

(обязательное к рабочей программе дисциплины)

Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Защита информации»

Уровень образования

бакалавриат

(бакалавриат/магистратура/специалитет)

для направления

09.03.01 Информатика и вычислительная техника

(код, наименование направления подготовки/специальности)

по профилю

Вычислительные машины, комплексы, системы и
сети

(наименование)

Разработчик



подпись

Качаева Г.И., к.э.н.

(ФИО уч. степень, уч. звание)

Фонд оценочных средств обсужден на заседании кафедры УиТСиВТ
«12» сентября 2019г., протокол №1

Зав. кафедрой



подпись

Асланов Т.Г., к.т.н.

(ФИО уч. степень, уч. звание)

СОДЕРЖАНИЕ

1. Область применения, цели и задачи фонда оценочных средств.....	17
2. Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля)	17
2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП .	18
2.1.2. Этапы формирования компетенций.....	20
2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания.....	23
2.2.1. Показатели уровней сформированности компетенций на этапах их формирования	23
2.2.2. Описание шкал оценивания.....	25
3. Типовые контрольные задания, иные материалы и методические рекомендации, необходимые для оценки сформированности компетенций в процессе освоения ОПОП.....	26
3.1. Задания и вопросы для входного контроля.....	26
3.2. Оценочные средства и критерии сформированности компетенций.....	26
3.2.1. Аттестационная контрольная работа №1	26
3.2.2. Список вопросов к зачету	26

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины Защита информации 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 09.03.01 Информатика и вычислительная техника.

Рабочей программой дисциплины Защита информации предусмотрено формирование следующей компетенции:

ОПК -2 Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решения задач профессиональной деятельности;

ОПК – 3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ОПК – 4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью.

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 -2 Способен понимать принципы работы современных информационных технологий и программных средств, в том числе	ОПК-2.1. Знать: современные информационные технологии и программные средства, в том числе	Знать принципы сбора, отбора и обобщения информации; Уметь: соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности; Иметь практический опыт работы с информационными источниками, опыт научного поиска, создания научных текстов; Владеть: навыками применения современных информационных технологий и программных средств, в том числе	№№1-8
	ответственного производителя, и использовать их при решении задач профессиональной деятельности		
ОПК-2.2. Уметь: выбирать современные информационные технологии и программные средства, в том числе	ответственного производителя, в том числе	Уметь: соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности; Иметь практический опыт работы с информационными источниками, опыт научного поиска, создания научных текстов; Владеть: навыками применения современных информационных технологий и программных средств, в том числе	№№1-8
	использовать их при решении задач профессиональной деятельности		
ОПК-2.3. Владеть: навыками применения современных информационных средств, в том числе	ответственного производителя, при решении задач профессиональной деятельности	Знать: основные методы информационной безопасности ИС Уметь: организовать работы по управлению проектом ИС	№№1-8
	программных средств, в том числе		
ОПК – 3 Способен решать стандартные задачи профессиональной	ОПК-3.1. Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и		

¹ Наименования разделов и тем должен соответствовать рабочей программе дисциплины.

<p>Деятельности на основе информационной и библиографической культуры с применением информационно-коммуникативных технологий и с учетом основных требований информационной безопасности</p>	<p>библиографической культуры с применением информационно-коммуникативных технологий и с учетом основных требований информационной безопасности</p> <p>ОПК-3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникативных технологий и с учетом основных требований информационной безопасности</p> <p>ОПК-3.3. Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p>	<p>Иметь навыки в проведении переговоров и способен осуществлять контроль версий</p>	
<p>ОПК – 4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью</p>	<p>ОПК-4.1. Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы</p> <p>ОПК-4.2. Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы</p>	<p>Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы</p> <p>Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы</p>	

	ОПК-4.3. Владеть: составления технической документации на различных этапах жизненного цикла информационной системы	Владеть: составления технической документации на различных этапах жизненного цикла информационной системы	
--	--	---	--

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине Защита информации 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 промежуточной аттестации
		Этап текущих аттестаций						
		1-5 недели	6-10 недели	11-15 недели	1-17 недели	КР/К П	18-20 недели	
ОПК -2 Способен понимать принципы работы современных информационных технологий и программных средств. в том числе отечественного производства, и исползовать их при решении задач профессиональной	ОПК-2.1. Знать: современные информационные технологии и программные средства. в том числе отечественного производства при решении задач профессиональной деятельности ОПК-2.2. Уметь: выбирать современные информационные технологии и программные средства, в том числе отечественного	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа №3		Тест, устный опрос	
ОПК -2 Способен понимать принципы работы современных информационных технологий и программных средств. в том числе отечественного производства, и исползовать их при решении задач профессиональной	ОПК-2.1. Знать: современные информационные технологии и программные средства. в том числе отечественного производства при решении задач профессиональной деятельности ОПК-2.2. Уметь: выбирать современные информационные технологии и программные средства, в том числе отечественного	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос	

Деятельности	производства при решении задач профессиональной деятельности							
	ОПК-2.3. Владеть: навыками применения современных информационных технологий и программных средств, в том числе ответственного производства, при решении задач профессиональной деятельности	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос	
ОПК – 3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос	
	ОПК-3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос	

ОПК – 4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1. Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ОПК-4.2. Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
ОПК – 4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.3. Владеть: составлением технической документации на различных этапах жизненного цикла информационной системы	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	ОПК-3.3. Владеть: навыками подготовки аннотаций, рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	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 Защита информации 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 (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.	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.

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

Показатели уровня 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 пятибалльная, двадцатибалльная и стобалльная шкалы знаний, умений, навыков.

Шкалы оценивания			Критерии оценивания
пятибалльная	двадцатибалльная	стобалльная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 – 100 баллов	Показывает высокий уровень сформированности компетенций, т.е.: <ul style="list-style-type: none"> - 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.: <ul style="list-style-type: none"> - 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.: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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. Дать определение информации.
2. Основные алгоритмы кодирования.
3. Системы счисления.
4. Правила алгебры логики.

3.2. Оценочные средства и критерии сформированности компетенций

3.2.1. Аттестационная контрольная работа №1

1. Основные понятия и определения информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности. Классификация атак. Модели сетевой безопасности и безопасности информационной системы.
2. Классическая задача криптографии. Угрозы со стороны злоумышленника и участников процесса информационного взаимодействия.
3. Шифры замены и перестановки. Mono- и многоалфавитные подстановки Шифры Цезаря, Виженера, Вернама. Методы дешифрования.
4. Классификация методов дешифрования. Модель предполагаемого противника. Правила Керкхоффа.
5. Совершенная секретность по Шеннону. Примеры совершенно секретных систем. Шифр Вернама. Понятие об управлении ключами.
6. Блочные криптосистемы с секретным ключом. Алгоритм DES. Описание DES. Основные этапы алгоритма.

3.2.2. Список вопросов к зачету

1. Основные понятия и определения информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности. Классификация атак. Модели сетевой безопасности и безопасности информационной системы.
2. Классическая задача криптографии. Угрозы со стороны злоумышленника и участников процесса информационного взаимодействия.
3. Шифры замены и перестановки. Mono- и многоалфавитные подстановки Шифры Цезаря, Виженера, Вернама. Методы дешифрования.
4. Классификация методов дешифрования. Модель предполагаемого противника. Правила Керкхоффа.
5. Совершенная секретность по Шеннону. Примеры совершенно секретных систем. Шифр Вернама. Понятие об управлении ключами.
6. Блочные криптосистемы с секретным ключом. Алгоритм DES. Описание DES. Основные этапы алгоритма.
7. Схема алгоритма DES. Раунд алгоритма. Преобразование ключа.
8. Алгоритм DES. Подстановка с помощью S-блоков. Расшифрование в DES.
9. Блочные криптосистемы с секретным ключом. Режимы работы. ГОСТ 28147-89 в режиме простой замены.
10. Поточные криптосистемы с секретным ключом. Синхронные и самосинхронизирующиеся поточные криптосистемы. Примеры. ГОСТ 28147-89 в режимах гаммирования.
11. Стандарт криптографической защиты 21 века (AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра.
12. Теория сложности вычислений. Классификация алгоритмов.
13. Алгоритм RSA. Математическая модель алгоритма. Стойкость алгоритма.
14. Криптосистема Эль-Гамала.

15. Электронная подпись. Варианты электронной подписи на основе алгоритмов RSA и Эль-Гамала.
16. Хэш-функции и их применение. Хеш-функция MD2.
17. Однонаправленные (односторонние) функции с секретом и их применение.
18. Обобщенная модель электронной цифровой подписи. Схема Диффи-Хеллмана, схема Эль-Гамала.
19. Цифровая подпись на основе алгоритма RSA.
20. Стандарт цифровой подписи DSS. Генерация цифровой подписи. Проверка цифровой подписи.
21. Основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны. Протоколы аутентификации с использованием поппе и временных меток.
22. Криптографические протоколы. Понятие криптографического протокола и обоснование необходимости их использования. Протокол обмена сеансовыми ключами. Вскрытие "человек-в-середине". Протокол "держась за руки".
23. Сертификация ключей с помощью цифровых подписей. Разделение секрета. Метки времени. Пример протокола защиты базы данных.
24. Основы криптоанализа. Обзор возможных вариантов криптоанализа. Метод вскрытия «встреча посередине». Вскрытие со словарем. Вскрытие системы Вижинера, использующей простой XOR.
25. Метод бесключевого чтения RSA. Атака на подпись RSA по выбранному шифротексту. Вскрытие хэш-функций с использованием парадокса дня рождения.
26. Криптосистемы на эллиптических кривых.

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.).