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 «Аудит информационных технологий и систем обеспечения 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 «Аудит информационных технологий и систем обеспечения 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 «Аудит информационных технологий и систем обеспечения информационной безопасности» предусмотрено формирование следующих компетенций:

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

ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем.

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)

- *Эссе*
- *Устный опрос*
- *Вопросы для проведения экзамена*

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-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1.7 знает основные документы по стандартизации в сфере управления ИБ	Знать: Перечень и содержание основных международных (ISO/IEC 27000 series), национальных (ГОСТ Р ИСО/МЭК 27000, ГОСТ Р 57580) и отраслевых стандартов в области управления информационной безопасностью. Структуру и назначение стандартов ISO 17799 (ISO 27002), ISO 15408 («Общие критерии»), COBIT, а также российских стандартов по защите информации. Уметь: Применять требования стандартов при проведении аудита ИБ, определять соответствие системы менеджмента информационной безопасности (СМИБ) требованиям стандартов, анализировать нормативную базу при разработке политик и процедур. Владеть: Навыками поиска и актуализации нормативных документов, методами сравнительного анализа стандартов, способностью интерпретировать требования стандартов для конкретной организации.	№№ 1-17
	ОПК-5.1.8 знает принципы формирования политики информационной безопасности в автоматизированных системах	Знать: Основные элементы политики ИБ (цели, задачи, принципы, область действия, роли и ответственность). Методологию разработки политик: анализ рисков, определение требований, согласование с бизнес-процессами. Виды политик (верхнего уровня, частные политики, процедуры, регламенты). Требования стандартов к содержанию политики ИБ. Уметь: Разрабатывать проекты политик ИБ для различных уровней управления, определять структуру и содержание документов, учитывать требования законодательства и стандартов при формировании политик. Владеть: Навыками документирования политик ИБ, методами внедрения политик в деятельность организации, способами оценки эффективности реализованных политик.	№№ 1-17
	ОПК-5.2.2 умеет анализировать и разрабатывать проекты локальных правовых актов,	Знать: Структуру и требования к оформлению организационно-распорядительных документов (приказы, положения, инструкции, регламенты). Нормативную базу, регулирующую документооборот в области ИБ. Методы анализа действующих документов на предмет соответствия требованиям и	№№ 1-17

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

	инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации	актуальности. Уметь: Анализировать существующие документы по ИБ, выявлять недостатки и противоречия. Разрабатывать проекты новых документов или вносить изменения в действующие. Согласовывать документы с заинтересованными сторонами. Владеть: Навыками подготовки официальных документов, методами нормоконтроля, умением использовать шаблоны и типовые формы.	
ОПК-13Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ОПК-13.2.4 умеет осуществлять контроль обеспечения уровня защищенности в автоматизированных системах	Знать: Показатели и критерии уровня защищенности. Методы контроля (тестирование на проникновение, анализ конфигурации, сканирование уязвимостей, мониторинг событий). Инструменты контроля (сетевые сканеры, анализаторы протоколов, системы обнаружения вторжений). Периодичность и процедуры контроля. Уметь: Планировать и проводить мероприятия по контролю защищенности. Интерпретировать результаты сканирования и тестирования. Выявлять отклонения от требуемого уровня защищенности. Владеть: Навыками работы со сканерами уязвимостей, инструментами анализа защищенности, методами составления отчётов по результатам контроля.	№№ 1-17
	ОПК-13.2.8 умеет контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	Знать: Методы оценки эффективности мер защиты (показатели результативности, метрики). Способы сбора и анализа данных о функционировании средств защиты. Критерии эффективности для различных типов мер (организационных, технических). Уметь: Собирать и анализировать данные о работе средств защиты (логи, отчёты, журналы). Сравнивать фактические показатели с целевыми. Выявлять неэффективные меры и предлагать корректирующие действия. Владеть: Навыками мониторинга средств защиты, методами статистического анализа инцидентов, умением готовить отчёты об эффективности.	№№ 1-17
	ОПК-13.2.9 умеет документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы	Знать: Требования к документированию процессов контроля (форма, содержание, периодичность). Виды документов: журналы, акты, протоколы, отчёты. Правила оформления результатов измерений и проверок. Уметь: Составлять акты и протоколы по результатам контроля. Вести журналы учёта событий и инцидентов. Готовить итоговые отчёты о состоянии защищённости с выводами и рекомендациями. Владеть: Навыками делопроизводства в области ИБ, методами архивирования и хранения документации, способами обеспечения целостности и подлинности документов.	№№ 1-17
	ОПК-15.1.3 знает программные средства, позволяющие вести автоматизированный аудит	Знать: Классификацию программных средств аудита ИБ: сканеры уязвимостей, анализаторы конфигурации, SIEM-системы, системы анализа защищённости (VA-системы), специализированные комплексы (CRAMM, КОНДОР, ГРИФ). Назначение, принципы работы и основные возможности перечисленных средств. Критерии выбора инструментов для аудита.	№№ 1-17

		Уметь: Выбирать подходящие программные средства для решения конкретных задач аудита. Оценивать функциональность и ограничения инструментов. Интерпретировать результаты работы автоматизированных средств. Владеть: Навыками работы с типовыми инструментами аудита (например, сканером уязвимостей). Способностью анализировать отчёты автоматизированных систем.	

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Аудит информационных технологий и систем обеспечения 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**
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1.7 знает основные документы по стандартизации в сфере управления ИБ	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
	ОПК-5.1.8 знает принципы формирования политики информационной безопасности в автоматизированных системах	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.2.2 умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена

ОПК-13Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ОПК-13.2.4 умеет осуществлять контроль обеспечения уровня защищенности в автоматизированных системах	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
	ОПК-13.2.8 умеет контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
	ОПК-13.2.9 умеет документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
	ОПК-15.1.3 знает программные средства, позволяющие вести автоматизированный аудит	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 «Аудит информационных технологий и систем обеспечения 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
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	Обучающийся владеет знаниями основного материал на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продемонстрирован базовый уровень владения

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
	устранения. Обучающимся продемонстрирован базовый уровень освоения компетенции	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. Дайте определение информационной безопасности. Какие основные свойства информации защищаются?
2. Перечислите основные виды угроз информационной безопасности автоматизированных систем.
3. Что такое политика информационной безопасности? Для чего она нужна?
4. Назовите известные вам стандарты в области информационной безопасности (международные и российские).
5. Что такое аудит? Какие виды аудита вы знаете?
6. Что такое риск? Как связаны риск, угроза и уязвимость?
7. Какие организационные меры защиты информации вы знаете?
8. Что такое средство защиты информации? Приведите примеры программных и аппаратных средств защиты.
9. Для чего проводится тестирование на проникновение?
10. Какие нормативные документы регулируют деятельность по защите информации в РФ?

3.2. Оценочные средства и критерии сформированности компетенций

3.2.1. Аттестационная контрольная работа №1

1. Перечислите цели и задачи информационной безопасности на предприятии.
2. Опишите модель построения системы информационной безопасности предприятия (основные элементы и их взаимосвязь).
3. Что понимается под аудитом информационной безопасности? Какие виды аудита существуют?
4. Назовите основные этапы анализа информационных рисков.
5. Сравните качественные и количественные методы оценки рисков. Приведите примеры.
6. Какие документы относятся к стандартам в области ИБ? Охарактеризуйте «Оранжевую книгу» (TCSEC).
7. Что такое «Общие критерии» (ISO 15408)? Каково их назначение?
8. Опишите структуру и содержание британского стандарта BS 7799 / ISO 17799.
9. Какие российские стандарты по безопасности информационных технологий вы знаете?
10. В чём отличие стандарта COBIT от стандартов серии ISO 27000?

3.2.3. Аттестационная контрольная работа №2

1. Раскройте основные понятия «Общих критериев»: объект оценки, профиль защиты, задание по безопасности, уровень доверия.
2. Какова методология оценки безопасности информационных технологий по ISO 15408?
3. Перечислите классы функциональных требований в «Общих критериях». Приведите примеры семейств.
4. Что такое уровень доверия (EAL)? Какие уровни установлены в ISO 15408?
5. Назначение и структура стандарта ISO 17799 (ISO 27002).
6. Какие разделы включает стандарт ISO 17799? Кратко охарактеризуйте каждый.
7. Что такое политика безопасности? Какие требования предъявляет ISO 17799 к политике?
8. Какие организационные меры обеспечения ИБ предусмотрены в ISO 17799?
9. Какие требования стандарт предъявляет к классификации ресурсов и управлению доступом?
10. Как стандарт регламентирует планирование бесперебойной работы организации?

3.2.4. Аттестационная контрольная работа №3

1. Перечислите основные типы программных средств, используемых для аудита информационной безопасности.
2. Опишите назначение и возможности системы CRAMM. Какие этапы оценки рисков в ней реализованы?
3. Что такое система КОНДОР? Для решения каких задач она применяется?
4. Для чего используются сетевые сканеры безопасности? Приведите примеры (не менее двух).
5. Какие подходы к проведению аудита ИБ существуют? Охарактеризуйте каждый.
6. Перечислите основные этапы проведения аудита информационной безопасности на предприятии.
7. Какие данные необходимо собрать для проведения аудита ИБ? Из каких источников?
8. Как формулируются рекомендации по итогам аудита? Из каких разделов состоит отчёт?
9. Что включает в себя экономическая оценка обеспечения ИБ?
10. Какие навыки и знания необходимы аудитору для качественного проведения аудита?

3.2.5. Список вопросов к экзамену

1. Понятие информационной безопасности, её цели и задачи.
2. Угрозы ИБ: классификация, источники, методы противодействия.
3. Модель построения системы информационной безопасности предприятия.
4. Разработка концепции обеспечения ИБ организации.
5. Аудит ИБ: определение, цели, виды (внешний/внутренний, инициативный/обязательный).
6. Методы сбора и анализа данных при аудите ИБ (интервью, анализ документов, инструментальный контроль).
7. Анализ информационных рисков: основные понятия (риск, угроза, уязвимость, актив).
8. Качественные и количественные методы оценки рисков.
9. Управление информационными рисками: обработка риска, принятие, избегание, передача.
10. Стандарты ИБ: назначение, классификация, обзор.
11. Стандарт TCSEC («Оранжевая книга»): уровни доверия, основные классы.
12. Гармонизированные критерии Европейских стран (ITSEC).
13. Британский стандарт BS 7799 и его эволюция в ISO 17799 / ISO 27002.
14. Международный стандарт ISO 15408 «Общие критерии»: структура, основные понятия.
15. Стандарт COBIT: назначение, области управления.
16. Российские стандарты в области ИБ (ГОСТ Р ИСО/МЭК 27000, ГОСТ Р 57580, документы ФСТЭК).
17. Оценка безопасности ИТ на основе «Общих критериев»: профиль защиты, задание по безопасности.
18. Уровни доверия EAL в ISO 15408: характеристика уровней 1–7.
19. Структура стандарта ISO 17799 (ISO 27002): основные разделы.
20. Политика безопасности: требования к разработке и содержанию.
21. Организационные меры обеспечения ИБ по ISO 17799.
22. Классификация и контроль ресурсов в стандартах ИБ.
23. Требования к безопасности персонала, физическая безопасность.
24. Управление доступом к информационным системам.
25. Планирование бесперебойной работы организации (резервное копирование, восстановление после сбоев).
26. Программные средства аудита ИБ: обзор, классификация.
27. Система CRAMM: назначение, этапы анализа рисков.
28. Система КОНДОР: возможности применения для аудита.

29. Сетевые сканеры безопасности (Nessus, OpenVAS, XSpider и др.): принципы работы.
30. Методика проведения аудита ИБ на предприятии: этапы, документирование, отчётность.

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.

Критерии оценки уровня сформированности компетенций по результатам проведения зачета:

- оценка «зачтено»: обучающийся демонстрирует всестороннее, систематическое и глубокое знание материала, свободно выполняет задания, предусмотренные программой дисциплины, усвоивший основную и дополнительную литературу. Обучающийся выполняет задания, предусмотренные программой дисциплины, на уровне не ниже базового;

- оценка «не зачтено»: обучающийся демонстрирует незнание материала, не выполняет задания, предусмотренные программой дисциплины. Обучающийся не выполняет задания, предусмотренные программой дисциплины, на уровне ниже базового. Дальнейшее освоение ОПОП не возможно без дополнительного изучения материала и подготовки к зачету.

Критерии оценки уровня сформированности компетенций по результатам проведения дифференцированного зачёта (зачета с оценкой) / экзамена:

- оценка **«отлично»:** обучающийся дал полный, развернутый ответ на поставленный вопрос, проявил совокупность осознанных знаний об объекте, доказательно раскрыл основные положения темы. В ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, явлений. Обучающийся подкрепляет теоретический ответ практическими примерами. Ответ сформулирован научным языком, обоснована авторская позиция обучающегося. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа или с помощью «наводящих» вопросов преподавателя. Обучающимся продемонстрирован высокий уровень владения компетенцией(-ями);

- оценка **«хорошо»:** обучающимся дан полный, развернутый ответ на поставленный вопрос, проявлено умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, но есть недочеты в формулировании понятий, решении задач. При ответах на дополнительные вопросы допущены незначительные ошибки. Обучающимся продемонстрирован повышенный уровень владения компетенцией(-ями);

- оценка **«удовлетворительно»:** обучающимся дан неполный ответ на вопрос, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, явлений, нарушена логика ответа, не сделаны выводы. Речевое оформление требует коррекции. Обучающийся испытывает затруднение при ответе на дополнительные вопросы. Обучающимся продемонстрирован базовый уровень владения компетенцией(-ями);

- оценки **«неудовлетворительно»:** обучающийся испытывает значительные трудности в ответе на вопрос, допускает существенные ошибки, не владеет терминологией, не знает основных понятий, не может ответить на «наводящие» вопросы преподавателя. Обучающимся продемонстрирован низкий уровень владения компетенцией(-ями).