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 **магистр**
(бакалавриат/магистратура/специалитет)

для программы магистратуры **11.04.01 Радиотехника**
(код, наименование направления подготовки/специальности)

по профилю **Системы и устройства 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
« 05 » сентября 2022 г., протокол № 1

Зав. кафедрой _____ _____
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 программе магистратуры 11.04.01 Радиотехника.

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

ОПК-3 - Способен приобретать и использовать новую информацию в своей предметной области, предлагать новые идеи и подходы к решению инженерных задач;

ОПК–4 - Способен разрабатывать и применять специализированное программно-математическое обеспечение для проведения исследований и решения инженерных задач.

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]
ОПК-3 - Способен приобретать и использовать новую информацию в своей предметной области, предлагать новые идеи и подходы к решению инженерных задач	ОПК-3.1. Знает принципы построения локальных и глобальных компьютерных сетей, основы Интернет-технологий, типовые процедуры применения проблемно-ориентированных прикладных программных средств в дисциплинах профессионального цикла и профессиональной сфере деятельности ОПК-3.2. Умеет использовать современные информационные и компьютерные технологии, средства коммуникаций, способствующие повышению эффективности научной и образовательной сфер деятельности ОПК-3.3. Владеет методами Математического моделирования радиотехнических устройств и систем, технологических процессов с использованием современных информационных технологий	Знать: принципы построения локальных и глобальных компьютерных сетей, основы Интернет-технологий, типовые процедуры применения проблемно-ориентированных прикладных программных средств в дисциплинах профессионального цикла и профессиональной сфере деятельности Уметь: использовать современные информационные и компьютерные технологии, средства коммуникаций, способствующие повышению эффективности научной и образовательной сфер деятельности Владеть методами: Математического моделирования радиотехнических устройств и систем, технологических процессов с использованием современных информационных технологий	№№1-9
ОПК – 4 - Способен разрабатывать и применять специализированное программно-математическое обеспечение для	ОПК-4.1. Знает методы расчета, проектирования, конструирования и модернизации радиотехнических устройств и систем с использованием систем автоматизированного проектирования и компьютерных средств	Знать: методы расчета, проектирования, конструирования и модернизации радиотехнических устройств и систем с использованием систем автоматизированного проектирования и компьютерных средств Уметь: осуществлять выбор наиболее оптимальных прикладных программных пакетов	№№1-9

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

проведения исследований и решения инженерных задач	ОПК-4.2. Умеет осуществлять выбор наиболее оптимальных прикладных программных пакетов для решения соответствующих задач научной и образовательной деятельности ОПК-4.3. Владеет современными программными средствами моделирования, оптимального проектирования и конструирования радиотехнических устройств и систем различного функционального назначения	для решения соответствующих задач научной и образовательной деятельности Владеть: современными программными средствами моделирования, оптимального проектирования и конструирования радиотехнических устройств и систем различного функционального назначения	

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 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**
ОПК-3 - Способен приобретать и использовать новую информацию в своей предметной области, предлагать новые	ОПК-3.1. Знает принципы построения локальных и глобальных компьютерных сетей, основы Интернет-технологий, типовые процедуры применения	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос

идеи и подходы к решению инженерных задач	проблемно-ориентированных прикладных программных средств в дисциплинах профессионального цикла и профессиональной сфере деятельности						
	ОПК-3.2. Умеет использовать современные информационные и компьютерные технологии, средства коммуникаций, способствующие повышению эффективности научной и образовательной сфер деятельности	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ОПК-3.3. Владеет методами Математического моделирования радиотехнических устройств и систем, технологических процессов с использованием современных информационных технологий	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
ОПК – 4 - Способен разрабатывать и применять специализированное программно-математическое обеспечение для проведения исследований и решения инженерных задач	ОПК-4.1. Знает методы расчета, проектирования, конструирования и модернизации радиотехнических устройств и систем с использованием систем автоматизированного проектирования и компьютерных средств	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ОПК-4.2. Умеет осуществлять выбор наиболее оптимальных прикладных	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос

	программных пакетов для решения соответствующих задач научной и образовательной деятельности						
	ОПК-4.3. Владеет современными программными средствами моделирования, оптимального проектирования и конструирования радиотехнических устройств и систем различного функционального назначения	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 вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции	Обучающимся усвоена взаимосвязь основных понятий дисциплины, в том числе для решения профессиональных задач. Ответы на вопросы оценочных средств самостоятельны, исчерпывающие, содержание вопроса/задания оценочного средства раскрыто полно, профессионально, грамотно. Даны ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции
Повышенный	Знания и представления по дисциплине	Сформированы в целом системные знания и

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
(оценка «хорошо», «зачтено»)	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	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. Оценочные средства и критерии сформированности компетенций

3.2.1. Аттестационная контрольная работа №1

1. Свойства информационной безопасности
2. Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности
3. Криптографические методы
4. Шифрование. Кодирование. Стеганография. Сжатие
5. Математика криптографии
6. Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение
7. Традиционные шифры перестановки. Одно и двух направленные. Поточные и блочные шифры.

3.2.2. Аттестационная контрольная работа №2

1. Механизация шифрования. Традиционные шифры замены
2. Шифры замены. Шифры многоалфавитной замены. Частотность символов
3. Криптоанализ
4. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста
5. Компьютерное шифрование. Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей.
6. Симметричное шифрование
7. Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES
8. Усовершенствованный стандарт шифрования AES. Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES.

3.2.3. Аттестационная контрольная работа №3

1. Российские стандарты симметричного шифрования. Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015
2. Проблема распределения ключей симметричного шифрования
3. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos
4. Асимметричное шифрование
5. Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках. Возведение в степень и логарифмы
6. Криптографическая система Эль-Гамаля. Криптосистемы на основе метода эллиптических кривых. ЭЦП.
7. Российские стандарты асимметричного шифрования. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012.
8. Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа
9. Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители

3.2.4. Список вопросов к экзамену

1. Свойства информационной безопасности
2. Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности
3. Криптографические методы
4. Шифрование. Кодирование. Стеганография. Сжатие
5. Математика криптографии
6. Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение
7. Традиционные шифры перестановки. Одно и двух направленные. Поточные и блочные шифры
8. Механизация шифрования. Традиционные шифры замены
9. Шифры замены. Шифры многоалфавитной замены. Частотность символов
10. Криптоанализ
11. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста
12. Компьютерное шифрование. Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей.
13. Симметричное шифрование
14. Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES
15. Усовершенствованный стандарт шифрования AES. Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES
16. Российские стандарты симметричного шифрования. Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015
17. Проблема распределения ключей симметричного шифрования
18. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos
19. Асимметричное шифрование
20. Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках. Возведение в степень и логарифмы
21. Криптографическая система Эль-Гамаля. Криптосистемы на основе метода эллиптических кривых. ЭЦП
22. Российские стандарты асимметричного шифрования. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012.
23. Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа
24. Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители.

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.).

	программно-математическое обеспечение для проведения исследований и решения инженерных задач	и модернизации радиотехнических устройств и систем с использованием систем автоматизированного проектирования и компьютерных средств
		ОПК-4.2. Умеет осуществлять выбор наиболее оптимальных прикладных программных пакетов для решения соответствующих задач научной и образовательной деятельности
		ОПК-4.3. Владеет современными программными средствами моделирования, оптимального проектирования и конструирования радиотехнических устройств и систем различного функционального назначения

4. Объем и содержание дисциплины (модуля)

Форма обучения	**очная**	**очно-заочная**	**заочная**
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	4/144		
Семестр	2		
Лекции, час	17		
Практические занятия, час	17		
Лабораторные занятия, час	-		
Самостоятельная работа, час	74		
Курсовой проект (работа), РГР, семестр	-		
Зачет (при заочной форме **4 часа** отводится на контроль)	-		
Часы на экзамен (при очной, очно-заочной формах **1 ЗЕТ – 36 часов**, при заочной форме **9 часов** отводится на контроль)	1 зет =36ч		

Форма промежуточной аттестации (по семестрам)	экзамен				Зачет/ зачет с оценкой/ экзамен				экзамен			
Итого	17	17	-	74								

К видам учебной работы в вузе отнесены: лекции, консультации, семинары, практические занятия, лабораторные работы, контрольные работы, коллоквиумы, самостоятельные работы, научно- исследовательская работа, практики, курсовое проектирование (курсовая работа). Вуз может устанавливать другие виды учебных занятий.

** - Разделы, тематику и вопросы по дисциплине следует разделить на три текущие аттестации в соответствии со сроками проведения текущих аттестаций. По материалу программы, пройденному студентом после завершения 3-ей аттестации до конца семестра (2-3 недели), контроль успеваемости осуществляется при сдаче зачета или экзамена.*

4.2. Содержание практических занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного (практического, семинарского) занятия	Количество часов			Рекомендуемая литература и методические разработки (№ источника из списка литературы)
			Очно	Очно-заочно	Заочно	
1	**2**	**3**	**4**	**5**	**6**	**7**
1.	1-2	Стеганографические методы скрытия информации	2			№№ 1-15
2.	1-4	Бинарная арифметика. Модульная арифметика	2			№№ 1-15
3.	1-5	Применение методов шифрования перестановкой. Применение методов шифрования заменой	2			№№ 1-15
4.	1-6	Применение методов шифрования многоалфавитной замены	2			№№ 1-15
5.	1-7	Криптоанализ методов перестановки. Криптоанализ методов замены	2			№№ 1-15
6.	1-8	Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа	1			№№ 1-15
7.	1-9	Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители	2			№№ 1-15
ИТОГО			**17**			