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 «Обеспечение информационной безопасности в информационных сетях»

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

для направления **11.03.01 Радиотехника**
(код, наименование направления подготовки/специальности)

по специализации **Радиотехнические средства передачи, приема и обработки сигналов**
(наименование)

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

Фонд оценочных средств обсужден на заседании кафедры РТиМ
« 03 » 09 20 19 г., протокол № 1

Зав. кафедрой _____ Гаджиев Х.Ш.
подпись (ФИО уч. степень, уч. звание)

СОДЕРЖАНИЕ

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины Обеспечение информационной безопасности в информационных сетях 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 направлению 11.03.01 Радиотехника.

Рабочей программой дисциплины Обеспечение информационной безопасности в информационных сетях предусмотрено формирование следующей компетенции:

ПК-1. Способен выполнять математическое моделирование объектов и процессов по типовым методикам, в том числе с использованием стандартных пакетов прикладных программ.

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)

- *Контрольная работа*
- *Устный опрос*
- *Вопросы для проведения экзамена*

Перечень оценочных средств при необходимости может быть дополнен.

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-1. Способен выполнять математическое моделирование объектов и процессов по типовым методикам, в том числе с использованием стандартных пакетов прикладных программ	ПК-1.1. Умеет строить физические и математические модели моделей, узлов, блоков радиотехнических устройств и систем ПК-1.2. Владеет навыками компьютерного моделирования	знать: - методологические и технологические основы комплексного обеспечения безопасности АС, - угрозы и методы нарушения безопасности АС, - формальные модели, лежащие в основе систем защиты АС, - стандарты по оценке защищенности АС и их теоретические основы, - методы и средства реализации защищенных АС, - методы и средства верификации и анализа надежности защищенных АС; уметь: - проводить анализ АС с точки зрения обеспечения компьютерной безопасности, - разрабатывать модели и политику безопасности, используя известные под-ходы, методы, средства и их теоретические основы, - применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС, - реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС; владеть навыками: - работы с АС распределенных вычислений и обработки информации; - работы с документацией АС, - использования критериев оценки защищенности АС, - построения формальных моделей систем защиты информации АС.	№№1-9

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине Обеспечение информационной безопасности в информационных сетях 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	Код и наименование индикатора	**Этапы формирования компетенции**

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

формируемой компетенции	достижения формируемой 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-1. Способен выполнять математическое моделирование объектов и процессов по типовым методикам, в том числе с использованием стандартных пакетов прикладных программ	ПК-1.1. Умеет строить физические и математические модели моделей, узлов, блоков радиотехнических устройств и систем	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ПК-1.2. Владеет навыками компьютерного моделирования	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос

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 Обеспечение информационной безопасности в информационных сетях является установление одного из уровней сформированности компетенций: высокий, повышенный, базовый, низкий.

Таблица 3

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
Высокий (оценка «отлично», «зачтено»)	Сформированы четкие системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные и верные. Даны развернутые ответы на дополнительные	Обучающимся усвоена взаимосвязь основных понятий дисциплины, в том числе для решения профессиональных задач. Ответы на вопросы оценочных средств самостоятельны, исчерпывающие, содержание

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
	вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции	вопроса/задания оценочного средства раскрыто полно, профессионально, грамотно. Даны ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции
Повышенный (оценка «хорошо», «зачтено»)	Знания и представления по дисциплине сформированы на повышенном уровне. В ответах на вопросы/задания оценочных средств изложено понимание вопроса, дано достаточно подробное описание ответа, приведены и раскрыты в тезисной форме основные понятия. Ответ отражает полное знание материала, а также наличие, с незначительными пробелами, умений и навыков по изучаемой дисциплине. Допустимы единичные негрубые ошибки. Обучающимся продемонстрирован повышенный уровень освоения компетенции	Сформированы в целом системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные, грамотные. Продемонстрирован повышенный уровень владения практическими умениями и навыками. Допустимы единичные негрубые ошибки по ходу ответа, в применении умений и навыков
Базовый (оценка «удовлетворительно», «зачтено»)	Ответ отражает теоретические знания основного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП. Обучающийся допускает неточности в ответе, но обладает необходимыми знаниями для их устранения. Обучающимся продемонстрирован базовый уровень освоения компетенции	Обучающийся владеет знаниями основного материал на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продемонстрирован базовый уровень владения практическими умениями и навыками, соответствующий минимально необходимому уровню для решения профессиональных задач
Низкий (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.: – продемонстрирует глубокое и прочное усвоение материала; – исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; – правильно формирует определения; – демонстрирует умения самостоятельной работы с нормативно-правовой литературой; – умеет делать выводы по излагаемому материалу.
«Хорошо» - 4 баллов	«Хорошо» - 15 - 17 баллов	«Хорошо» - 70 - 84 баллов	Показывает достаточный уровень сформированности компетенций, т.е.: – демонстрирует достаточно полное знание материала, основных теоретических положений; – достаточно последовательно, грамотно логически стройно излагает материал; – демонстрирует умения ориентироваться в нормальной литературе; – 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.: – демонстрирует общее знание изучаемого материала; – испытывает серьезные затруднения при ответах на дополнительные вопросы; – знает основную рекомендуемую литературу; – умеет строить ответ в соответствии со структурой излагаемого материала.
«Неудовлетворительно» - 2 баллов	«Неудовлетворительно» - 1-11 баллов	«Неудовлетворительно» - 1-55 баллов	Ставится в случае: – незнания значительной части программного материала; – не владения понятийным аппаратом дисциплины; – допущения существенных ошибок при изложении учебного материала; – неумение строить ответ в соответствии со структурой излагаемого вопроса; – 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. Понятие информации.
2. Система управления информационной безопасностью.
3. Политика информационной безопасности.
4. Инфраструктура информационной безопасности.
5. Физическая безопасность и безопасность окружающей среды.
6. Управление доступом к системам.

3.2.1. Аттестационная контрольная работа №1

3. Основные понятия информационной безопасности.
4. Автоматизированная система обработки информации. Представление информации в АС.
5. Базовые свойства информации
6. Допуск к информации. Базовые понятия
7. Определение угрозы безопасности для АС. Противодействие угрозам безопасности
8. Классификация возможных угроз информационной безопасности АС. Важные свойства информации и систем ее обработки.
9. Уровни доступа к информации. Анализ угроз информационной безопасности.
10. Базовая эталонная модель взаимодействия открытых систем
11. Протокол. Сеть как набор протоколов
12. Стек протоколов TCP/IP. Соответствие уровней стека TCP/IP уровням модели OSI.
13. IP адресация. Классы IP сетей. Характеристики классов IP-адресов. Выделенные IP-адреса.

3.2.2. Аттестационная контрольная работа №2

1. Шлюзы и мосты. Маска подсети. Подсети ? первый бастион защиты.
2. Интернет протоколы: Протокол пересылки файлов FTP; Протокол Telnet; Протокол SNMP; Протокол SMTP; Сетевая файловая система NFS; Протокол передачи гипертекста (HTTP); Сервис DNS.
3. Схема инкапсуляции данных в стеке протоколов TCP/IP. ARP-таблица.
4. Проблемы безопасности IP-сетей. Угрозы безопасности IP-сетей. Анализ угроз сетевой безопасности.
5. Сетевые атаки: Подслушивание; Изменение данных; Анализ сетевого трафика; Подмена доверенного субъекта; Посредничество; Атака man-in-the-middle; Перехват сеанса; Парольные атаки; Угадывание ключа; Атаки на уровне приложений; Отказ в обслуживании (Denial of Service, DoS); Сетевая разведка; Злоупотребление доверием.
6. Угрозы и уязвимости проводных корпоративных информационных систем.
7. Угрозы и уязвимости беспроводных сетей. Точки доступа в беспроводных сетях. Вещание радиомаяка.

3.2.3. Аттестационная контрольная работа №3

1. Способы обеспечения информационной безопасности. Комплексный подход. Необходимость применения стандартов
2. Криптография. Шифрование с закрытым ключом. Понятие диффузии и конфузии. Структура алгоритма симметричного шифрования. Криптоанализ. Используемые критерии при разработке алгоритмов. Сеть Фейштеля. Понятие слабого ключа.
3. Асимметричное шифрование. Основные принципы построения криптосистем с открытым ключом. Основные алгоритмы построения систем с открытым ключом.
4. Электронная цифровая подпись. Цель аутентификации электронных документов. Формат электронной цифровой подписи. Хэш-функция. Одно направленные Хэш-функции. Основы построения хэш-функций.

3.2.4. Список вопросов к экзамену

1. Основные понятия информационной безопасности.
2. Автоматизированная система обработки информации. Представление информации в АС.
3. Базовые свойства информации
4. Допуск к информации. Базовые понятия
5. Определение угрозы безопасности для АС. Противодействие угрозам безопасности
6. Классификация возможных угроз информационной безопасности АС. Важные свойства информации и систем ее обработки.
7. Уровни доступа к информации. Анализ угроз информационной безопасности.
8. Базовая эталонная модель взаимодействия открытых систем
9. Протокол. Сеть как набор протоколов
10. Стек протоколов TCP/IP. Соответствие уровней стека TCP/IP уровням модели OSI.
11. IP адресация. Классы IP сетей. Характеристики классов IP-адресов. Выделенные IP-адреса.
12. Шлюзы и мосты. Маска подсети. Подсети ? первый бастион защиты.
13. Интернет протоколы: Протокол пересылки файлов FTP; Протокол Telnet; Протокол SNMP; Протокол SMTP; Сетевая файловая система NFS; Протокол передачи гипертекста (HTTP); Сервис DNS.
14. Схема инкапсуляции данных в стеке протоколов TCP/IP. ARP-таблица.
15. Проблемы безопасности IP-сетей. Угрозы безопасности IP-сетей. Анализ угроз сетевой безопасности.
16. Сетевые атаки: Подслушивание; Изменение данных; Анализ сетевого трафика; Подмена доверенного субъекта; Посредничество; Атака man-in-the-middle; Перехват сеанса; Парольные атаки; Угадывание ключа; Атаки на уровне приложений; Отказ в обслуживании (Denial of Service, DoS); Сетевая разведка; Злоупотребление доверием.
17. Угрозы и уязвимости проводных корпоративных информационных систем.
18. Угрозы и уязвимости беспроводных сетей. Точки доступа в беспроводных сетях. Вещание радиомаяка.
19. Способы обеспечения информационной безопасности. Комплексный подход. Необходимость применения стандартов
20. Криптография. Шифрование с закрытым ключом. Понятие диффузии и конфузии. Структура алгоритма симметричного шифрования. Криптоанализ. Используемые критерии при разработке алгоритмов. Сеть Фейштеля. Понятие слабого ключа.
21. Асимметричное шифрование. Основные принципы построения криптосистем с открытым ключом. Основные алгоритмы построения систем с открытым ключом.
22. Электронная цифровая подпись. Цель аутентификации электронных документов. Формат электронной цифровой подписи. Хэш-функция. Одно направленные Хэш-функции. Основы построения хэш-функций.
23. Технологии межсетевых экранов. Функции МЭ. Классификация МЭ. Фильтрация трафика. Критерии анализа информационного потока. Выполнение функций посредничества. Способы разграничения доступа к ресурсам внешней/внутренней сети. Кэширование данных. Особенности функционирования МЭ на различных уровнях модели OSI. Варианты исполнения МЭ. Схемы сетевой защиты на базе МЭ. Формирование политики межсетевого взаимодействия. Основные схемы подключения МЭ. Персональные и распределенные сетевые экраны. Проблемы безопасности МЭ.
24. Виртуальные защищенные сети (VPN). Туннель VPN. VPN-клиент. VPN-сервер. Шлюз безопасности VPN. Варианты построения виртуальных защищенных каналов. Достоинства применения технологии VPN. Протоколы формирования защищенных каналов на канальном уровне. Протоколы формирования защищенных каналов на сеансовом уровне. 25. Защита беспроводных сетей.
25. Физический уровень стандарта IEE 802.11. Стандарт WPA.
26. Защита на сетевом уровне. Протокол IPSec. Архитектура средств безопасности IPSec. Защита передаваемых данных с помощью протоколов AH и ESP. Протокол AH.

Протокол инкапсулирующей защиты ESP. Алгоритмы аутентификации и шифрования в IPSec. Структура алгоритма HMAC. Протокол управления криптоключами IKE. Установление безопасной ассоциации SA. Базы данных SAD и SPD. Основные схемы применения IPSec.

27. Инфраструктура защиты на прикладном уровне. Управление идентификацией и доступом. Особенности управления доступом. Функционирование системы управления доступом. Средства управления сетевым доступом. Средства управления Web-доступом. Организация защищенного удаленного доступа. Протоколы аутентификации удаленных пользователей. Централизованный контроль удаленного доступа на примере TACACS.
28. Концепция адаптивного управления безопасностью. Этапы осуществления атаки на информационную систему. Концепция адаптивного управления безопасностью. Обнаружение атак. Адаптивный компонент. Модель адаптивной безопасности сети. Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности ОС. Методы анализа сетевой информации. Классификация систем обнаружения атак. Системы обнаружения атак. Методы реагирования.
29. Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусов. Жизненный цикл вирусов. Вредоносные программы других типов. Антивирусные программы и комплексы. Внешние признаки деятельности вирусов. Методы обнаружения вирусов. Виды антивирусных программ. Критерии качества антивирусной программы. Профилактические меры защиты. Построение системы антивирусной защиты корпоративной сети.
30. Задачи управления системой сетевой безопасности. Архитектура управления средствами сетевой безопасности. Концепция глобального управления безопасностью. Глобальная политика безопасности. Локальная политика безопасности.
31. Требования по защите информации от несанкционированного доступа для автоматизированных систем.
32. Комплексный подход к защите информации. Средства защиты информации.
33. DLP ? системы.

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.

Критерии оценки уровня сформированности компетенций для проведения экзамена/дифференцированного зачёта (зачета с оценкой) зависят от их форм проведения (тест, вопросы, задания, решение задач и т.д.).