***Приложение А***

**(обязательное к рабочей программе дисциплины)**

**Министерство науки и высшего образования Российской Федерации**

**ФГБОУ ВО «Дагестанский государственный технический университет»**

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

**по дисциплине «Моделирование автоматизированных систем в защищённом исполнении»**

Уровень образования — **специалитет**
(бакалавриат/магистратура/специалитет)

Специальность — **10.05.03 Информационная безопасность автоматизированных систем**
(код, наименование специальности)

Специализация — **Безопасность открытых информационных систем**
(наименование)

Разработчик _____ Качаева Г.И.
подпись (ФИО уч. степень, уч. звание)

Фонд оценочных средств обсужден на заседании кафедры ИБиПИ «15_» октября 2025г., протокол № 2

Зав. кафедрой _____ Качаева Г.И.
подпись (ФИО уч. степень, уч. звание)

г. Махачкала 2025

**СОДЕРЖАНИЕ**

## 1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Моделирование автоматизированных систем в защищённом исполнении» и предназначен для контроля и оценки образовательных достижений обучающихся (в т.ч. по самостоятельной работе студентов, далее – СРС), освоивших программу данной дисциплины.

Целью фонда оценочных средств является установление соответствия уровня подготовки обучающихся требованиям ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем.

Рабочей программой дисциплины «Моделирование автоматизированных систем в защищённом исполнении» предусмотрено формирование следующих компетенций:

ПК-11 Способен осуществлять моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации

## 2. Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля)

Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля), и используемые оценочные средства приведены в таблице 1.

*Перечень оценочных средств, рекомендуемых для заполнения таблицы 1 (в ФОС не приводится, используется только для заполнения таблицы)*

- *Эссе*
- *Устный опрос*
- *Вопросы для проведения экзамена*

**2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП**

**Таблица 1**

| Код и наименование формируемой компетенции | Код и наименование индикатора достижения формируемой компетенции | Критерии оценивания | Наименование контролируемых разделов и тем[1] |
|---|---|---|---|
| ПК-11<br>Способен осуществлять моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации | ПК-11.1 применять методы и инструментальные средства моделирования для анализа уязвимостей автоматизированных систем и оценки эффективности применяемых средств и способов защиты информации. | Знать:<br>Классификацию методов моделирования и области их применения для задач анализа защищённости АС. Математические основы моделирования систем защиты информации. Типовые модели угроз и модели нарушителя. Принципы построения моделей каналов утечки информации и процессов функционирования средств защиты. Назначение и функциональные возможности инструментальных средств моделирования.<br>Уметь: Выбирать адекватный метод моделирования для конкретной задачи анализа уязвимостей и оценки эффективности средств защиты. Разрабатывать концептуальные и математические модели фрагментов защищённых АС. Строить модели угроз и модели нарушителя с учётом особенностей объекта информатизации. Использовать инструментальные средства для реализации моделей и проведения вычислительных экспериментов. Интерпретировать промежуточные результаты моделирования.<br>Владеть: Навыками работы с программными средами имитационного и графового моделирования. Методикой формализации задач защиты информации в виде математических моделей. Способностью оценивать адекватность разработанных моделей реальным процессам. Приёмами верификации и валидации моделей. | №№ 1-17 |
| | ПК-11.2 анализировать результаты моделирования, | Знать: Методы анализа и интерпретации результатов моделирования. Показатели эффективности систем защиты | №№ 1-17 |

[1] *Наименования разделов и тем должен соответствовать рабочей программе дисциплины.*

| | | | |
|---|---|---|---|
| | выявлять «узкие места» в системе защиты и разрабатывать рекомендации по повышению уровня защищенности автоматизированных систем на основе проведенных модельных исследований. | информации. Типовые «узкие места» в архитектуре защищённых АС. Подходы к формированию рекомендаций по совершенствованию системы защиты на основе модельных исследований.<br>Уметь: Обрабатывать и анализировать данные, полученные в ходе моделирования. Выявлять закономерности, определять наиболее критичные элементы системы защиты. Оценивать эффективность различных вариантов защиты путём сравнения результатов моделирования. Формулировать обоснованные рекомендации по изменению архитектуры, настроек средств защиты или организационных мер. Документировать результаты анализа и предложения в виде отчётов и презентаций.<br>Владеть: Навыками критической оценки результатов моделирования и их практической значимости. Методами визуализации данных для наглядного представления «узких мест». Способностью обосновывать предлагаемые решения перед руководством и заказчиками. Приёмами оформления технической документации по результатам проведённых исследований. | |

### 2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Моделирование автоматизированных систем в защищённом исполнении» определяется на следующих этапах:

1. **Этап текущих аттестаций** *(Для проведения текущих аттестаций могут быть использованы оценочные средства, указанные в разделе 2*)

2. **Этап промежуточных аттестаций** (*Для проведения промежуточной аттестации могут быть использованы другие оценочные средства*)

**Таблица 2**

| Код и наименование формируемой компетенции | Код и наименование индикатора достижения формируемой компетенции | **Этапы формирования компетенции** | | | | | |
|---|---|---|---|---|---|---|---|
| | | **Этап текущих аттестаций** | | | | | **Этап промежуточной аттестации** |
| | | **1-5 неделя** | **6-10 неделя** | **11-15 неделя** | **1-17 неделя** | | **18-20 неделя** |
| | | Текущая аттестация №1 | Текущая аттестация №2 | Текущая аттестация №3 | СРС | КР/КП | Промежуточная аттестация |
| **1** | | **2** | **3** | **4** | **5** | **6** | **7** |
| ПК-11 Способен осуществлять моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации | ПК-11.1 применять методы и инструментальные средства моделирования для анализа уязвимостей автоматизированных систем и оценки эффективности применяемых средств и способов защиты информации. | Контрольная работа №1 | Контрольная работа №2 | Контрольная работа №3 | | | Вопросы для проведения экзамена |
| | ПК-11.2 анализировать результаты моделирования, выявлять «узкие места» в системе | Контрольная работа №1 | Контрольная работа №2 | Контрольная работа №3 | | | Вопросы для проведения экзамена |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | защиты и разрабатывать рекомендации по повышению уровня защищенности автоматизированных систем на основе проведенных модельных исследований. | | | | | | |

**СРС** – самостоятельная работа студентов;
**КР** – курсовая работа;
**КП** – курсовой проект.

### 2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания

#### 2.2.1. Показатели уровней сформированности компетенций на этапах их формирования

Результатом освоения дисциплины «Моделирование автоматизированных систем в защищённом исполнении» является установление одного из уровней сформированности компетенций: высокий, повышенный, базовый, низкий.

**Таблица 3**

| Уровень | Универсальные компетенции | Общепрофессиональные/ профессиональные компетенции |
|---|---|---|
| Высокий<br>(оценка «отлично», «зачтено») | Сформированы четкие системные знания и представления по дисциплине.<br>Ответы на вопросы оценочных средств полные и верные.<br>Даны развернутые ответы на дополнительные вопросы.<br>Обучающимся продемонстрирован высокий уровень освоения компетенции | Обучающимся усвоена взаимосвязь основных понятий дисциплины, в том числе для решения профессиональных задач.<br>Ответы на вопросы оценочных средств самостоятельны, исчерпывающие, содержание вопроса/задания оценочного средства раскрыто полно, профессионально, грамотно. Даны ответы на дополнительные вопросы.<br>Обучающимся продемонстрирован высокий уровень освоения компетенции |
| Повышенный<br>(оценка «хорошо», «зачтено») | Знания и представления по дисциплине сформированы на повышенном уровне.<br>В ответах на вопросы/задания оценочных средств изложено понимание вопроса, дано достаточно подробное описание ответа, приведены и раскрыты в тезисной форме основные понятия.<br>Ответ отражает полное знание материала, а также наличие, с незначительными пробелами, умений и навыков по изучаемой дисциплине. Допустимы единичные негрубые ошибки.<br>Обучающимся продемонстрирован повышенный уровень освоения компетенции | Сформированы в целом системные знания и представления по дисциплине.<br>Ответы на вопросы оценочных средств полные, грамотные.<br>Продемонстрирован повышенный уровень владения практическими умениями и навыками.<br>Допустимы единичные негрубые ошибки по ходу ответа, в применении умений и навыков |
| Базовый<br>(оценка «удовлетворительно», «зачтено») | Ответ отражает теоретические знания основного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП.<br>Обучающийся допускает неточности в ответе, но обладает необходимыми знаниями для их | Обучающийся владеет знаниями основного материал на базовом уровне.<br>Ответы на вопросы оценочных средств неполные, допущены существенные ошибки.<br>Продемонстрирован базовый уровень владения |

| Уровень | Универсальные компетенции | Общепрофессиональные/ профессиональные компетенции |
|---|---|---|
| | устранения.<br>Обучающимся продемонстрирован базовый уровень освоения компетенции | практическими умениями и навыками, соответствующий минимально необходимому уровню для решения профессиональных задач |
| Низкий<br>(оценка «неудовлетворительно», «не зачтено») | Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие практических умений и навыков | |

Показатели уровней сформированности компетенций могут быть изменены, дополнены и адаптированы к конкретной рабочей программе дисциплины.

### 2.2.2. Описание шкал оценивания

В ФГБОУ ВО «ДГТУ» внедрена модульно-рейтинговая система оценки учебной деятельности студентов. В соответствии с этой системой применяются пятибальная, двадцатибальная и стобальная шкалы знаний, умений, навыков.

| **Шкалы оценивания** | | | **Критерии оценивания** |
|---|---|---|---|
| пятибальная | двадцатибальная | стобальная | |
| «Отлично» - 5 баллов | «Отлично» - 18-20 баллов | «Отлично» - 85 – 100 баллов | Показывает высокий уровень сформированности компетенций, т.е.:<br>– продемонстрирует глубокое и прочное усвоение материала;<br>– исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал;<br>– правильно формирует определения;<br>– демонстрирует умения самостоятельной работы с нормативно-правовой литературой;<br>– умеет делать выводы по излагаемому материалу. |
| «Хорошо» - 4 баллов | «Хорошо» - 15 - 17 баллов | «Хорошо» - 70 - 84 баллов | Показывает достаточный уровень сформированности компетенций, т.е.:<br>– демонстрирует достаточно полное знание материала, основных теоретических положений;<br>– достаточно последовательно, грамотно логически стройно излагает материал;<br>– демонстрирует умения ориентироваться в нормальной литературе;<br>– умеет делать достаточно обоснованные выводы по излагаемому материалу. |
| «Удовлетворительно» - 3 баллов | «Удовлетворительно» - 12 - 14 баллов | «Удовлетворительно» - 56 – 69 баллов | Показывает пороговый уровень сформированности компетенций, т.е.:<br>– демонстрирует общее знание изучаемого материала;<br>– испытывает серьезные затруднения при ответах на дополнительные вопросы;<br>– знает основную рекомендуемую литературу;<br>– умеет строить ответ в соответствии со структурой излагаемого материала. |
| «Неудовлетворительно» - 2 баллов | «Неудовлетворительно» - 1-11 баллов | «Неудовлетворительно» - 1-55 баллов | Ставится в случае:<br>– незнания значительной части программного материала;<br>– не владения понятийным аппаратом дисциплины;<br>– допущения существенных ошибок при изложении учебного материала;<br>– неумение строить ответ в соответствии со структурой излагаемого вопроса;<br>– неумение делать выводы по излагаемому материалу. |

## 3. Типовые контрольные задания, иные материалы и методические рекомендации, необходимые для оценки сформированности компетенций в процессе освоения ОПОП

### 3.1. Задания и вопросы для входного контроля

1. Дайте определение автоматизированной системы (АС). Назовите основные компоненты АС.
2. Что такое уязвимость информационной системы? Приведите примеры типовых уязвимостей.
3. Какие угрозы информационной безопасности наиболее характерны для современных вычислительных сетей?
4. Что такое модель угроз и для чего она разрабатывается?
5. Какие существуют модели разграничения доступа (дискреционная, мандатная, ролевая)? Опишите их.
6. Что такое криптографическая защита и для решения каких задач она применяется?
7. Перечислите основные протоколы защищённого сетевого взаимодействия (VPN, TLS/SSL, IPSec).
8. Какие средства защиты информации от несанкционированного доступа вы знаете?
9. Что такое политика безопасности и какие разделы она обычно включает?
10. Назовите известные вам программные средства для моделирования сетей и систем.

### 3.2. Оценочные средства и критерии сформированности компетенций

#### 3.2.1. Аттестационная контрольная работа №1

1. Дайте определение модели и моделирования. Какие цели преследует моделирование защищённых АС?
2. Перечислите основные виды моделирования (натурное, физическое, математическое, имитационное). Охарактеризуйте каждый вид.
3. Что такое концептуальная модель? Какие этапы включает процесс концептуального моделирования?
4. Какие математические теории лежат в основе моделирования систем защиты информации (теория вероятностей, теория массового обслуживания, теория графов, теория игр)?
5. Опишите общий подход к построению модели угроз информационной безопасности автоматизированной системы.
6. Какие факторы учитываются при разработке модели нарушителя? Приведите классификацию нарушителей.
7. Что такое дерево атак (attack tree) и как оно используется для моделирования угроз?
8. В чём отличие качественных и количественных методов оценки рисков? Как модели могут помочь в количественной оценке?
9. Какие требования предъявляются к модели, используемой для анализа уязвимостей?
10. Приведите пример концептуальной модели защищённой АС (основные элементы и связи).

#### 3.2.3. Аттестационная контрольная работа №2

1. Какие параметры характеризуют нарушителя в модели? Как задаются его возможности?
2. Опишите метод аналитического моделирования для оценки времени преодоления рубежей защиты.
3. Каковы основные этапы имитационного моделирования процессов функционирования средств защиты информации?
4. Что такое событийный подход в имитационном моделировании? Приведите пример.

5. Какие вероятностные распределения чаще всего используются для описания потоков событий в системах защиты?
6. Как оценить вероятность обнаружения атаки с помощью вероятностной модели?
7. Что такое граф атак (attack graph) и для чего он строится?
8. Как с помощью графовой модели можно найти кратчайший путь реализации угрозы?
9. Какие метрики защищённости можно вычислить на основе графовой модели (например, метрики на основе теории графов)?
10. Приведите пример использования метода Монте-Карло для оценки эффективности системы защиты.

### 3.2.4. Аттестационная контрольная работа №3

1. Как формализуются политики безопасности (дискреционная, мандатная, ролевая) в моделях управления доступом?
2. Какие инструментальные средства моделирования защищённых АС вы знаете? Опишите одно из них.
3. Каковы основные этапы проведения вычислительного эксперимента по оценке защищённости АС?
4. Какие показатели эффективности системы защиты можно получить в результате моделирования?
5. Как осуществляется обработка и статистический анализ результатов имитационного эксперимента?
6. Что понимается под «узкими местами» системы защиты? Как их выявить по результатам моделирования?
7. Как моделируются каналы утечки информации (например, акустический, ПЭМИН)? Какие параметры учитываются?
8. Каким образом результаты моделирования используются для обоснования выбора средств защиты?
9. Что такое оценка рисков на основе моделей? Приведите пример расчёта риска.
10. Как проверить адекватность разработанной модели реальной системе?

## 3.3. Список вопросов к экзамену

1. Понятие моделирования, цели и задачи моделирования защищённых АС.
2. Классификация видов моделирования (натурное, физическое, математическое, имитационное).
3. Концептуальное моделирование: этапы, требования к концептуальной модели.
4. Математические основы моделирования систем защиты информации (теория вероятностей, ТМО, теория графов).
5. Моделирование угроз информационной безопасности: подходы, этапы.
6. Модель нарушителя: классификация, характеристики, способы задания.
7. Деревья атак (attack trees): построение, анализ, применение.
8. Аналитические модели оценки уязвимостей: достоинства, ограничения, примеры.
9. Имитационное моделирование процессов защиты информации: общая схема, этапы.
10. Дискретно-событийное имитационное моделирование: основные понятия.
11. Вероятностные модели оценки эффективности средств защиты: показатели, методы расчёта.
12. Метод Монте-Карло в задачах анализа защищённости.
13. Графовые модели анализа защищённости компьютерных сетей.
14. Графы атак (attack graphs): построение, алгоритмы анализа.
15. Метрики защищённости на основе графовых моделей.
16. Моделирование политик безопасности: формальные модели (HRU, BLP, Biba).
17. Ролевое управление доступом (RBAC): модель и её анализ.
18. Инструментальные средства моделирования защищённых АС (обзор, возможности).

19. Среда имитационного моделирования (например, GPSS, AnyLogic) для задач ИБ.
20. Планирование вычислительного эксперимента по оценке защищённости.
21. Обработка и интерпретация результатов моделирования.
22. Выявление «узких мест» системы защиты на основе модельных исследований.
23. Моделирование каналов утечки информации (акустических, виброакустических, ПЭМИН).
24. Оценка рисков информационной безопасности с использованием моделей.
25. Применение результатов моделирования для обоснования проектных решений.
26. Верификация и валидация моделей систем защиты информации.
27. Моделирование процессов обнаружения компьютерных атак.
28. Моделирование систем контроля и управления доступом (СКУД).
29. Перспективные направления развития технологий моделирования защищённых АС.
30. Примеры практического использования моделирования для повышения уровня защищённости.

### 3.4. Вопросы по остаточным знаниям

1. Дайте определение моделирования. Для каких целей оно применяется при создании защищённых автоматизированных систем?
2. Перечислите основные виды моделирования, используемые для анализа уязвимостей.
3. Что такое модель угроз и модель нарушителя? Какие элементы они включают?
4. Опишите суть имитационного моделирования и приведите пример его применения в области ИБ.
5. Как графовые модели (деревья атак, графы атак) помогают выявлять пути реализации угроз?
6. Какие вероятностные методы используются для оценки эффективности систем защиты?
7. Какие инструментальные средства моделирования защищённых АС вам известны?
8. Как на основе результатов моделирования можно определить «узкие места» системы защиты?
9. Каким образом результаты моделирования помогают обосновать выбор средств и способов защиты?
10. В чём заключается оценка рисков информационной безопасности и как модели могут быть использованы для её проведения?

Зачеты и экзамены могут быть проведены в письменной форме, а также в письменной форме с устным дополнением ответа. Зачеты служат формой проверки качества выполнения студентами лабораторных работ, усвоения семестрового учебного материала по дисциплине (модулю), практических и семинарских занятий (при отсутствии экзамена по дисциплине).

По итогам зачета, соответствии с модульно – рейтинговой системой университета, выставляются баллы с последующим переходом по шкале баллы – оценки за зачет, выставляемый как по наименованию «зачтено», «не зачтено», так и дифференцированно т.е. с выставлением отметки по схеме – «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно», определяемое решением Ученого совета университета и прописываемого в учебном плане.

Экзамен по дисциплине (модулю) служит для оценки работы студента в течении семестра (года, всего срока обучения и др.) и призван выявить уровень, качество и систематичность полученных им теоретических и практических знаний, приобретения навыков самостоятельной работы, развития творческого мышления, умения синтезировать полученные знания и применять их в решении практических задач. По итогам экзамена, в соответствии с модульно – рейтинговой системой университета выставляются баллы, с последующим переходом по шкале оценок на оценки: «отлично», «хорошо»,

«удовлетворительно» и «неудовлетворительно», свидетельствующие о приобретенных компетенциях или их отсутствии.

Критерии оценки уровня сформированности компетенций по результатам проведения зачета:

- оценка «зачтено»: обучающийся демонстрирует всестороннее, систематическое и глубокое знание материала, свободно выполняет задания, предусмотренные программой дисциплины, усвоивший основную и дополнительную литературу. Обучающийся выполняет задания, предусмотренные программой дисциплины, на уровне не ниже базового;

- оценка «не зачтено»: обучающийся демонстрирует незнание материала, не выполняет задания, предусмотренные программой дисциплины. Обучающийся не выполняет задания, предусмотренные программой дисциплины, на уровне ниже базового. Дальнейшее освоение ОПОП не возможно без дополнительного изучения материала и подготовки к зачету.

Критерии оценки уровня сформированности компетенций по результатам проведения дифференцированного зачёта (зачета с оценкой) / экзамена:

- оценка **«отлично»:** обучающийся дал полный, развернутый ответ на поставленный вопрос, проявил совокупность осознанных знаний об объекте, доказательно раскрыл основные положения темы. В ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, явлений. Обучающийся подкрепляет теоретический ответ практическими примерами. Ответ сформулирован научным языком, обоснована авторская позиция обучающегося. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа или с помощью «наводящих» вопросов преподавателя. Обучающимся продемонстрирован высокий уровень владения компетенцией(-ями);

- оценка **«хорошо»:** обучающимся дан полный, развернутый ответ на поставленный вопрос, проявлено умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, но есть недочеты в формулировании понятий, решении задач. При ответах на дополнительные вопросы допущены незначительные ошибки. Обучающимся продемонстрирован повышенный уровень владения компетенцией(-ями);

- оценка **«удовлетворительно»:** обучающимся дан неполный ответ на вопрос, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, явлений, нарушена логика ответа, не сделаны выводы. Речевое оформление требует коррекции. Обучающийся испытывает затруднение при ответе на дополнительные вопросы. Обучающимся продемонстрирован базовый уровень владения компетенцией(-ями);

- оценки **«неудовлетворительно»:** обучающийся испытывает значительные трудности в ответе на вопрос, допускает существенные ошибки, не владеет терминологией, не знает основных понятий, не может ответить на «наводящие» вопросы преподавателя. Обучающимся продемонстрирован низкий уровень владения компетенцией(-ями).