сети, анализа трафика и эксплуатации уязвимостей;
- освоение методов анализа защищенности веб-приложений, сетевой инфраструктуры и операционных систем, включая поиск типовых ошибок конфигурации и ошибок кода.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-3 Способен проводить анализ уязвимостей внедряемой системы защиты информации

ПК-3.1 Выполняет оценку информационных рисков

Знать:

ПК-3.1/Зн1 Методологии и стандарты оценки рисков информационной безопасности, этапы идентификации активов, угроз и уязвимостей, а также качественные и количественные методы расчета уровня риска для обоснования выбора мер защиты на этапе проектирования СЗИ

ПК-3.1/Зн2 Классификацию угроз информационной безопасности и уязвимостей автоматизированных систем

Уметь:

ПК-3.1/Ум1 Идентифицировать критичные активы и актуальные угрозы, применять методики расчета рисков и интерпретировать полученные результаты для определения приоритетов внедрения средств защиты

ПК-3.1/Ум2 Рассчитывать уровень риска для различных сценариев атак на основе данных, полученных в ходе пентеста

Владеть:

ПК-3.1/Нв2 Навыками использования специализированных шкал и калькуляторов для приведения технических характеристик уязвимости к показателям уровня риска

ПК-3.2 Проводит экспертизу состояния защищенности автоматизированных систем и применяемых средств защиты информации

Знать:

ПК-3.2/Зн1 Нормативные требования к защите информации, типовые уязвимости компонентов автоматизированных систем, а также методы и инструменты проведения анализа защищенности

ПК-3.2/Зн2 Методы и этапы проведения тестирования на проникновение

Уметь:

ПК-3.2/Ум2 Планировать и организовывать проведение тестирования на проникновение для оценки реального уровня защищенности АС

Владеть:

ПК-3.2/Нв2 Методиками проведения различных видов тестирования на проникновение

ПК-3.2/Нв3 Навыками работы с современными инструментальными средствами пентеста

ПК-3.2/Нв4 Техниками выявления и эксплуатации уязвимостей веб-приложений, сетевых протоколов, операционных систем и СУБД

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.В.09 «Технология проведения тестирования на проникновение» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 8.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
8 семестр	108	3	45	63	Зачет с оценкой
Всего	108	3	45	63	

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотношенные с результатами освоения программы
Раздел 1. Организационно-правовая подготовка и планирование работ	17	6	11	ПК-3.1

Тема 1.1. Нормативно-правовые и этические аспекты пентеста	7	2	5	ПК-3.1 ПК-3.2
Тема 1.2. Планирование и методология тестирования	10	4	6	
Раздел 2. Разведка и инвентаризация цели перед проведением пентеста	30	13	17	
Тема 2.1. Пассивная разведка (OSINT) и сбор информации	16	7	9	
Тема 2.2. Активное сканирование и обнаружение активов	14	6	8	
Раздел 3. Эксплуатация уязвимостей и пост-эксплуатация	40	18	22	ПК-3.2
Тема 3.1. Эксплуатация уязвимостей приложений и сервисов	22	10	12	
Тема 3.2. Пост-эксплуатация и закрепление в системе	18	8	10	
Раздел 4. Анализ результатов проведения пентеста и формирование отчета для заказчика	21	8	13	ПК-3.2
Тема 4.1. Документирование результатов и оценка рисков	12	5	7	
Тема 4.2. Разработка рекомендаций и повторное тестирование	9	3	6	
Итого	108	45	63	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Организационно-правовая подготовка и планирование работ

Тема 1.1. Нормативно-правовые и этические аспекты пентеста

Законодательство РФ в области информационной безопасности (УК РФ, КоАП, ФЗ «О персональных данных»), ответственность за неправомерный доступ, понятие этичного хакинга, стандарты и методики, договор на проведение работ, соглашение о неразглашении (NDA), определение границ и правил взаимодействия.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 1.2. Планирование и методология тестирования

Этапы проведения тестирования на проникновение, выбор подхода (black box, white box, grey box), сбор вводных данных, формирование технического задания, определение целей и объема тестирования, планирование временных ресурсов, выбор инструментария, техника безопасности при проведении активных тестов.

Текущий контроль
Вид (форма) контроля
Тестирование

Раздел 2. Разведка и инвентаризация цели перед проведением пентеста

Тема 2.1. Пассивная разведка (OSINT) и сбор информации

Методы сбора данных из открытых источников, поиск поддоменов и связанных ресурсов, анализ DNS-записей, использование поисковых систем, сбор адресов электронной почты, утечки данных, анализ метаданных документов.

Текущий контроль
Вид (форма) контроля
Тестирование

Тема 2.2. Активное сканирование и обнаружение активов

Техники сканирования портов, идентификация сервисов и их версий, использование Nmap, определение операционных систем, построение сетевой карты, анализ топологии сети, сканирование уязвимостей с помощью Nessus, интерпретация результатов сканирования, верификация обнаруженных сервисов.

Текущий контроль
Вид (форма) контроля
Тестирование

Раздел 3. Эксплуатация уязвимостей и пост-эксплуатация

Тема 3.1. Эксплуатация уязвимостей приложений и сервисов

Поиск и использование эксплойтов, эксплуатация уязвимостей веб-приложений (SQL-инъекции, XSS, LFI/RFI, CSRF, SSRF), применение Burp Suite, SQLmap, атаки на механизмы аутентификации, подбор учетных данных (Hydra), анализ защищенности API.

Текущий контроль
Вид (форма) контроля
Тестирование

Тема 3.2. Пост-эксплуатация и закрепление в системе

Повышение привилегий, дампы паролей и хешей, сбор конфиденциальной информации, создание бэкдоров и закрепление доступа, сокрытие следов (очистка логов), организация туннелирования и проксирования трафика, передача данных наружу, анализ защищенности внутренних ресурсов.

Текущий контроль
Вид (форма) контроля
Тестирование

Раздел 4. Анализ результатов проведения пентеста и формирование отчета для заказчика

Тема 4.1. Документирование результатов и оценка рисков

Структура итогового отчета, описание методологии и объема работ, перечень выявленных уязвимостей, доказательная база (скриншоты, логи, видео), ранжирование уязвимостей по степени критичности (CVSS), оценка рисков, соотнесение с бизнес-процессами, формирование выводов.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 4.2. Разработка рекомендаций и повторное тестирование

Подготовка практических рекомендаций по устранению уязвимостей, приоритизация мер защиты, планирование повторного тестирования (ретеста), подготовка презентации для руководства, защита результатов заказчику, обсуждение ограничений проведенного тестирования и дальнейших шагов.

Текущий контроль

Вид (форма) контроля
Тестирование

6. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Зачет с оценкой, 8 семестр.

Зачет оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний при анализе практических вопросов;
- зачтено с оценкой «хорошо» выставляется обучающемуся в случае соблюдения тех же требований, но наличия в ответе обучающегося по некоторым перечисленным показателям недостатков принципиального характера, что вызывает замечания или поправки преподавателя;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся в случае соблюдения тех же требований, но в случае наличия в ответе ошибок, необходимости существенной помощи в виде поправок и наводящих вопросов преподавателя;
- не зачтено («не удовлетворительно») – обучающийся не смог ответить на 2/3 вопросов; не

справился с практическим заданием или выполнено менее 50 % практических заданий.

7. Оценочные материалы текущего контроля

Раздел 1. Организационно-правовая подготовка и планирование работ

Контролируемые ИДК: ПК-3.1

Тема 1.1. Нормативно-правовые и этические аспекты пентеста

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие статьи Уголовного кодекса РФ могут быть применены к лицу, проводящему тестирование на проникновение без соответствующего договора и согласия владельца системы?
2. Что такое «правила взаимодействия» в контексте пентеста и какие параметры они обязательно должны фиксировать?
3. В чём различие между понятиями «этичный хакер» (white hat) и «неэтичный хакер» (black hat) с правовой и профессиональной точек зрения?
4. Какова роль соглашения о неразглашении (NDA) при подготовке к проведению пентеста?

Тема 1.2. Планирование и методология тестирования

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Перечислите основные этапы тестирования на проникновение согласно методологии PTES.
2. Чем отличаются подходы «чёрного ящика» (black box), «белого ящика» (white box) и «серого ящика» (grey box) при тестировании на проникновение?
3. Какие разделы должно содержать техническое задание на проведение тестирования на проникновение?
4. Что такое «ложное срабатывание» (false positive) и почему важно его учитывать при планировании анализа уязвимостей?

Раздел 2. Разведка и инвентаризация цели перед проведением пентеста

Контролируемые ИДК: ПК-3.1 ПК-3.2

Тема 2.1. Пассивная разведка (OSINT) и сбор информации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие данные можно получить с помощью Google Hacking и приведите 2-3 примера таких операторов.
2. Для чего используется сервис Shodan в ходе пассивной разведки и какую информацию он предоставляет?
3. Что такое DNS-разведка и какие типы записей DNS представляют наибольший интерес для пентестера?
4. Какие инструменты из состава Kali Linux можно использовать для пассивного сбора информации о сотрудниках и электронной почте организации?

Тема 2.2. Активное сканирование и обнаружение активов

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. С какой целью применяется сканирование UDP-портов и в чём его сложность по сравнению со сканированием TCP-портов?
2. Объясните принцип работы NSE-скриптов и приведите примеры задач, решаемых с их помощью.
3. Что такое идентификация операционной системы (OS fingerprinting) и на каких принципах она основана?
4. Какие риски для целевой системы несёт активное сканирование с агрессивными настройками?

Раздел 3. Эксплуатация уязвимостей и пост-эксплуатация

Контролируемые ИДК: ПК-3.2

Тема 3.1. Эксплуатация уязвимостей приложений и сервисов

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. В чём суть SQL-инъекции и какие типы данных можно извлечь при её успешной реализации?
2. Опишите принцип работы межсайтового скриптинга (XSS) и назовите основные типы XSS-атак.
3. Для чего предназначен инструмент Burp Suite и перечислите его основные модули, используемые при тестировании веб-приложений.
4. Что такое подбор учётных данных (brute-force) и какие методы защиты от него существуют?
5. Какие типы уязвимостей веб-приложений входят в категорию OWASP Top 10 (назовите 3-4 примера)?

Тема 3.2. Пост-эксплуатация и закрепление в системе

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое повышение привилегий (privilege escalation) и какие два основных типа повышения привилегий существуют?
2. Какую полезную информацию можно извлечь из оперативной памяти (дамп памяти) взломанной системы с помощью инструментов типа Mimikatz?
3. Для чего пентестер создаёт бэкдор в скомпрометированной системе? Какие методы маскировки бэкдоров используются?
4. Что такое туннелирование трафика и в каких случаях оно применяется на этапе пост-эксплуатации?
5. Какие действия входят в этап «сокрытие следов» и почему это важно для качественного пентеста?

Раздел 4. Анализ результатов проведения пентеста и формирование отчета для заказчика

Контролируемые ИДК: ПК-3.2

Тема 4.1. Документирование результатов и оценка рисков

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Назовите обязательные разделы итогового отчёта о тестировании на проникновение.
2. Что такое вектор CVSS и для чего он используется при подготовке отчёта?
3. Как связаны результаты пентеста с оценкой информационных рисков? Приведите пример.

Тема 4.2. Разработка рекомендаций и повторное тестирование

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие типы рекомендаций должны быть предложены заказчику по итогам пентеста и чем различаются технические и организационные рекомендации?

8. Оценочные материалы промежуточной аттестации

8 семестр, Зачет с оценкой

Контролируемые ИДК: ПК-3.1 ПК-3.2

Вопросы/Задания:

1. Юридические и этические границы тестирования на проникновение
2. Методологии проведения пентеста
3. Проблема ложных срабатываний и ложных отрицаний при автоматическом сканировании уязвимостей
4. Техники пассивной разведки
5. Google Hacking как метод сбора информации
6. DNS-разведка и её роль в построении карты сети
7. Сравнение методов активного сканирования
8. Идентификация сервисов и операционных систем
9. Сканеры уязвимостей против ручного тестирования
10. SQL-инъекции
11. Межсайтовый скриптинг (XSS)
12. Уязвимости контроля доступа
13. Эксплуатация уязвимостей веб-приложений с использованием Burp Suite
14. Подбор учётных данных (brute-force)
15. Методология OWASP Top 10
16. Использование Metasploit Framework в пентесте
17. Повышение привилегий в ОС семейства Windows
18. Повышение привилегий в ОС семейства Linux

19. Инструменты и техники пост-эксплуатации
20. Способы закрепления в системе
21. Туннелирование и обход сетевых ограничений
22. Обнаружение и обход систем защиты в процессе пентеста
23. Соккрытие следов присутствия
24. Моделирование угроз и построение профиля нарушителя как связующее звено между разведкой и эксплуатацией
25. Составление отчёта по результатам пентеста
26. Методика расчёта критичности уязвимостей по стандарту CVSS
27. Интеграция результатов тестирования на проникновение в процесс управления рисками
28. Разработка практических рекомендаций после пентеста
29. Повторное тестирование как элемент верификации устранения уязвимостей
30. Современные вызовы пентеста

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Основы тестирования КИИ на проникновение: учебное пособие: учебное пособие / А. И. Елисеев, Д. В. Поляков, В. В. Севенюк, К. В. Стародубов. - Основы тестирования КИИ на проникновение - Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2019. - 84 с. - 978-5-8265-2090-1. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/99777.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Белоус А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. - Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения - Москва: Техносфера, 2021. - 482 с. - 978-5-94836-612-8. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/108023.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Баланов А. Н. Кибербезопасность: учебное пособие для вузов: учебное пособие для вузов / А. Н. Баланов. - Санкт-Петербург: Лань, 2024. - 680 с. - 978-5-507-49562-7. - Текст: электронный. // Издательство Лань: [сайт]. - URL: <https://e.lanbook.com/img/cover/book/422558.jpg> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Баланов А. Н. Защита информационных систем. Кибербезопасность: учебное пособие для вузов: учебное пособие для вузов / А. Н. Баланов. - 2-е изд., стер. - Санкт-Петербург: Лань, 2025. - 280 с. - 978-5-507-50467-1. - Текст: электронный. // Издательство Лань: [сайт]. - URL: <https://e.lanbook.com/img/cover/book/438971.jpg> (дата обращения: 16.03.2025). - Режим доступа: по подписке

9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

Не используются.

Ресурсы «Интернет»

1. <https://www.iprbookshop.ru/> - IPR BOOKS
2. <https://e.lanbook.com/> - Электронная библиотечная система "Лань"
3. <https://rusneb.ru/> - Национальная электронная библиотека (НЭБ)
4. <https://znanium.ru/> - Электронно-библиотечная система "Znanium"
5. <https://www.elibrary.ru/> - НЭБ eLIBRARY
6. <https://intuit.ru/> - Электронная образовательная среда "ИНТУИТ"

9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения

(обновление производится по мере появления новых версий программы)

Не используется.

Перечень информационно-справочных систем

(обновление выполняется еженедельно)

Не используется.

9.4. Оборудование и технические средства обучения

Компьютерный класс

Маркерная доска - 0 шт.

Моноблок - 64 шт.

Проектор - 4 шт.

10. Методические указания по освоению дисциплины (модуля)

С целью успешного освоения данного предмета студенту необходимо выполнять домашние работы по указанным преподавателям темам и представленным на занятиях материалам. Для более успешного выполнения работы студенту предлагается использование учебно-методических материалов, соответствующих указанной теме.

Самостоятельная работа студентов описывается и регулируется методическими рекомендациями по дисциплине.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной

информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.