



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.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): 2024

Срок получения образования: 2 года

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

Москва, 2024

**Разработчики:**

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<br>лицо                        | ФИО             | Виза        | Дата, протокол<br>(при наличии) |
|---|-----------------------------------------------------------------|----------------------------------------------|-----------------|-------------|---------------------------------|
| 1 | факультет<br>Геоинформатики и<br>информационной<br>безопасности | Председатель<br>ученого совета<br>факультета | Матерухин А. В. | Рассмотрено | 14.12.2023, №<br>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 анализа безопасности компьютерных систем.

Задачи изучения дисциплины:

- Развитие у студентов соответствующих профессиональных компетенций.;
- Формирование знаний нормативных документов в области анализа безопасности компьютерных систем.;
- Формирование умения выстраивать процесс оценки уровня безопасности компьютерных систем.;
- Выработка умений и практических навыков применения современных программных и программно-аппаратных решений для анализа защищенности компьютерных систем..

## **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/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

*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

*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, соотношенные с результатами освоения программы |
|-----------------------------------------------------------------------------------------------|----------|--------------------|----------------------|------------------------|---------------------------------------------------------------------------------|
| <b>Раздел 1. Нормативное регулирование в области анализа безопасности компьютерных систем</b> | <b>8</b> | <b>4</b>           | <b>4</b>             |                        | ПК-2.1                                                                          |

|                                                                                                                                                                                                                           |           |          |          |          |                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|----------|----------|----------|----------------------------|
| 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        |          |                            |
| <b>Раздел 2. Методы и инструменты проведения анализа безопасности компьютерных систем</b>                                                                                                                                 | <b>14</b> | <b>6</b> | <b>6</b> | <b>2</b> | ПК-2.2                     |
| 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        |                            |
| <b>Раздел 3. Сбор информации об объекте анализа</b>                                                                                                                                                                       | <b>14</b> | <b>4</b> | <b>8</b> | <b>2</b> | ПК-2.3                     |
| Тема 3.1. Сбор и анализ сведений об объекте анализа. Определение топологии и структуры объекта оценки.                                                                                                                    | 14        | 4        | 8        | 2        |                            |
| <b>Раздел 4. Особенности анализа безопасности СУБД</b>                                                                                                                                                                    | <b>10</b> | <b>6</b> | <b>4</b> |          | ПК-2.2<br>ПК-2.3           |
| Тема 4.1. Политика и модели безопасности в СУБД. Анализ угроз и уязвимостей СУБД.                                                                                                                                         | 10        | 6        | 4        |          |                            |
| <b>Раздел 5. Особенности анализа безопасности телекоммуникационного оборудования</b>                                                                                                                                      | <b>8</b>  | <b>4</b> | <b>4</b> |          | 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        |          |                            |
| <b>Раздел 6. Особенности анализа защищенности беспроводных сетей</b>                                                                                                                                                      | <b>8</b>  | <b>4</b> | <b>4</b> |          | 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        |          |                            |
| <b>Раздел 7. Анализ безопасности мобильных приложений</b>                                                                                                                                                                 | <b>10</b> | <b>6</b> | <b>4</b> |          | ПК-2.1<br>ПК-2.2           |

|                                                                                                 |           |           |           |          |        |
|-------------------------------------------------------------------------------------------------|-----------|-----------|-----------|----------|--------|
| Тема 7.1. Особенности архитектуры ОС Android. Первичный анализ мобильных приложений ОС Android. | 10        | 6         | 4         |          | ПК-2.3 |
| <b>Итого</b>                                                                                    | <b>72</b> | <b>34</b> | <b>34</b> | <b>4</b> |        |

## 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.

### ***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 аппаратное-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.

### ***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. Топо-логия и структура объекта оценки. Направления движения информационных потоков. Выделение наиболее важных составляющих объекта оценки.

### ***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.

## **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.

## **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.

## **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.

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: Экзамен, I семестр.*

Экзамен 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 наличии 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 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: Тестирование

Вопросы/Задания:

1. Какие существуют основные классы атак? Выберите несколько из 4 вариантов ответа:

1. Локальная атака
2. Удаленная атака
3. Атака на поток данных
4. Распределенная атака

2. ... - совокупность процедур или мероприятий, которые производятся при нарушении или подозрении на нарушение информационной безопасности.

1. Реагирование на инциденты
2. Управление конфигурацией
3. Управление пользователями
4. Управление рисками
5. Обеспечение устойчивости

3. ... - это вариант атаки, когда злоумышленник не видит ту рабочую станцию, с которой он работает. Выберите один из 5 вариантов ответа:

1. Локальная атака
2. Удаленная атака
3. Атака на поток данных
4. Рейдерская атака
5. Социальная инженерия

4. ... - это вариант атаки, когда атакуемый компьютер активно отправляет, принимает или обменивается с данными с другими компьютерами сети, локальной или глобальной, а местом приложения атакующего воздействия является сегмент сети или сетевой узел между этими системами. Выберите один из 5 вариантов

1. Локальная атака

2. Удаленная атака
3. Атака на поток данных
4. Рейдерская атака
5. Социальная инженерия

5. ... - идейный борец за свободу информации, вторгающийся в чужие системы в основном из интереса, без прямой материальной заинтересованности. Выберите один из 5 вариантов ответа:

1. Хакер
2. Кракер
3. Фрикер
4. Джокер
5. Анонимайзер

6. ... - тот, кто взламывает чужие системы, преследуя собственный финансовый интерес. Выберите один из 5 вариантов ответа:

1. Хакер
2. Кракер
3. Фрикер
4. Джокер
5. Анонимайзер

7. ... - злоумышленник, использующий в собственных интересах уязвимости в телефонных системах. Выберите один из 5 вариантов ответа:

1. Хакер
2. Кракер
3. Фрикер
4. Джокер
5. Анонимайзер

8. К методам защиты от НСД относятся:

1. Разделение доступа
2. Разграничение доступа
3. Увеличение доступа
4. Ограничение доступа
5. Аутентификация и идентификация

9. Выделите группы, на которые делятся средства защиты информации:

1. Физические, аппаратные, программные, криптографические, комбинированные
2. Химические, аппаратные, программные, криптографические, комбинированные
3. Физические, аппаратные, программные, этнографические, комбинированные

10. Что такое компьютерный вирус?

1. Разновидность программ, которые способны к размножению
2. Разновидность программ, которые самоуничтожаются
3. Разновидность программ, которые не работают
4. Разновидность программ, которые плохо работают

11. Как подразделяются вирусы в зависимости от деструктивных возможностей?:

1. Сетевые, файловые, загрузочные, комбинированные
2. Безвредные, неопасные, опасные, очень опасные
3. Резидентные, нерезидентные
4. Полиморфные, макровирусы, вирусы-невидимки, "паразитические", "черви", компаньон-вирусы

12. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется ор-ганизация в своей деятельности называется:

1. Политикой информации
2. Защитой информации
3. Политикой безопасности

#### 4. Организацией безопасности

13. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется:

1. Системой угроз
2. Системой защиты
3. Системой безопасности
4. Системой уничтожения

14. Какие атаки предпринимают хакеры на программном уровне?

1. Атаки на уровне ОС
2. Атаки на уровне сетевого ПО
3. Атаки на уровне пакетов прикладных программ
4. Атаки на уровне СУБД

15. Что такое криптография?

1. Метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом
2. Область доступной информации
3. Область тайной связи, с целью защиты от ознакомления и модификации посторонним лицом

16. Какими методами можно оценить защищенность компьютерной системы?

1. Пентестирование
2. Анализ рисков
3. Опрос пользователей
4. Все вышеперечисленные методы

17. Какие виды уязвимостей могут быть обнаружены при пентестировании компьютер-ной системы?

1. Уязвимости в конфигурации
2. Уязвимости в коде программного обеспечения
3. Уязвимости в сетевых протоколах
4. Все вышеперечисленные виды уязвимостей

18. Какие виды атак могут использоваться для компрометации компьютерной системы?

1. Phishing
2. Brute-force атаки
3. DoS/DDoS атаки
4. Все вышеперечисленные виды атак

19. Между какими уровнями работает протокол SSL?

1. Канальным и физическим
2. Сетевым и канальным
3. Транспортным и сетевым
4. Прикладным и транспортным

20. Какие из следующих популярных VPN-протоколов работают на сетевом уровне модели ISO/OSI?

1. OpenVPN
2. PPTP
3. IPSEC
4. L2TP

21. МЭ уровня приложения создает:

1. Виртуальное соединение между клиентом и сервером
2. Туннель между клиентом и сервером
3. Временное соединение между клиентом и сервером
4. Реальное соединение между клиентом и сервером

22. Какое средство необходимо использовать для определения того, уязвим ли хост к известным атакам?

1. Honey Pot
2. Padded Cell
3. Сканер безопасности

23. Что из указанного ниже является активными сетевыми атаками?

1. Анализ данных межсетевого информационного обмена
2. Пассивный перехват
3. Спуфинг
4. Подглядывание за вводом пользователя

24. Какой вид атаки на WiFi-сети направлен на получение доступа к данным, передаваемым между устройствами и точкой доступа?

1. Атака Man-in-the-Middle
2. Атака Replay Attack
3. Атака Rogue Access Point
4. Атака Denial-of-Service (DoS)

25. Какая из этих угроз безопасности СУБД связана с неправильной конфигурацией доступа?

1. SQL Injection
2. Buffer Overflow
3. Denial of Service (DoS)
4. Утечка данных (Data Leakage)

26. Сканирование сетевых портов помогает определить:

1. Установленное программное обеспечение
2. Версию операционной системы
3. Запущенные сетевые сервисы
4. Все из перечисленного

27. Программное обеспечение Wireshark чаще всего применяется для:

1. Перехвата и анализа сетевого трафика
2. Подбора паролей
3. Проведения фаззинг-тестирования
4. Для организации vpn-соединения

28. Что означает аббревиатура VPN?

1. Virtual Private Network
2. Virus Protection Network
3. Visual Private Network
4. Virtual Protection Network

29. К сетевым сканерам относятся:

1. Nmap
2. John the Ripper
3. Honey Pot
4. Ни одно из перечисленных средств

30. Что из перечисленного является примером межсайтового скриптинга (XSS)?

1. Изменение содержимого веб-страницы
2. Взлом сервера базы данных
3. Подмена запросов
4. Удаленное управление компьютером пользователя

## **8. Оценочные материалы промежуточной аттестации**

*I семестр, Экзамен*

Вопросы/Задания:

1. Какая проблема возникает при использовании асимметричной криптографии?
2. В чём заключается суть атаки «человек посередине» при обмене открытыми ключами?
3. Какие уязвимости обычно устраняются путём установки обновлений ("патчей")?
4. Как может быть выполнено отслеживание маршрута при ограничении прохождения трафика UDP и ICMP?
5. Какие методы выявления уязвимостей применяются в локальных сканерах (устанавливаемых в виде агентов)?
6. Какие ограничения имеются при использовании ARP Ping для идентификации сетевых объектов?
7. Проверки какого типа требуют дополнительной верификации наличия уязвимости?
8. Какие предположение относительно операционной системы удалённого узла можно сделать, основываясь на том, что на узле открыты порты 3389/tcp, 135/tcp, 445/tcp?
9. Какие из вариантов аутентификации EAP уязвимы к атакам по словарю?
10. Какие из вариантов аутентификации EAP предполагают аутентификацию клиента на основе сертификата?
11. В каком случае атака SSL Strip окажется неуспешной?
12. От имени какой учётной записи запускается поток, обслуживающий запрос к web-приложению с анонимным доступом?
13. Какая техника может быть использована для фиксации идентификатора сессии при атаке на клиента web-приложения?
14. Каким образом можно использовать внедрение SQL кода для просмотра произвольных таблиц на сервере SQL?
15. С помощью какой уязвимости можно получить доступ к содержимому сценария на web-сервере?
16. Как может быть получен список файлов на web-сервере, помимо использования уязвимости «Индексирование директорий»?
17. Какой вариант XSS-атаки требует перехода по ссылке, сформированной злоумышленником?
18. На чём основан децентрализованный вариант управления бот-сетями?

19. При использовании DNS-туннелирования нуждается ли клиентская часть в прямом доступе к серверной части?

20. На чём основано использование протоколов прикладного уровня для создания скрытых каналов взаимодействия?

21. В чём заключается главный недостаток использования заголовков сетевого и транспортного уровней для создания скрытых каналов взаимодействия?

22. Что такое Exploit Kit?

23. Что такое landing page (целевая страница) в составе Exploit Kit?

24. По какой части идентификатора пользователя Windows (SID) можно выделить учётную запись локального администратора?

25. Как можно быстро перечислить сайты, расположенные на одном адресе?

26. Как работает технология VMBR (Virtual Machine Based Rootkit)?

27. Как можно использовать неавторизованный сервер DHCP для атак «человек посередине»?

28. На истощение какого ресурса чаще всего направлена атака UDP Flood?

29. Какие угрозы связаны с использованием протокола DHCP?

30. В каком случае более точно перечислены типы проверок, используемых в сетевых сканерах безопасности?

31. В каком случае наиболее правильно перечислены "векторы атак" на сервис DNS?

32. Какой из механизмов реализации сетевых атак не подразумевает использования какой-либо уязвимости?

33. Можно ли использовать ARP-запрос для добавления записи в ARP-таблицу?

34. Какие алгоритмы используются для обеспечения целостности передаваемых данных?

35. Как может быть использовано нарушителем сообщение "ICMP Redirect"?

36. К какому шагу цикла PDCA (Plan, Do, Check, Act) относится тестирование на проникновение?

37. Какой из методов идентификации узлов сети работает только в пределах только одного сетевого сегмента?

38. В каком из методов идентификации узлов сети вывод об обнаружении узла основывается на получении в ответ ICMP сообщения об ошибке?

39. Какой из методов сканирования портов позволяет определить факт фильтрации порта TCP?
40. Какие типы проверок используются в сетевых сканерах безопасности?
41. В каком случае более точно названы типы агентов сканирования, используемых в современных системах управления уязвимостями?
42. Что лежит в основе технологии «Domain flux», использующейся для управления бот-сетями?
43. Как можно избежать появления сообщения о конфликте IP-адресов при ARP-спуфинге с использованием ARP-запроса?
44. Какой SSID указывается во фрейме Probe Request при поиске беспроводных сетей методом активного сканирования?
45. Как можно узнать SSID беспроводной сети, настроенной на работу в скрытом режиме?
46. Какое устройство рассылает фреймы Beacon в беспроводных сетях без точки доступа?
47. Какой фрейм можно использовать для принудительного отключения клиента от точки доступа?
48. В каком фрейме передаётся пароль для беспроводной сети с аутентификацией WPA2-PSK?
49. В чём главное отличие ложного сервера RADIUS от штатного, используемого для аутентификации беспроводных клиентов?

## **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: 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> (дата обращения: 16.03.2025). - Режим доступа: по подписке
2. Киренберг А. Г. Системное администрирование и информационная безопасность сетей ЭВМ: учебное пособие: учебное пособие / А. Г. Киренберг. - Системное администрирование и информационная безопасность сетей ЭВМ - Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. - 119 с. - 978-5-00137-292-9. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/128406.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Тарков М. С. Нейрокомпьютерные системы: учебное пособие: учебное пособие / М. С. Тарков. - Нейрокомпьютерные системы - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. - 170 с. - 978-5-4497-3308-5. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/142276.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

#### *Дополнительная литература*

1. Сидоренко В. Г. Аспекты информационной безопасности: учебное пособие: 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> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. 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

### **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://rusneb.ru/> - Национальная электронная библиотека (НЭБ)
3. <https://www.elibrary.ru/> - НЭБ eLIBRARY

### **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**

#### *Учебная аудитория*

- 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;
- Методическими рекомендациями по организации самостоятельной работы студентов МИИГАиК;

### ***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.