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 «Теоретические основы компьютерной безопасности»

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 ИБ «20» сентября 2021г., протокол № 2

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

г. Махачкала 2021

СОДЕРЖАНИЕ

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Теоретические основы компьютерной безопасности» 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 «Теоретические основы компьютерной безопасности» предусмотрено формирование следующих компетенций:

ОПК-3. Способен использовать математические методы, необходимые для решения задач профессиональной деятельности;

ОПК-10 - Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

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)

- *Устный опрос*
- *Курсовая работа / курсовой проект*
- *Вопросы для проведения зачета*

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 использовать математические методы, необходимые для решения задач профессиональной деятельности	ОПК-3.2.1 - умеет исследовать функциональные зависимости, возникающие для решения стандартных прикладных задач ОПК-3.1.20 - знает основные понятия и определения теории информации	Знать: выявление угроз и оценка уязвимости информационных систем; обоснование выборов функциональной структуры, принципов организации технического, программного и информационного обеспечения систем, средств и технологий обеспечения информационной безопасности объектов защиты; Уметь: выбирать стратегии защиты информации в информационных системах Владеть: навыками работы с программными и аппаратными средствами защиты информации	№№1-17
ОПК-10 - . Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.2.2 - умеет контролировать эффективность принятых мер по реализации политик безопасности информации в современных операционных системах	Знать: выявление угроз и оценка уязвимости информационных систем; обоснование выборов функциональной структуры, принципов организации технического, программного и информационного обеспечения систем, средств и технологий обеспечения информационной безопасности объектов защиты; Уметь: выбирать стратегии защиты информации в информационных системах Владеть: навыками работы с программными и аппаратными средствами защиты информации	№№1-17 №№1-17

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

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине Теоретические основы компьютерной безопасности 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 использовать математические методы, необходимые для решения задач профессиональной деятельности	ОПК-3.2.1 - умеет исследовать функциональные зависимости, возникающие для решения стандартных прикладных задач	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
	ОПК-3.1.20 - знает основные понятия и определения теории информации	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
ОПК-10 - . Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.2.2 - умеет контролировать эффективность принятых мер по реализации политик безопасности информации в современных операционных системах	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена

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 Теоретические основы компьютерной безопасности 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. 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

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
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. Системы счисления.
2. Составление модели угроз информационной системе.
3. Формирование требований к системе защиты информации.
4. Формирование требований к политике информационной безопасности.
5. Формирование регламента действий при возникновении нештатных ситуаций.

3.2. Оценочные средства и критерии сформированности компетенций

3.2.1. Курсовая работа/курсовой проект

Примерные темы курсовых работ/курсовых проектов

1. Парольные системы защиты.
2. Целостность данных.
3. Модель Кларка-Вилсона.
4. Стеганография.
5. Криптография. Шифрование.
6. Криптография. Электронно-цифровая подпись и хеширование.
7. Субъект-объектная модель. Изолированная программная среда.
8. Работа с матрицей доступов. Домены безопасности.
9. Модель Take-Grant.
10. Нарушение дискреционной политики безопасности программой «Троянский конь».
11. Мандатные политики безопасности.
12. Стандарты в области защиты информации в компьютерных системах.

Требования к структуре, содержанию и оформлению курсовых работ (проектов) приводятся в методических указаниях/рекомендациях.

Критерии оценки уровня сформированности компетенций при выполнении курсовой работы/курсового проекта:

- оценка «отлично»: продемонстрировано блестящее владение проблемой исследования, материал выстроен логично, последовательно, обучающийся аргументированно отстаивает свою точку зрения. Во введении приводится обоснование выбора конкретной темы, чётко определены цель и задачи работы (проекта). Использован достаточный перечень источников и литературы для методологической базы исследования. Обучающийся грамотно использует профессиональные термины, актуальные исходные данные. Проведен самостоятельный анализ (исследование) объекта. По результатам работы сделаны логичные выводы. Оформление работы соответствует методическим рекомендациям. Объем и содержание работы соответствует требованиям. На защите обучающийся исчерпывающе отвечает на все дополнительные вопросы;
- оценка «хорошо»: обучающийся демонстрирует повышенный уровень владения проблемой исследования, логично, последовательно и аргументированно отстаивает ее концептуальное содержание. Во введении содержатся небольшие неточности в формулировках цели, задач. В основной части допущены незначительные погрешности в расчетах (в исследовании). Выводы обоснованы, аргументированы. Оформление работы соответствует методическим рекомендациям. Объем работы соответствует требованиям. На защите обучающийся отвечает на все дополнительные вопросы;

- оценка «удовлетворительно»: обучающийся демонстрирует базовый уровень владения проблемой исследования. Во введении указаны цель и задачи исследования, но отсутствуют их четкие формулировки. Работа является компиляцией чужих исследований с попыткой формулировки собственных выводов в конце работы. Изложение материала логично и аргументировано. Наблюдается отступление от требований в оформлении и объеме работы. При ответе на вопросы обучающийся испытывает затруднения;

- оценка «неудовлетворительно»: обнаруживается несамостоятельность выполнения курсовой работы, некомпетентность в исследуемой проблеме. Нарушена логика изложения. Работа не соответствует требованиям, предъявляемым к оформлению и содержанию. На защите курсовой работы обучающийся не отвечает на вопросы.

3.2.2. Аттестационная контрольная работа №1

1. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты.
2. Доступ. Информационный поток. Основная аксиома теории защиты информации.
3. Ценность информации. Модели ценности. Решетка ценности и ее свойства.
4. Общая методология построения систем защиты.
5. Принципы построения системы защиты. Каналы утечки информации.
6. Понятие политики безопасности. Субъект-объектная модель политики безопасности.
7. Дискреционная политика безопасности. Определение.
8. Проблема безопасности при атаке вида «Троянский конь».

3.2.3. Аттестационная контрольная работа №1

1. Ролевая и мандатная политика безопасности. Определения.
2. Политика безопасности информационных потоков.
3. Реализация политики безопасности в терминах субъект-объектной модели.
4. Базовая теорема изолированной программной среды (ИПС).
5. Базовая теорема изолированной программной среды (ИПС).
6. Политика изолированной программной среды.

3.2.4. Аттестационная контрольная работа №1

1. Модель Харрисона-Руззо-Ульмана (HRU). Анализ безопасности модели HRU.
2. Теоремы безопасности для модели HRU.
3. Основные положения модели Take-Grant.
4. Анализ механизмов передачи прав доступа для модели Take-Grant.
5. Расширенная модель Take-Grant.
6. Де-факто правила и определение информационных потоков.
7. Замыкание графов доступов и информационных потоков расширенной модели Take-Grant.
8. Анализ путей распространения прав доступа и информационных потоков расширенной модели Take-Grant.
9. Классическая модель Белла-ЛаПадула.
10. Свойства безопасности для классической модели Белла-ЛаПадула.
11. Базовая теорема безопасности для классической модели Белла-ЛаПадула.
12. Политика low-watermark в модели Белла-ЛаПадула.
13. Безопасность переходов для модели Белла-ЛаПадула.
14. Базовая теорема безопасности для модели Белла-ЛаПадула с функцией переходов. Безопасность в смысле администрирования.

3.2.5. Список вопросов к зачету

1. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты.
2. Доступ. Информационный поток. Основная аксиома теории защиты информации.
3. Ценность информации. Модели ценности. Решетка ценности и ее свойства.

4. Общая методология построения систем защиты.
5. Принципы построения системы защиты. Каналы утечки информации.
6. Понятие политики безопасности. Субъект-объектная модель политики безопасности.
7. Дискреционная политика безопасности. Определение.
8. Проблема безопасности при атаке вида «Троянский конь».
9. Ролевая и мандатная политика безопасности. Определения.
10. Политика безопасности информационных потоков.
11. Реализация политики безопасности в терминах субъект-объектной модели.
12. Базовая теорема изолированной программной среды (ИПС).
13. Базовая теорема изолированной программной среды (ИПС).
14. Политика изолированной программной среды.
15. Модель Харрисона-Руззо-Ульмана (HRU). Анализ безопасности модели HRU.
16. Теоремы безопасности для модели HRU.
17. Основные положения модели Take-Grant.
18. Анализ механизмов передачи прав доступа для модели Take-Grant.
19. Расширенная модель Take-Grant.
20. Де-факто правила и определение информационных потоков.
21. Замыкание графов доступов и информационных потоков расширенной модели Take-Grant.
22. Анализ путей распространения прав доступа и информационных потоков расширенной модели Take-Grant.
23. Классическая модель Белла-ЛаПадула.
24. Свойства безопасности для классической модели Белла-ЛаПадула.
25. Базовая теорема безопасности для классической модели Белла-ЛаПадула.
26. Политика low-watermark в модели Белла-ЛаПадула.
27. Безопасность переходов для модели Белла-ЛаПадула.
28. Базовая теорема безопасности для модели Белла-ЛаПадула с функцией переходов. Безопасность в смысле администрирования.
29. Модель мандатной политики целостности информации Биба.
30. Модель системы военных сообщений (СВС). Неформальное описание модели.
31. Модель системы военных сообщений (СВС). Формальное описание модели.
32. Модель системы военных сообщений (СВС). Безопасность переходов.

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.