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
24 марта 2025 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «Б1.В.05 АНАЛИЗ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ»

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): 2025

Срок получения образования: 2 года

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

Москва, 2025

**Разработчики:**

Преподаватель кафедры Информационно-измерительных систем
Калмыков С. А.

Доцент кафедры Информационно-измерительных систем, к.т.н.
Тележников В. Ю.

Рабочая программа дисциплины (модуля) составлена 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 | 14.10.2024, № 10-24 |

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 - сформировать способность обоснованно оценивать защищенность компьютерной системы: выбирать методы анализа, исследовать код, конфигурации, сетевой трафик и журналы, отделять подтвержденные нарушения от предположений и представлять проверяемые предложения по защите.

Задачи изучения дисциплины:

- освоить определение границ анализа, применимости нормативных требований, модели угроз и возможностей нарушителя;
- научиться выбирать методы статического и динамического анализа, сканирования и фаззинга, проверять сообщения инструментов и воспроизводимость наблюдений;
- получить опыт анализа учебного трафика в Wireshark, восстановления потоков и сопоставления событий по подтверждаемым признакам;
- освоить проверку прав СУБД, конфигураций сетевого оборудования, беспроводных настроек и первичный анализ Android-приложений;
- научиться готовить аналитический отчет, связывать угрозы с проверяемыми требованиями и обосновывать защиту процесса, использующего БЯМ.Научиться готовить аналитический отчет, связывать угрозы с проверяемыми требованиями и обосновывать защиту процесса, использующего БЯМ.

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

*Компетенции, индикаторы и результаты обучения*

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/Ум1 Оценивать эффективность защиты информации

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/Зн1 Методы и методики оценки безопасности программно-аппаратных средств защиты информации

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/Ум1 Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных

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

## 3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.В.05 «Анализ безопасности компьютерных систем» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 1.

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) | Лекционные занятия (часы) | Практические занятия (часы) | Самостоятельная работа (часы) | Промежуточная аттестация (часы) |
|---|---|---|---|---|---|---|
| 1 семестр | 108 | 3 | 34 | 34 | 4 | Экзамен (36) |
| Всего | 108 | 3 | 34 | 34 | 4 | 36 |

## 5. Содержание дисциплины (модуля)

### 5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

| Наименование раздела, темы | Всего | Лекционные занятия | Практические занятия | Самостоятельная работа | Планируемые результаты обучения, соотнесенные с результатами освоения программы |
|---|---|---|---|---|---|
| **Раздел 1. Нормативное регулирование в области анализа безопасности компьютерных систем** | **8** | **4** | **4** | | ПК-2.1<br>ПК-2.2<br>ПК-2.3 |
| Тема 1.1. Аудит информационной безопасности. Построение модели угроз и модели нарушителя. Применение модели угроз и модели нарушителя при выполнении анализа безопасности компьютерных систем | 8 | 4 | 4 | | |
| **Раздел 2. Методы и инструменты проведения анализа безопасности компьютерных систем** | **14** | **6** | **6** | **2** | ПК-2.1<br>ПК-2.2<br>ПК-2.3 |
| Тема 2.1. Сканеры безопасности. Динамический анализ объектов оценки. Средства статического анализа исходного кода. Проведение тестирования на проникновения (оценки реального уровня защищенности). Фаззинг-тестирование | 14 | 6 | 6 | 2 | |
| **Раздел 3. Сбор информации об объекте анализа** | **14** | **4** | **8** | **2** | ПК-2.1<br>ПК-2.2<br>ПК-2.3 |
| Тема 3.1. Сбор и анализ сведений об объекте анализа. Определение топологии и структуры объекта оценки | 14 | 4 | 8 | 2 | |
| **Раздел 4. Особенности анализа безопасности СУБД** | **10** | **6** | **4** | | ПК-2.1<br>ПК-2.2<br>ПК-2.3 |
| Тема 4.1. Политика и модели безопасности в СУБД. Анализ угроз и уязвимостей СУБД | 10 | 6 | 4 | | |
| **Раздел 5. Особенности анализа безопасности телекоммуникационного оборудования** | **8** | **4** | **4** | | ПК-2.1<br>ПК-2.2<br>ПК-2.3 |

| | | | | | |
|---|---|---|---|---|---|
| Тема 5.1. Исследование программного обеспечения телекоммуникационного оборудования. Исследование конфигурационных файлов | 8 | 4 | 4 | | |
| **Раздел 6. Особенности анализа защищенности беспроводных сетей** | **8** | **4** | **4** | | ПК-2.1<br>ПК-2.2<br>ПК-2.3 |
| Тема 6.1. Компьютерные атаки в беспроводных сетях. Основные средства оценки уязвимостей в беспроводных сетях. Обнаружение скрытых сетей | 8 | 4 | 4 | | |
| **Раздел 7. Анализ безопасности мобильных приложений** | **10** | **6** | **4** | | ПК-2.1<br>ПК-2.2<br>ПК-2.3 |
| Тема 7.1. Особенности архитектуры ОС Android. Первичный анализ мобильных приложений ОС Android | 10 | 6 | 4 | | |
| **Итого** | **72** | **34** | **34** | **4** | |

### 5.2. Содержание разделов, тем дисциплин и формы текущего контроля

***Раздел 1. Нормативное регулирование в области анализа безопасности компьютерных систем***

*Тема 1.1. Аудит информационной безопасности. Построение модели угроз и модели нарушителя. Применение модели угроз и модели нарушителя при выполнении анализа безопасности компьютерных систем*

.. Основные термины и определения. Нормативные документы, связанные с вопросами анализа безопасности компьютерных систем. Требования регуляторов по проведению анализа защищенности государственных информационных систем и систем персональных данных. Аудит информационной безопасности. Особенности проведения аудита информационной безопасности объектов критической информационной инфраструктуры (КИИ). Понятие модели угроз и модели нарушителя, методы их построения и применения при выполнении анализа безопасности компьютерных систем. Границы и доказательная база анализа, проверка применимости действующей редакции нормативного документа к виду системы. Сервисный портал с БЯМ: защищаемые данные, границы доверия, возможности нарушителя, сценарии воздействия через недоверенные данные, требования и наблюдаемые критерии.

Текущий контроль

| Вид (форма) контроля |
|---|
| Тестирование |
| Практическая работа |

***Раздел 2. Методы и инструменты проведения анализа безопасности компьютерных систем***

*Тема 2.1. Сканеры безопасности. Динамический анализ объектов оценки. Средства статического анализа исходного кода. Проведение тестирования на проникновения (оценки реального уровня защищенности). Фаззинг-тестирование*

Цели и задачи анализа безопасности компьютерных систем. Основные этапы проведения анализа безопасности компьютерных систем. Основные методы, программные и аппаратно-программные средства проведения анализа безопасности компьютерных систем. Сканеры безопасности. Динамический анализ объектов оценки. Средства статического анализа исходного кода. Проведение тестирования на проникновения (оценки реального уровня защищенности). Фаззинг-тестирование. Проверка ложных срабатываний и воспроизводимость результатов. Сравнение наблюдений с гипотезой; границы вывода об уязвимости. Оценка предлагаемого механизма защиты БЯМ по условиям научного исследования и собственным проверяемым сценариям.

Текущий контроль

| Вид (форма) контроля |
|---|
| Тестирование |
| Практическая работа |

***Раздел 3. Сбор информации об объекте анализа***

*Тема 3.1. Сбор и анализ сведений об объекте анализа. Определение топологии и структуры объекта оценки*

Методы сбора и анализа сведений об объекте анализа. Топология и структура объекта оценки. Направления движения информационных потоков. Выделение наиболее важных составляющих объекта оценки. Анализ предоставленных записей PCAP/PCAPNG средствами Wireshark: адреса, протоколы, фильтры, потоки, передаваемые объекты и признаки утечки. Журналы и подтверждение выводов. Архитектура сервисного портала с БЯМ, общие данные, состояния, внешняя доставка уведомлений и неизвестный результат операции.

Текущий контроль

| Вид (форма) контроля |
|---|
| Тестирование |
| Практическая работа |

***Раздел 4. Особенности анализа безопасности СУБД***

*Тема 4.1. Политика и модели безопасности в СУБД. Анализ угроз и уязвимостей СУБД*

Угрозы безопасности БД. Целостность и аудит. Многоуровневая защита информации в СУБД. Политика и модели безопасности в СУБД. Анализ угроз и уязвимостей СУБД. Минимальные полномочия ролей, параметризованные запросы и сведения журнала. Контроль предложения БЯМ по разрешенным действиям и бизнес-правилам; сохранение только существующим прикладным сервисом.

Текущий контроль

| Вид (форма) контроля |
|---|
| Практическая работа |

***Раздел 5. Особенности анализа безопасности телекоммуникационного оборудования***

*Тема 5.1. Исследование программного обеспечения телекоммуникационного оборудования. Исследование конфигурационных файлов*

Цели и задачи анализа защищенности телекоммуникационного оборудования. Исследование программного обеспечения телекоммуникационного оборудования. Исследование конфигурационных файлов. Привязка результатов к модели устройства и версии ПО, разрешенные служебные подключения, порядок применения правил и проверка изменений на учебном стенде.

Текущий контроль

| Вид (форма) контроля |
|---|
| Практическая работа |

***Раздел 6. Особенности анализа защищенности беспроводных сетей***

*Тема 6.1. Компьютерные атаки в беспроводных сетях. Основные средства оценки уязвимостей в беспроводных сетях. Обнаружение скрытых сетей*

Компьютерные атаки в беспроводных сетях. Слабости применяемых протоколов шифрования. Основные средства оценки уязвимостей в беспроводных сетях. Режимы работы WiFi-адаптеров. Обнаружение скрытых сетей. Различие между сокрытием имени сети, аутентификацией и защитой содержимого обмена. Ограничения адаптера, драйвера, канала и времени наблюдения.

Текущий контроль

| Вид (форма) контроля |
|---|
| Практическая работа |

***Раздел 7. Анализ безопасности мобильных приложений***

*Тема 7.1. Особенности архитектуры ОС Android. Первичный анализ мобильных приложений ОС Android*

Первичный анализ мобильных приложений ОС Android. UID и изоляция приложений. Состав манифеста, объявленные компоненты и разрешения. Сопоставление статических сведений с наблюдением поведения, обработка отказа в разрешении.

Текущий контроль

| Вид (форма) контроля |
|---|
| Практическая работа |

## 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: Экзамен, 1 семестр.*
Промежуточная аттестация по дисциплине проводится в форме экзамена. 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:
Экзамен оценивается по пятибалльной шкале:
- оценка «отлично» выставляется, если обучающийся набрал 86–100 баллов и продемонстрировал системное и полное освоение содержания дисциплины; ответы правильные, обоснованные и терминологически точные;
- оценка «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, если основное содержание освоено; допущены отдельные неточности, не влияющие на общее понимание материала;
- оценка «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если освоены базовые понятия и положения, но имеются существенные пробелы и ошибки;
- оценка «неудовлетворительно» выставляется, 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:
Экзамен оценивается по пятибалльной шкале:
- оценка «отлично» выставляется, если даны полные, правильные и логически последовательные ответы; терминология применяется корректно; приведены необходимые обоснования и примеры; дополнительные вопросы раскрыты;
- оценка «хорошо» выставляется обучающемуся, если вопросы раскрыты правильно и достаточно полно; отдельные неточности исправлены после уточняющих вопросов;
- оценка «удовлетворительно» выставляется обучающемуся, если основные положения раскрыты фрагментарно; имеются существенные неточности, однако базовое понимание продемонстрировано;
- оценка «неудовлетворительно» выставляется, если вопросы не раскрыты либо допущены принципиальные ошибки; отсутствует владение базовой терминологией.

## 7. Оценочные материалы текущего контроля

***Раздел 1. Нормативное регулирование в области анализа безопасности компьютерных систем***

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

*Тема 1.1. Аудит информационной безопасности. Построение модели угроз и модели нарушителя. Применение модели угроз и модели нарушителя при выполнении анализа безопасности компьютерных систем*

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Границы анализа и применимость требований

Для учебной информационной системы определить назначение, данные и границы проверки. По предоставленным нормативным документам составить таблицу «требование — основание применимости — способ проверки», отдельно указав неподтвержденные сведения.

2. Модель угроз сервисного портала

Для выбранной операции портала описать данные, участников, возможности нарушителя и три простых сценария воздействия. Связать каждый сценарий с последствиями, требованием и наблюдаемым признаком его выполнения.

3. Угроза и защита операции с БЯМ

Для одной операции сервисного портала обозначить данные модели, допустимые действия, границы доверия и роль человека. Описать один сценарий воздействия через входные данные и связать его с механизмом защиты и наблюдаемой проверкой.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте учебный анализ: последствия оценивают после определения объекта, сценарий — после возможностей нарушителя.

А. Описать объект и его данные
Б. Уточнить возможности нарушителя
В. Описать сценарий реализации угрозы
Г. Определить негативные последствия

2. В курсовой работе гипотезу формулируют после изучения процесса, а защиту выбирают по выявленным угрозам. Укажите порядок.

А. Выделить угрозы нового варианта
Б. Выбрать связанные с угрозами защитные механизмы
В. Изучить исходный процесс
Г. Обосновать операцию с БЯМ

3. Требование выбирают по угрозе, а наблюдаемый критерий — по требованию. Упорядочьте действия.

А. Определить требование безопасности
Б. Описать сценарий угрозы
В. Проверить выполнение критерия
Г. Задать наблюдаемый критерий выполнения

4. Исправьте порядок работы над моделью: сравнение возможно только после двух вариантов, итог — после сравнения.

А. Построить вариант с защитой
Б. Сформулировать вывод и ограничения
В. Описать исходный вариант процесса
Г. Сопоставить их по выбранному критерию

***Раздел 2. Методы и инструменты проведения анализа безопасности компьютерных систем***

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

*Тема 2.1. Сканеры безопасности. Динамический анализ объектов оценки. Средства статического анализа исходного кода. Проведение тестирования на проникновения (оценки реального уровня защищенности). Фаззинг-тестирование*

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Проверка сообщения статического анализатора

Изучить небольшой учебный фрагмент кода и сообщения инструмента. Проверить контекст двух сообщений, определить, подтверждается ли предполагаемая ошибка, и предложить исправление подтвержденного недостатка.

2. Наблюдение поведения на некорректном входе

На изолированном учебном приложении сравнить обработку обычного и некорректного входа. Сохранить данные и условия опыта, повторить наблюдение и объяснить, что подтверждает найденная реакция.

3. Разбор результатов сетевого сканирования

На предоставленном отчете или разрешенном учебном стенде выделить узлы, порты и службы. Сопоставить их с назначением системы и выбрать два наблюдения для уточняющей проверки.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте разбор сообщения статического анализатора: отчет готовят после проверки контекста.

А. Получить сообщение анализатора
Б. Найти соответствующий участок кода
В. Зафиксировать обоснованный вывод
Г. Проверить сообщение с учетом контекста

2. Для учебного фаззинга вход задают до запуска, повтор выполняют по сохраненному наблюдению. Укажите порядок.

А. Повторить опыт для проверки воспроизводимости
Б. Сохранить вход и наблюдаемый результат
В. Подготовить тестовый вход
Г. Передать его программе на стенде

3. Сканирование проводится только после согласования области. Дальнейший разбор опирается на сохраненный результат. Укажите порядок.

А. Сохранить сведения о найденных службах
Б. Выполнить согласованную проверку
В. Уточнить разрешенные узлы и проверки
Г. Разобрать значение полученных сведений

4. В учебном сценарии исправление делают после подтверждения дефекта, закрытие — после повторной проверки. Укажите порядок.

А. Внести исправление подтвержденного дефекта
Б. Повторить проверку в сопоставимых условиях
В. Проверить обоснованность сообщения
Г. Зафиксировать результат исправления

***Раздел 3. Сбор информации об объекте анализа***

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

*Тема 3.1. Сбор и анализ сведений об объекте анализа. Определение топологии и структуры объекта оценки*

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Топология по учебному трафику

Открыть net.pcap или pcap.pcap из материалов преподавателя, выделить основные адреса и наблюдаемые обмены. Построить схему исследуемого фрагмента сети и подтвердить связи номерами пакетов, отметив, чего по записи установить нельзя.

2. Передача объекта в потоке

В challenge.pcapng найти обмен, содержащий передаваемый объект. Указать участников и протокол, исследовать доступные метаданные объекта и объяснить, какие признаки подтверждают передачу. Извлеченные данные не исполнять.

3. Проверка гипотезы об утечке по PCAP

В exfiltration.pcapng выделить обмены, относящиеся к проверяемой гипотезе о передаче данных за границу учебного контура. Объяснить, какие наблюдения поддерживают гипотезу, а какие требуют дополнительного контекста.

4. Поиск нужного обмена и сопоставление следов

В sharkfin.pcap или happyhalloween2018.pcapng выбрать один доступный эпизод обмена, сузить поиск фильтром и восстановить его последовательность. При наличии выданного журнала сопоставить события по времени и адресам; перечислить ограничения сопоставления.

5. Согласование состояний и неизвестного результата

На схеме портала разобрать ситуацию, когда результат отправки уведомления неизвестен. Показать проверку статуса, предотвращение необоснованного повтора и согласование состояния карточки с другими процессами; оформить короткое аналитическое заключение.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Укажите порядок анализа файла: пакет выбирают из результата фильтрации, вывод делают после просмотра его полей.

А. Применить подходящий фильтр отображения
Б. Исследовать поля выбранного пакета
В. Открыть предоставленный файл трафика
Г. Записать подтвержденное наблюдение

2. Таблицу узлов строят по собранным адресам, схему — по таблице и связям. Укажите порядок.

А. Собрать сведения об адресах
Б. Составить таблицу узлов
В. Построить схему исследуемого фрагмента сети
Г. Выделить наблюдаемые связи

3. В отчете поток рассматривают после его выбора, вывод — после фиксации данных. Укажите порядок.

А. Выбрать относящийся к нему поток
Б. Зафиксировать существенные поля и номера пакетов
В. Объяснить, что именно подтверждает этот обмен
Г. Найти пакет нужного обмена

4. В заданном портале изменения сохраняет прикладной сервис после проверки предложения. Укажите порядок.

А. Сохранить допустимое изменение прикладным сервисом
Б. Проверить предложение и полномочия операции
В. Собрать разрешенные для задачи данные
Г. Получить предложение БЯМ

***Раздел 4. Особенности анализа безопасности СУБД***

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

*Тема 4.1. Политика и модели безопасности в СУБД. Анализ угроз и уязвимостей СУБД*

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Проверка полномочий ролей СУБД

Для учебной базы портала составить роли чтения, обработки и администрирования. Проверить одну разрешенную и одну запрещенную операцию каждой роли, затем устранить выявленное избыточное право и повторить проверку.

2. Отделение данных от SQL-команды

На двух коротких примерах сравнить построение запроса конкатенацией строки и передачей параметров. Объяснить, где пользовательское значение может изменить структуру команды, и подготовить безопасный вариант учебного запроса.

3. Аудит изменения записи

По учебному журналу восстановить, кто и когда пытался изменить запись, каков результат и какими событиями это подтверждено. Предложить недостающие поля журнала и исключить запись ненужных секретов.

***Раздел 5. Особенности анализа безопасности телекоммуникационного оборудования***

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

*Тема 5.1. Исследование программного обеспечения телекоммуникационного оборудования. Исследование конфигурационных файлов*

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Исследование конфигурации сетевого устройства

Для предоставленной конфигурации учебного маршрутизатора установить назначение интерфейсов и разрешенных служебных подключений. Сопоставить настройки с требуемой схемой взаимодействия и предложить обоснованное ограничение избыточного доступа.

2. Проверка правил фильтрации

Для заданного порядка обработки правил определить результат четырех учебных соединений. Сравнить расчет с журналом или поведением стенда, исправить одно конфликтующее правило и повторить проверку.

***Раздел 6. Особенности анализа защищенности беспроводных сетей***

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

*Тема 6.1. Компьютерные атаки в беспроводных сетях. Основные средства оценки уязвимостей в беспроводных сетях. Обнаружение скрытых сетей*

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Оценка настроек учебной Wi-Fi-сети

По предоставленным настройкам точки доступа раздельно оценить объявление имени, аутентификацию и защиту передаваемых данных. Объяснить, какие выводы нельзя делать только по наличию или отсутствию SSID в списке.

2. Анализ ограничений беспроводного захвата

На учебной записи кадров или согласованном стенде определить канал, доступные адресные сведения и интервал наблюдения. Разобрать, как возможности адаптера и режим захвата ограничивают выводы о сети.

***Раздел 7. Анализ безопасности мобильных приложений***

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

*Тема 7.1. Особенности архитектуры ОС Android. Первичный анализ мобильных приложений ОС Android*

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Первичный анализ Android-приложения

Для выданного учебного приложения изучить идентификатор, версию, компоненты и разрешения в манифесте. Сопоставить запросы полномочий с назначением приложения и составить план двух коротких проверок.

2. Поведение при отказе в разрешении

В учебном эмуляторе или ВМ проверить согласованную функцию Android-приложения при предоставленном и отклоненном разрешении. Зафиксировать наблюдения, доступную пользователю функцию и обработку отказа.

## 8. Оценочные материалы промежуточной аттестации

*1 семестр, Экзамен*

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

Вопросы/Задания:

1. Какие сведения нужны, чтобы описать конкретную угрозу системе?

2. Для чего проверяют применимость нормативного документа?

3. Чем нарушение конфиденциальности отличается от нарушения целостности?

4. Как сделать требование безопасности проверяемым?

5. Что остается у прикладных сервисов после добавления БЯМ в заданный портал?

6. Чем различаются статический и динамический анализ?

7. Почему сообщения анализатора требуют проверки?

8. Для чего при фаззинге сохраняют вызвавший сбой вход?

9. Что показывает открытый сетевой порт?

10. Зачем заранее задавать границы активной сетевой проверки?

11. Чем фильтр отображения отличается от удаления пакетов?

12. Что необходимо включить в подтверждение вывода по PCAP?

13. Почему по короткому захвату нельзя автоматически восстановить всю сеть?

14. Как связать события разных журналов с одним запросом?

15. Почему тайм-аут внешнего сервиса не всегда означает отсутствие выполненного действия?

16. Что означает принцип минимальных полномочий для учетной записи приложения?

17. Как параметризованный запрос противодействует SQL-инъекции?

18. Какие сведения помогают разбирать изменение записи БД?

19. Почему после отзыва одного разрешения доступ нужно проверить повторно?

20. Почему предложение БЯМ не следует исполнять как произвольный запрос к БД?

21. Для чего при анализе оборудования нужны модель и версия ПО?

22. Как оценить разрешающее правило межсетевого экрана?

23. Почему порядок правил иногда влияет на итоговое решение?

24. Как журнал помогает объяснить отказ соединения?

25. Зачем сохранять исходную конфигурацию перед учебным изменением?

26. Почему SSID нельзя считать средством шифрования?

27. Какие условия влияют на доступность режима монитора?

28. Почему при анализе Wi-Fi учитывают канал?

29. Что следует оценивать отдельно от сокрытия имени сети?

30. Какие ограничения у вывода, сделанного по одному короткому беспроводному захвату?

## 9. Материально-техническое и учебно-методическое обеспечение дисциплины

### 9.1. Перечень основной и дополнительной учебной литературы

*Основная литература*

1. Киренберг А. Г. Информационная безопасность современных операционных систем: учебное пособие / А. Г. Киренберг. - Информационная безопасность современных операционных систем - Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. - 138 с. - 978-5-00137-320-9. - Текст: электронный // IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/128393.html - Режим доступа: по подписке

2. Киренберг А. Г. Системное администрирование и информационная безопасность сетей ЭВМ: учебное пособие / А. Г. Киренберг. - Кемерово: КузГТУ имени Т.Ф. Горбачева, 2022. - 120 с. - 978-5-00137-292-9. - Текст: электронный // Издательство Лань: [сайт]. - URL: https://e.lanbook.com/book/257564 - Режим доступа: по подписке

3. Информационная безопасность современных операционных систем: учебное пособие / Киренберг, Г. А. . - Кемерово: КузГТУ имени Т.Ф. Горбачева, 2022. - 138 с. - 978-5-00137-320-9. - Текст: электронный // Издательство Лань: [сайт]. - URL: https://e.lanbook.com/book/295736 - Режим доступа: по подписке

*Дополнительная литература*

1. Сидоренко В. Г. Аспекты информационной безопасности: учебное пособие / В. Г. Сидоренко, Н. Н. Скоробогатова. - Аспекты информационной безопасности - Москва: Российский университет транспорта (МИИТ), 2018. - 64 с. - 2227-8397. - Текст: электронный // IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/115921.html - Режим доступа: по подписке

2. Старолетов С. М. Основы тестирования программного обеспечения: учебное пособие для спо / С. М. Старолетов. - 5-е изд., стер. - Санкт-Петербург: Лань, 2025. - 192 с. - 978-5-507-53820-1. - Текст: электронный // Издательство Лань: [сайт]. - URL: https://e.lanbook.com/book/499391 - 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://rusneb.ru/ - Национальная электронная библиотека (НЭБ)
2. https://urait.ru - Образовательная платформа «Юрайт»
3. https://intuit.ru/ - Электронная образовательная среда "ИНТУИТ"
4. https://www.elibrary.ru/ - НЭБ eLIBRARY
5. https://scholar.google.ru/ - Гугл Академия

## 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)*

1. Sublime Text 3;
2. 7Zip;
3. Microsoft Office;
4. Notepad++;
5. Microsoft Visual Studio;

*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 - 5 шт.
Автоматизированное рабочее место (АРМ) - 15 шт.
Доска настенная одноэлементная - 2 шт.

Учебная аудитория

Автоматизированное рабочее место (АРМ) - 1 шт.
Проектор - 2 шт.

Доска настенная одноэлементная - 1 шт.

Смешанный тип

Автоматизированное рабочее место (АРМ) - 1 шт.
Доска настенная одноэлементная - 2 шт.
Интерактивная панель - 1 шт.
Проектор - 1 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.