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 «Технология построения защищенных автоматизированных систем»

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 «Технология построения защищенных автоматизированных систем» 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 «Технология построения защищенных автоматизированных систем» предусмотрено формирование следующих компетенций:

ОПК-14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений;

ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности 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)

- *Устный опрос*
- *Тесты*
- *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-14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	ОПК-14.1.2 знает критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем	**Знать:** Классификацию и назначение средств защиты информации (СЗИ) для программного обеспечения АС. Понятия эффективности и надежности СЗИ, их показатели и методы оценки. Нормативные и методические документы, регламентирующие требования к эффективности и надежности СЗИ (стандарты, руководящие документы ФСТЭК). Методы тестирования и верификации защитных механизмов ПО. Критерии оценки защищенности автоматизированных систем. **Уметь:** Анализировать техническую документацию на СЗИ для выделения показателей эффективности и надежности. Применять методики оценки эффективности и надежности для конкретных СЗИ в составе АС. Интерпретировать результаты испытаний и проверок для формулировки выводов о пригодности СЗИ к эксплуатации. **Владеть:** Навыками работы с руководящими документами по сертификации и оценке СЗИ. Методами расчета показателей надежности. Способностью обосновывать выбор СЗИ на основе сравнительного анализа их характеристик.	№№1-9
	ОПК-14.2.1 умеет осуществлять планирование и организацию работы персонала	**Знать:** Роли и ответственность персонала при эксплуатации защищенных АС. Принципы разделения обязанностей и минимизации привилегий. Требования	№№1-9

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

	автоматизированной системы с учетом требований по защите информации	к персоналу в нормативных документах (квалификация, допуск, инструктажи). Методы планирования работ по обеспечению ИБ (графики, регламенты, планы мероприятий). Порядок действий при инцидентах и нештатных ситуациях. **Уметь:** Разрабатывать должностные инструкции и регламенты для персонала, учитывающие требования по защите информации. Организовывать проведение инструктажей и обучение сотрудников. Планировать и контролировать выполнение персоналом мероприятий по обеспечению ИБ. Взаимодействовать с различными подразделениями для согласования организационных мер. **Владеть:** Навыками составления организационно-распорядительной документации. Методами контроля соблюдения персоналом политик безопасности. Способностью анализировать и корректировать схемы распределения прав доступа.	
ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.2.6 умеет осуществлять выбор и обоснование критериев эффективности функционирования защищенных автоматизированных информационных систем	**Знать:** Систему показателей эффективности защищенных АС (функциональные, стоимостные, временные, надежностные). Классификацию критериев эффективности (частные и обобщенные, качественные и количественные). Методы многокритериальной оценки и выбора. Взаимосвязь критериев эффективности с целями создания системы и требованиями по защите информации. Методики обоснования выбора критериев для конкретных типов АС. **Уметь:** Формулировать цели функционирования защищенной АС и выводить из них требования к эффективности. Выбирать совокупность критериев, адекватно отражающих степень достижения целей. Обосновывать выбор приоритетных критериев с учетом особенностей решаемых задач и ограничений. Применять методы свертки критериев для получения	№№1-9

		интегральной оценки. **Владеть:** Навыками построения дерева целей и критериев. Методами экспертного оценивания для обоснования критериев. Способностью документировать результаты выбора и обоснования критериев в проектной и эксплуатационной документации.	

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Открытые информационные системы» 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-14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	ОПК-14.1.2 знает критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения зачета
	ОПК-14.2.1 умеет осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения зачета

ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.2.6 умеет осуществлять выбор и обоснование критериев эффективности функционирования защищенных автоматизированных информационных систем	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения зачета

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 «Открытые информационные» системы 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 единичны е негрубые ошибки.	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

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
	Обучающимся продемонстрирован повышенный уровень освоения компетенции	
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. Дайте определение информационной безопасности. Перечислите основные свойства защищаемой информации.
2. Какие виды угроз информационной безопасности вы знаете? Приведите примеры.
3. Что такое операционная система? Назовите основные функции ОС.
4. Какие модели разграничения доступа реализованы в современных ОС (дискреционная, мандатная, ролевая)?
5. Что такое система управления базами данных (СУБД)? Какие требования предъявляются к защите БД?
6. Перечислите основные методы аутентификации пользователей (по факторам).
7. Что такое криптографическая защита информации? Приведите примеры криптографических алгоритмов.
8. Какие организационные меры защиты информации применяются на предприятии?
9. Что такое политика безопасности? Из каких разделов она состоит?
10. Какие стандарты и нормативные документы в области ИБ вы знаете (международные и российские)?

3.2. Оценочные средства и критерии сформированности компетенций

3.2.1. Комплект заданий для контрольной работы №1 для первой аттестации

1. Дайте определение автоматизированной системы (АС). Перечислите основные компоненты АС.
2. Охарактеризуйте этапы жизненного цикла автоматизированной системы.
3. Что понимается под защищённой АС? Какие подходы к созданию защищённых АС существуют?
4. Какие проблемы возникают при проектировании и реализации защищённых АС?
5. Что такое доверенная среда функционирования? Какими техническими средствами она обеспечивается?
6. Перечислите основные меры по обеспечению безопасности информации в государственных информационных системах (ГИС).
7. Какие требования предъявляются к защите АС в зависимости от класса защищённости?
8. Что такое персональные средства криптографической защиты информации (СКЗИ)? Назовите проблемы их использования и примеры решений.
9. Какие защищённые носители ключевой и аутентификационной информации вы знаете?
10. Как организуется безопасный терминальный доступ? Какие инструменты контроля доступа применяются для удалённой работы?

3.2.2. Комплект заданий для контрольной работы №2 для второй аттестации

1. Каков состав и особенности функционирования систем виртуализации?
2. В чём особенности защиты виртуальных машин по сравнению с физическими?
3. Как реализуется доверенная загрузка и контроль целостности систем виртуализации?
4. Назовите средства защиты систем виртуализации для гипервизоров KVM и VMware (приведите примеры).
5. Что такое инфраструктура безопасного «облака»? Какие угрозы актуальны для облачных

сред?

6. Что такое контейнеризация? Каковы особенности и инструменты защиты контейнеров?
7. Какие организационно-правовые и технические аспекты необходимо учитывать при размещении средств вычислительной техники (СВТ) вне контролируемой зоны?
8. Что представляет собой доверенная интеграционная платформа? Каковы её состав и назначение?
9. Какие методы и средства защиты комплекса технических средств от инвазивных воздействий применяются?
10. Как обеспечивается идентификация и аутентификация в доверенной интеграционной платформе? Какие подсистемы видеонаблюдения и охранной сигнализации интегрируются?

3.2.3. Комплект заданий для контрольной работы №3 для третьей аттестации

1. Что такое слепая обработка данных в системах искусственного интеллекта? Как организуется доверие участников к системе?
2. Каков состав и назначение СВТ в защищённом исполнении как части АС?
3. Как организовано оповещение участников о нештатных ситуациях в защищённой АС?
4. Какие методы и средства защиты данных, размещённых в АС, от неинвазивных и инвазивных воздействий существуют?
5. Что такое «новая биометрия»? В чём её отличие от классических средств биометрической защиты?
6. Назовите технические решения на базе новой биометрии и перспективы их развития.
7. Каковы общие принципы построения систем видеонаблюдения и контроля доступа (СВКД)?
8. Как осуществляется интеграция подсистемы информационной безопасности в общую информационную систему предприятия?
9. В чём заключается интеграция СЗИ НСД (средств защиты от несанкционированного доступа) и СКУД (систем контроля и управления доступом)?
10. Какие методы контроля доступа (дискреционная, мандатная, ролевая модели) применяются в современных АС и каковы особенности их реализации?

3.3. Задания для промежуточной аттестации (зачета и (или) экзамена)

Список вопросов к зачету

1. Автоматизированные системы: основные термины и определения. Жизненный цикл АС.
2. Понятие защищённой АС. Подходы к созданию защищённых АС.
3. Проблемы проектирования и реализации защищённых автоматизированных систем.
4. Подход к среде функционирования АС. Технические средства обеспечения доверенной среды.
5. Меры по обеспечению безопасности информации в государственных информационных системах (ГИС).
6. Требования к защите автоматизированных систем (по классам защищённости).
7. Персональные средства криптографической защиты информации (СКЗИ): проблемы использования и примеры решений.
8. Защищённые носители вычислительной среды, ключевой и аутентификационной

информации.

9. Инструменты контроля доступа для организации удалённой работы. Безопасный терминальный доступ.
10. Защита информационных систем персональных данных (ИСПДн) с применением технологии терминального доступа.
11. Системы виртуализации: состав и особенности функционирования.
12. Особенности защиты виртуальных машин. Доверенная загрузка и контроль целостности систем виртуализации.
13. Средства защиты систем виртуализации для гипервизоров KVM и VMware.
14. Инфраструктура безопасного «облака». Контейнеризация и инструменты защиты контейнеров.
15. Особенности размещения средств вычислительной техники вне контролируемой зоны: организационно-правовые и технические аспекты.
16. Доверенная интеграционная платформа: состав, назначение, модель угроз и модель нарушителя.
17. Методы и средства защиты комплекса технических средств от инвазивных воздействий. Защищённые стойки.
18. Идентификация и аутентификация в доверенной интеграционной платформе. Подсистемы видеонаблюдения и охранной сигнализации.
19. Слепая обработка данных в системах искусственного интеллекта. Организация доверия участников к системе.
20. СВТ в защищённом исполнении как часть АС: состав, назначение, взаимодействие участников.
21. Оповещение участников о нештатных ситуациях. Организация дистанционного голосования по ключевым вопросам.
22. Методы и средства защиты данных, размещённых в АС, от неинвазивных и инвазивных воздействий.
23. Методы контроля криптографических ключей в СВТ ЗИ.
24. Классические средства биометрической защиты. «Новая биометрия»: замысел защиты и технические решения.
25. Системы видеонаблюдения и контроля доступа (СВКД): общие принципы построения.
26. Интеграция подсистемы информационной безопасности в общую информационную систему предприятия.
27. Интеграция средств защиты от несанкционированного доступа (СЗИ НСД) и систем контроля и управления доступом (СКУД).
28. Интеграция СЗИ НСД и систем видеомониторинга.
29. Критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем.
30. Планирование и организация работы персонала АС с учётом требований по защите информации. Выбор и обоснование критериев эффективности функционирования защищённых АС.

3.4. Вопросы по остаточным знаниям

1. Дайте определение защищённой автоматизированной системы. Назовите основные этапы её жизненного цикла.
2. Какие меры по обеспечению безопасности информации применяются в государственных информационных системах?

3. Что такое доверенная среда функционирования и какими средствами она обеспечивается?
4. Перечислите основные проблемы использования персональных СКЗИ и пути их решения.
5. Какие существуют подходы к защите систем виртуализации (на примере гипервизоров KVM и VMware)?
6. Что такое доверенная интеграционная платформа и для каких целей она применяется?
7. В чём заключается слепая обработка данных в системах искусственного интеллекта и как обеспечивается доверие участников?
8. Назовите основные отличия «новой биометрии» от классических биометрических методов.
9. Как осуществляется интеграция систем контроля доступа (СКУД) и средств защиты от НСД?
10. Какие критерии используются для оценки эффективности и надёжности средств защиты информации?

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.

В ФОС размещается пример заполненного экзаменационного билета. Весь комплект экзаменационных билетов по дисциплине хранится на кафедре в соответствии с утвержденной номенклатурой дел.

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).