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 «Стандарты ИСО и ГОСТы в области информационной 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 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 Стандарты ИСО и ГОСТы в области информационной 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 Стандарты ИСО и ГОСТы в области информационной безопасности предусмотрено формирование следующей компетенции:

УК-1 - Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере 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)

- *Контрольная работа*
- *Решение задач (заданий)*
- *Тест (для текущего контроля)*
- *Устный опрос*
- *Задания / 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]
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1.3 знает основные источники информации о проблемных ситуациях в профессиональной деятельности и подходы к критическому анализу этой информации	**Знать:** Основные источники информации в области стандартизации информационной безопасности: официальные сайты ISO, IEC, Росстандарта, ФСТЭК России, электронные библиотеки, специализированные базы данных, научные журналы. Критерии оценки достоверности и актуальности нормативных документов. Методы критического анализа и систематизации информации, выявления противоречий и пробелов в требованиях стандартов. **Уметь:** Осуществлять целенаправленный поиск действующих версий международных и национальных стандартов ИБ. Анализировать структуру и содержание стандартов, выделять ключевые требования, сопоставлять различные документы, выявлять области их применимости. Формулировать проблемные ситуации, возникающие при внедрении стандартов, и определять возможные пути их решения. **Владеть:** Навыками работы с текстами стандартов, методами контент-анализа и сравнительного анализа нормативных документов. Способностью обобщать информацию из различных источников для	№№1-17

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

		подготовки аналитических обзоров и заключений.	
	УК-1.1.4 знает порядок принятия решений при возникновении проблемных ситуаций в профессиональной деятельности	**Знать:** Структуру процесса принятия решений: идентификация проблемы, сбор информации, генерация альтернатив, оценка последствий, выбор оптимального варианта. Методы анализа проблемных ситуаций. Особенности принятия решений в области стандартизации и сертификации систем менеджмента информационной безопасности. **Уметь:** Идентифицировать проблемные ситуации, связанные с несоответствием требованиям стандартов, и разрабатывать обоснованные рекомендации по их устранению. Оценивать альтернативные варианты действий при выборе применимых стандартов или подходов к обеспечению ИБ. Принимать решения с учётом требований нормативных документов, рисков и ресурсных ограничений. **Владеть:** Навыками структурирования проблем и постановки задач в области применения стандартов ИБ. Способностью документировать принятые решения и обосновывать их перед руководством и проверяющими органами.	№№1-17
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1.1 знает основы законодательства Российской Федерации, систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации	**Знать:** Структуру и иерархию законодательных и нормативных актов РФ в области ИБ: Конституция РФ, федеральные законы, указы Президента, постановления Правительства. Место и роль подзаконных актов. Взаимосвязь российских стандартов с международными стандартами. Систему технического регулирования и сертификации средств защиты информации. **Уметь:** Ориентироваться в многообразии	№№1-17

		нормативных документов, определять применимость конкретного акта к заданной ситуации. Анализировать требования нормативных документов и сопоставлять их с положениями международных стандартов. Использовать справочно-правовые системы для поиска актуальных редакций документов. **Владеть:** Навыками работы с правовыми и нормативными документами, методами их систематизации и комментирования. Способностью применять нормы законодательства при разработке внутренних документов организации	
	ОПК-5.2.1 умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	**Знать:** Классификацию конфиденциальной информации. Требования законодательства РФ к защите персональных данных и основные положения стандартов. Понятие интеллектуальной собственности, объекты авторского права и смежных прав, патентного права. Методы правовой охраны результатов интеллектуальной деятельности. **Уметь:** Формулировать требования к защите конфиденциальной информации при разработке локальных нормативных актов (положение о коммерческой тайне, политика обработки персональных данных). Определять перечень мер, необходимых для соблюдения законодательства и стандартов. Оценивать достаточность разработанных требований и их соответствие нормативной базе. **Владеть:**иНавыками подготовки проектов документов, регламентирующих защиту конфиденциальной информации и персональных данных. Способностью аргументированно обосновывать необходимость принятия тех или иных	№№1-17

		требований перед руководством и персоналом организации.	

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине Стандарты ИСО и ГОСТы в области информационной 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**
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1.3 знает основные источники информации о проблемных ситуациях в профессиональной деятельности и подходы к критическому анализу этой информации	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
	УК-1.1.4 знает порядок принятия решений при возникновении проблемных ситуаций в профессиональной деятельности	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы,	ОПК-5.1.1 знает основы законодательства Российской Федерации, систему нормативных правовых актов, нормативных и методических	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3	Контрольная работа		Тест, устный опрос

регламентирующие деятельность по защите информации в сфере профессиональной деятельности	документов в области информационной безопасности и защиты информации						
	ОПК-5.2.1 умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	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 Стандарты ИСО и ГОСТы в области информационной 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

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные 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. Дать определение бита, байта.
2. Привести пример двоичного числа.
3. Сложить (вычесть) два двоичных числа.
4. Восьмеричная система счисления. Представления чисел в восьмеричной системе счисления.
5. Шестнадцатеричная система счисления. Представления чисел в шестнадцатеричной системе счисления.
6. Перевести число в его двоичное представление.
7. Алгоритмы сложения и вычитания в позиционной системе счисления.
8. Переменные, метки, константы.

3.2. Оценочные средства и критерии сформированности компетенций

3.2.1. Аттестационная контрольная работа №1

1. Дайте определение информационной безопасности. Перечислите основные свойства информации.
2. Что такое угроза информационной безопасности? Приведите примеры.
3. Назовите основные законодательные акты РФ в области защиты информации.
4. Что такое конфиденциальная информация? Какие виды конфиденциальной информации вы знаете?
5. Что такое система менеджмента информационной безопасности (СМИБ)?
6. Какие международные организации занимаются разработкой стандартов в области ИБ?
7. Что такое стандарт? Для чего нужна стандартизация?
8. Перечислите известные вам российские стандарты в области ИБ.
9. Что такое сертификация соответствия? Для чего она проводится?
10. Какие риски информационной безопасности вы знаете?

3.2.1. Аттестационная контрольная работа №2

1. Назовите основные организации, разрабатывающие международные стандарты в области ИБ. Каковы их функции?
2. Охарактеризуйте структуру семейства стандартов ISO/IEC 27000. Перечислите основные стандарты серии и их назначение.
3. Каковы цели и задачи системы менеджмента информационной безопасности (СМИБ) по ISO/IEC 27001?
4. Опишите процессный подход PDCA (Plan-Do-Check-Act) в контексте управления ИБ. Как он реализован в ISO/IEC 27001?
5. Какова структура стандарта ISO/IEC 27001? Назовите основные разделы.
6. Для чего предназначен стандарт ISO/IEC 27002? В чём его отличие от ISO/IEC 27001?
7. Перечислите основные домены (области) управления ИБ, описанные в ISO/IEC 27002.
8. Что понимается под «контекстом организации» в ISO/IEC 27001? Какие факторы необходимо учитывать?
9. Какие требования предъявляются к политике информационной безопасности согласно ISO/IEC 27001?
10. Как определяются роли, ответственность и полномочия в рамках СМИБ?

3.2.1. Аттестационная контрольная работа №3

1. Опишите процесс управления рисками информационной безопасности согласно ISO/IEC 27005.

2. Какие методы оценки рисков (качественные, количественные) используются на практике?
3. Какие требования предъявляются к аудиторам СМИБ согласно стандартам серии ISO/IEC 27007?
4. В чём отличие аудита СМИБ от аудита средств защиты информации (ISO/IEC 27008)?
5. Какие дополнительные требования к безопасности предъявляются в отраслевых стандартах ISO/IEC 27017 (облачные вычисления) и ISO/IEC 27018 (защита ПДн в облаке)?
6. Опишите жизненный цикл управления инцидентами информационной безопасности по ISO/IEC 27035.
7. Какие стандарты регламентируют безопасность приложений и жизненный цикл разработки ПО?
8. Каковы основные этапы процесса сертификации СМИБ на соответствие ISO/IEC 27001?
9. Какие документы необходимо подготовить для прохождения сертификационного аудита?
10. Как поддерживается и подтверждается сертификат соответствия СМИБ?

3.2.4. Список вопросов к экзамену

1. Роль и место стандартов в современной системе обеспечения информационной безопасности.
2. Международные и национальные организации по стандартизации (ISO, IEC, Росстандарт): структура, цели, функции.
3. Семейство стандартов ISO/IEC 27000: общая характеристика, структура, взаимосвязь.
4. Основные термины и определения в области стандартизации ИБ (ISO/IEC 27000).
5. Стандарт ISO/IEC 27001: цели, структура, основные требования к СМИБ.
6. Процессный подход PDCA (Plan-Do-Check-Act) и его реализация в ISO/IEC 27001.
7. Стандарт ISO/IEC 27002: назначение, структура, содержание основных разделов.
8. Обзор руководящих принципов и мер безопасности по доменам ИБ.
9. Контекст организации и лидерство в ISO/IEC 27001 (разделы 4-5).
10. Планирование действий по оценке рисков и возможностей (раздел 6 ISO/IEC 27001).
11. Постановка целей в области информационной безопасности.
12. Поддержка и эксплуатация СМИБ (разделы 7-8 ISO/IEC 27001).
13. Оценка производительности и улучшение СМИБ (разделы 9-10 ISO/IEC 27001).
14. Национальная система стандартизации в области ИБ. Ключевые ГОСТ Р.
15. ГОСТ Р ИСО/МЭК 27001-2022: анализ национальной версии, отличия от международной.
16. ГОСТ Р ИСО/МЭК 27002-2022: особенности применения в РФ.
17. Стандарты по управлению рисками информационной безопасности (ISO/IEC 27005, ГОСТ Р ИСО/МЭК 27005).
18. Процесс управления рисками ИБ: идентификация, анализ, оценка, обработка рисков.
19. Методологии оценки рисков: качественные и количественные методы.
20. Стандарты для аудиторов ИБ (ISO/IEC 27007, 27008). Требования к компетенции.
21. Методика проведения внутреннего и внешнего аудита СМИБ.
22. Отраслевые стандарты ИБ: ISO/IEC 27017 (облачные вычисления), ISO/IEC 27018 (защита ПДн в облаке), ISO/IEC 27019 (энергетика).
23. Стандарты в области управления инцидентами ИБ (ISO/IEC 27035, ГОСТ Р 56611).
24. Жизненный цикл управления инцидентами: обнаружение, регистрация, расследование, устранение, извлечение уроков.
25. Стандарты по безопасности приложений и жизненному циклу разработки (ISO/IEC 27034, 27037).
26. Процесс сертификации СМИБ на соответствие ISO/IEC 27001.
27. Выбор органа по сертификации. Этапы сертификационного аудита.
28. Документационное обеспечение СМИБ: политики, процедуры, регламенты, записи.

29. Интеграция требований стандартов с законодательством РФ (ФЗ-152, коммерческая тайна).
30. Перспективы развития стандартизации в области информационной безопасности.

3.2.5. Вопросы по остаточным знаниям

1. Назовите основные международные и национальные организации, разрабатывающие стандарты в области информационной безопасности.
2. Какова структура семейства стандартов ISO/IEC 27000? Какие стандарты являются ключевыми?
3. В чём отличие стандарта ISO/IEC 27001 от ISO/IEC 27002?
4. Опишите цикл PDCA и его применение в управлении информационной безопасностью.
5. Какие основные разделы включает стандарт ISO/IEC 27001?
6. Каков порядок оценки рисков информационной безопасности согласно ISO/IEC 27005?
7. Назовите основные требования к проведению внутреннего аудита СМИБ.
8. Какие существуют отраслевые стандарты ИБ (на примере облачных вычислений или энергетики)?
9. Как осуществляется сертификация системы менеджмента информационной безопасности на соответствие ISO/IEC 27001?
10. Какие российские национальные стандарты (ГОСТ Р) соответствуют основным международным стандартам серии ISO/IEC 27000?

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 экзамена, 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 (экзамена с оценкой) зависят от их форм проведения (тест, вопросы, задания, решение задач и т.д.).