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: 5BFEE1D286E9C95A0C0D2C611E434BD5
Владелец: Степанченко Алексей Леонидович
Действителен: с 23.09.2026 по 17.12.2027

«УТВЕРЖДАЮ»
Проректор
А. Л. Степанченко
15 мая 2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ) «Б1.В.04 ИНСТРУМЕНТЫ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ»

Уровень высшего образования: магистратура

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль) подготовки: Защита информации в геоинформационных системах и системах сбора пространственных данных

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Год набора (приема на обучение): 2026

Срок получения образования: 2 года

Объем: в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Москва, 2026

Разработчики:

Старший преподаватель кафедры
Информационно-измерительных систем Сутягин Д. Д.

Преподаватель кафедры Информационно-измерительных систем
Ширинкин С. Г.

Фонд оценочных средств по дисциплине (модулю) составлен в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки от 26.11.2020 № 1455

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	05.11.2025, № 12-25

1. Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения образовательной программы

ПК-2 Способен проводить анализ безопасности компьютерных систем (включая выполнение научно-исследовательских работ по этой тематике)

ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности

Знать:

ПК-2.1/Зн1 Способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности

ПК-2.1/Зн2 Основные нормативные документы в области анализа безопасности компьютерных систем

Уметь:

ПК-2.1/Ум2 Оценивать реальный уровень защищенности анализируемых компьютерных систем

Владеть:

ПК-2.1/Нв1 Навыками подготовки аналитического отчета по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах

ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных

Знать:

ПК-2.2/Зн2 Основные методы реализации угроз безопасности информации и способы их предотвращения

ПК-2.2/Зн3 Классы инструментов тестирования на про-никновения, принципы их действия

Уметь:

ПК-2.2/Ум2 Выбирать инструменты тестирования на проникновение под конкретные условия при анализе безопасности компьютерных систем

Владеть:

ПК-2.2/Нв1 Навыками анализа программно-аппаратных средств защиты с целью определения уровня обеспечиваемых ими защищенности и доверия

ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах

Знать:

ПК-2.3/Зн1 Методы и инструменты оценки уровня защищенности

Уметь:

ПК-2.3/Ум1 Подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах

Владеть:

ПК-2.3/Нв1 Навыками работы с инструментами анализа защищенности

ПК-2.3/Нв2 Навыками анализа журналов событий и других источников информации о состоянии компьютерной системы

2. Показатели и критерии оценивания компетенций

Планируемые результаты освоения программы	Уровень овладения	Критерии оценивания (перечень сформированных ИДК/ЗУВ по уровням освоения)
ПК-2 Способен проводить анализ безопасности компьютерных систем (включая выполнение научно-исследовательских работ по этой тематике)	Повышенный	ИДК ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности Знать: ПК-2.1/Зн1 Способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности ПК-2.1/Зн2 Основные нормативные документы в области анализа безопасности компьютерных систем

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
Отлично	ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности ПК-2.1/Зн1 Способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности ПК-2.1/Зн2 Основные нормативные документы в области анализа безопасности компьютерных систем
Неудовле-творительно	Результаты обучения не сформированы на достаточном уровне
Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
Не зачтено	Результаты обучения не сформированы на достаточном уровне

4. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Практическая работа Тестирование
Промежуточная аттестация	Зачет Зачет с оценкой

№ п/п	Наименование раздела	Контролируемые ИДК	Вид контроля/ используемые оценочные материалы	
			Текущий	Промежут. аттестация
1	Инструменты сбора информации о системах и сетях	ПК-2.3	Практическая работа Тестирование	Зачет Зачет с оценкой
2	Инструменты эксплуатации систем и сетей	ПК-2.2	Практическая работа Тестирование	Зачет Зачет с оценкой

3	Инструменты закрепления в системе и сети	ПК-2.2	Практическая работа Тестирование	Зачет Зачет с оценкой
4	Инструменты эксфильтрации данных	ПК-2.2	Практическая работа Тестирование	Зачет Зачет с оценкой
5	Применение инструментов тестирования на проникновение в лабораторных условиях	ПК-2.1	Практическая работа Тестирование	Зачет Зачет с оценкой

5. 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, 3 семестр.

Промежуточная аттестация по дисциплине проводится в форме зачета. Она может быть организована как компьютерное тестирование либо как устное собеседование по билетам. Билет включает два теоретических вопроса и одно простое практическое задание. Конкретная форма утверждается кафедрой и доводится до обучающихся в установленный срок.

Критерии оценивания при проведении промежуточной аттестации в форме компьютерного тестирования:

Зачет оценивается по двухбалльной шкале («зачтено/не зачтено»):

- зачтено выставляется, если обучающийся набрал 60–100 %; достигнут необходимый уровень: основные понятия поняты, типовая задача решена корректно и с учетом установленных ограничений;
- не зачтено выставляется, если обучающийся набрал 0–59 %; не достигнут необходимый уровень: имеются принципиальные ошибки в понятиях, последовательности действий или обосновании решения.

Критерии оценивания при проведении промежуточной аттестации в форме устного собеседования по билетам:

Зачет оценивается по двухбалльной шкале («зачтено/не зачтено»):

- зачтено выставляется, если ответ раскрывает основные положения вопросов билета; термины применены корректно, практическая задача решена допустимым способом, существенные ошибки отсутствуют;
- не зачтено выставляется, если ответ отсутствует либо содержит принципиальные ошибки; не раскрыты основные понятия, практическая задача не решена или предложено недопустимое действие.

Промежуточная аттестация: Зачет с оценкой, 4 семестр.

Промежуточная аттестация по дисциплине проводится в форме «дифференцированный зачет».

Конкретная форма проведения — компьютерное тестирование по теоретическому материалу или устное собеседование по вопросам билетов — утверждается кафедрой и доводится до сведения обучающихся не позднее чем за месяц до начала промежуточной аттестации. При компьютерном тестировании итоговый результат определяется как отношение количества набранных баллов к максимально возможному количеству баллов. При устном собеседовании билет включает вопросы из перечня вопросов; преподаватель вправе задать дополнительные и уточняющие вопросы.

Критерии оценивания при проведении промежуточной аттестации в форме компьютерного тестирования:
Зачет оценивается по пятибалльной шкале:
- зачтено с оценкой «отлично» выставляется, если обучающийся набрал 86–100 баллов и продемонстрировал системное и полное освоение содержания дисциплины; ответы правильные, обоснованные и терминологически точные;
- зачтено с оценкой «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, в случае, если основное содержание освоено, но допущены отдельные неточности, не влияющие на общее понимание материала;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если освоены базовые понятия и положения, но имеются существенные пробелы и ошибки;
- не зачтено («не удовлетворительно») – если обучающийся набрал 0–55 баллов, не освоен необходимый минимум содержания дисциплины; результаты обучения не достигнуты.

Критерии оценивания при проведении промежуточной аттестации в форме устного собеседования по билетам:
Зачет оценивается по пятибалльной шкале:
- зачтено с оценкой «отлично» выставляется, если обучающийся набрал 86–100 баллов и дал полные, правильные и логически последовательные ответы; терминология применяется корректно, приведены необходимые обоснования и примеры, дополнительные вопросы раскрыты;
- зачтено с оценкой «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, если вопросы раскрыты правильно и достаточно полно, а отдельные неточности исправлены после уточняющих вопросов;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если основные положения раскрыты фрагментарно, имеются существенные неточности, однако базовое понимание продемонстрировано;
- не зачтено («не удовлетворительно») – если обучающийся набрал 0–55 баллов, вопросы не раскрыты либо допущены принципиальные ошибки, отсутствует владение базовой терминологией.

6. Оценочные материалы текущего контроля

Раздел 1. Инструменты сбора информации о системах и сетях
Контролируемые ИДК: ПК-2.3

Тема 1.1. Инструменты сбора информации о системах и сетях

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Проверка открытых сведений об учебной организации

Собрать из подготовленного преподавателем открытого набора сведения о сервисах и программных продуктах учебной организации. Для каждого утверждения указать источник, дату, степень подтвержденности и сведения, которых не хватает для вывода

2. Сопоставление пассивного и активного наблюдения

По учебному PCAP выделить узлы и соединения, затем сравнить их с результатом ограниченной проверки разрешенного виртуального сегмента. Объяснить различия с учетом времени, точки наблюдения, фильтрации и настроек средств

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как расшифровывается OSINT по смыслу источников данных?

2. Удаляет ли фильтр отображения Wireshark неподходящие пакеты из уже открытого файла захвата?

3. Какой транспортный протокол устанавливает соединение перед обычной передачей прикладного потока: TCP или UDP?

4. Достаточно ли номера 443, чтобы достоверно установить название и версию программы, которая его слушает?

Раздел 2. Инструменты эксплуатации систем и сетей

Контролируемые ИДК: ПК-2.2

Тема 2.1. Инструменты эксплуатации систем и сетей

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Проверка применимости готового PoC

Изучить выданный исходный пример проверки известного недостатка и сопоставить его условия с подготовленной уязвимой версией на стенде. Выполнить согласованный опыт с безвредным наблюдаемым эффектом и описать только подтвержденное воздействие

2. Адаптация и собственный проверочный пример

Изучить выданный исходный пример проверки известного недостатка и сопоставить его условия с подготовленной уязвимой версией на стенде. Выполнить согласованный опыт с безвредным наблюдаемым эффектом и описать только подтвержденное воздействие

3. Веб-прокси и управляемые тестовые входы

С помощью прокси исследовать запрос учебного веб-приложения и изменить один разрешенный параметр. Подготовить небольшой набор обычных и граничных входов, в том числе безвредную контрольную метку как учебную нагрузку, и сравнить реакции приложения

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как называется недостаток программы, который может быть использован для реализации угроз безопасности информации?

2. Какой идентификатор используют для однозначной ссылки на опубликованную уязвимость: CVE или номер TCP-порта?

3. Где обычно выполняется внедренный сценарий при XSS: в браузере пользователя или в программе архиватора?

4. При CSRF браузер отправил нежелательный запрос с действующим сеансом пользователя. Доказывает ли это кражу пароля?

Раздел 3. Инструменты закрепления в системе и сети

Контролируемые ИДК: ПК-2.2

Тема 3.1. Инструменты закрепления в системе и сети

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Наблюдение механизмов автозапуска Linux и Windows

На подготовленных учебных образах сопоставить списки служб, заданий и объектов автозапуска до и после заданного изменения преподавателя. Выделить следы изменения и

объяснить, какие сведения нужны для оценки его допустимости

2. Анализ полномочий и управляющего обмена

Исследовать подготовленные журналы процесса с измененным контекстом полномочий и синтетическую запись обмена учебных управляющего и управляемого компонентов. Выбрать средства для подтверждения фактических прав и связать команды с наблюдаемыми ответами.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой UID обычно имеет суперпользователь root в Linux?

2. Как называется автоматический запуск задачи в заранее заданное время?

3. Пользователь мог читать только свои записи, а после изменения роли получил административные функции. Какой вид расширения полномочий произошел?

4. Доказывает ли регулярное HTTPS-соединение с сервером само по себе наличие канала C2?

5. Счетчик переданных данных вырос со 100 до 160 байт. Сколько байт добавилось за интервал?

Раздел 4. Инструменты эксфильтрации данных

Контролируемые ИДК: ПК-2.2

Тема 4.1. Инструменты эксфильтрации данных

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Проверка передачи синтетических данных

Передать специально помеченный учебный файл между согласованными узлами и сопоставить событие с журналами отправителя, получателя и контроля передачи. Проверить предусмотренные сценарием разрешенную и запрещенную операции

2. Распознавание изменения представления передаваемых данных

По подготовленным файлам и захватам сравнить обычную передачу, передачу с изменением имени файла и передачу упакованных данных. Оценить, какие признаки остаются видимыми и каких данных не хватает, если содержимое канала зашифровано

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Можно ли гарантированно прочитать содержимое корректно защищенного TLS-потока только по PCAP, не имея нужных ключей?

2. Файл переименовали из report.txt в picture.jpg, не меняя байты. Изменилось ли его фактическое содержимое?

3. Снимок ВМ сохраняет состояние на определенный момент. Является ли один такой снимок полной заменой отдельной резервной копии всего стенда?

Раздел 5. Применение инструментов тестирования на проникновение в лабораторных условиях

Контролируемые ИДК: ПК-2.1

Тема 5.1. Применение инструментов тестирования на проникновение в лабораторных условиях

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Подготовка и восстановление лабораторного стенда

Развернуть рабочую и целевую ВМ в предусмотренном виртуальном сегменте, сохранить исходное состояние и проверить восстановление после контрольного изменения. Отдельно учесть подключенные каталоги и иные ресурсы вне сохраняемого состояния

2. Программа инструментальной проверки

На основе учебного требования безопасности выбрать проверяемые свойства и методы. Сопоставить используемые положения ГОСТ Р 56939-2024, методические рекомендации OWASP и руководства средств, не приписывая методическим документам статус обязательного закона

3. Сравнение настроек сетевого исследования

В одном и том же разрешенном сегменте сравнить результаты двух заранее заданных режимов средства обнаружения узлов и служб. Зафиксировать состав целей, время, интенсивность и ограничения, объяснить причину возможных расхождений

4. Проверка прав учебного веб-приложения

По заданной матрице ролей проверить доступ к собственным и чужим фиктивным объектам, а также к операции изменения роли. Сохранить запросы и результаты, отличив серверную проверку полномочий от ограничения элементов интерфейса

5. Учебная проверка фишингового сценария

Настроить локальный макет рассылки в учебные почтовые ящики без обращения к внешним получателям и без сбора настоящих паролей. Зафиксировать доставку, открытие учебной ссылки и срабатывания защиты как разные события

6. Выбор и ограничение учебной нагрузки

В предоставленном примере инструмента выбрать нагрузку, выполняющую только оговоренное безвредное действие, например выдачу контрольной строки. Объяснить связь между недостатком, способом его проверки и наблюдаемым действием нагрузки, сохранив исходный и полученный результат

7. Анализ синтетического управляющего обмена

По предоставленной записи сетевого обмена и журналам учебных компонентов восстановить связь задания и ответа. Сопоставить наблюдаемый поток с обычным служебным обменом и оценить, какие сведения позволяют подтвердить назначение соединения

8. Проверка контроля исходящих данных

Настроить предусмотренное преподавателем правило для синтетического набора и проверить его действие на разрешенной и запрещенной передаче. Сопоставить блокировку, предупреждение и фактическое получение данных, учитывая различие этих результатов

9. Проверка сообщения анализатора

Получить сообщение средства на выданном контрольном наборе, проверить его применимость и сопоставить с независимым наблюдением. Описать подтвержденные и неподтвержденные выводы, влияние неполных журналов и измененной конфигурации

10. Исправление и повторная проверка

На копии учебного объекта применить подготовленное исправление подтвержденного недостатка. Повторить исходный тест и проверить одну необходимую рабочую функцию, затем сопоставить состояния до и после изменения

11. Итоговый аналитический отчет по стенду

Объединить результаты выбранных инструментальных проверок в отчет: определить область и ограничения, привести доказательства, обоснованно описать последствия и меры исправления. Подготовить краткое резюме и технические карточки, удалив из выдаваемой копии секреты и сохранив исходные свидетельства

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Снимок ВМ сохраняет состояние на определенный момент. Является ли один такой снимок полной заменой отдельной резервной копии всего стенда?

2. В каком числовом диапазоне выражается базовая оценка CVSS v4.0?

3. Какой каталог описывает типовые слабости программных и аппаратных средств: CWE или PCAP?

4. Как называется инструментальный анализ исходного кода, выполняемый без его исполнения?

5. Какое событие нужно зафиксировать, если сканер не смог войти с выданной учебной учетной записью?

6. По условию код завершения 0 означает, что инструмент отработал без внутреннего сбоя. Доказывает ли этот код отсутствие уязвимостей?

7. Достаточно ли отсутствия ответа на один проверочный запрос, чтобы уверенно признать учебный узел выключенным?

8. Какую копию исходного файла результатов следует сохранить неизменной для последующего сопоставления?

9. Для опыта задано не более 5 запросов в секунду. Соответствует ли ограничению режим 20 запросов в секунду?

10. Дает ли подключение каталога хоста к контейнеру в режиме только чтения право менять файлы через это подключение?

11. Сканер указал возможный дефект, а контрольный опыт еще не выполнен. Какой статус точнее: «подтверждено» или «требует проверки»?

12. Может ли поставщик исправить недостаток в поддерживаемом выпуске, не переходя на новую основную версию программы?

13. Означает ли наличие администратора внутри контейнера автоматически полные административные права на хосте?

14. При захвате зафиксирована потеря пакетов. Можно ли считать полученный PCAP гарантированно полным описанием всего обмена?

15. Учебное разрешение на активную проверку действует до 16:00. Можно ли продолжить ее в 16:10 без согласованного продления?

7. Оценочные материалы промежуточной аттестации

3 семестр, Зачет

Контролируемые ИДК: ПК-2.1 ПК-2.2 ПК-2.3

Вопросы/Задания:

1. Как учитывать давность открытого источника при описании текущей инфраструктуры

2. Почему одинаковые настройки сканера не гарантируют одинаковый результат из разных сетевых сегментов?

3. Какие ограничения нужно указать при выводах по одному предоставленному PCAP?

4. Почему найденное доменное имя и IP-адрес следует фиксировать как связанную пару с датой?

5. Что отличает предположение о службе от подтвержденных сведений о ее версии?

6. Какие сведения должны сопровождать собственный учебный PoC для воспроизведения результата?

7. Как контрольный отрицательный случай помогает понять результат проверки?

8. Когда ручной просмотр обмена полезно сочетать с автоматическим средством?

9. Почему следует отдельно описывать эксплуатируемый недостаток и действие учебной нагрузки?

10. Что проверяет локальный учебный фишинговый сценарий и какие выводы требуют дополнительных данных?

11. Как сопоставление исходного и текущего состояния помогает исследовать автозапуск?

12. Какие основания нужны для вывода о неразрешенном повышении полномочий?

13. Почему классификация канала управления требует сведений о поведении компонентов?

14. Почему одинаковое имя учетной записи не всегда означает одинаковые фактические права?

15. Как подтвердить завершение учебного опыта после остановки управляющего компонента?

16. Что необходимо различать при оценке операции передачи данных?

17. Как меняется состав доступных наблюдений при шифровании прикладного канала?

18. Почему уменьшение числа видимых пакетов не всегда означает уменьшение объема переданных данных?

19. Чем отличаются предупреждение о передаче и ее фактическая блокировка?

20. Почему контроль по расширению файла недостаточен для оценки его содержания?

4 семестр, Зачет с оценкой
Контролируемые ИДК: ПК-2.1 ПК-2.2 ПК-2.3
Вопросы/Задания:

1. Как обеспечить воспроизводимость самостоятельного лабораторного исследования?

2. Какова роль нормативного документа, методики и руководства инструмента в одной проверке?

3. Как связать вывод отчета с конкретным свидетельством?

4. Почему техническая серьезность и приоритет исправления могут различаться?

5. Какие ограничения остаются после успешной повторной проверки исправления?