

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Баламирзоев Назим Лиодинович  
Должность: И.о. ректора  
Дата подписания: 09.11.2023 16:11:16  
Уникальный программный ключ:  
2a04bb882d7edb7f479cb280eb4aaadede1ccab49

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 «Инфраструктура открытых ключей в СЗИ»

Уровень образования

специалитет

(бакалавриат/магистратура/специалитет)

Специальность

10.05.03 Информационная безопасность  
автоматизированных систем

(код, наименование специальности)

Специализация

Безопасность открытых информационных систем

(наименование)

Разработчик



подпись

Качаева Г.И.

(ФИО уч. степень, уч. звание)

Фонд оценочных средств обсужден на заседании кафедры ИБ «20» сентября 2021г.,  
протокол № 2

Зав. кафедрой



подпись

Качаева Г.И.

(ФИО уч. степень, уч. звание)

г. Махачкала 2021

## СОДЕРЖАНИЕ

1. Область применения, цели и задачи фонда оценочных средств.....	3
2. Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля) .....	3
2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП.....	4
2.1.2. Этапы формирования компетенций.....	5
2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания.....	6
2.2.1. Показатели уровней сформированности компетенций на этапах их формирования ..	6
2.2.2. Описание шкал оценивания.....	8
3. Типовые контрольные задания, иные материалы и методические рекомендации, необходимые для оценки сформированности компетенций в процессе освоения ОПОП.....	9
3.1. Задания и вопросы для входного контроля.....	9
3.2. Оценочные средства и критерии сформированности компетенций.....	9
3.2.1. Аттестационная контрольная работа №1 .....	9
3.2.2. Аттестационная контрольная работа №2 .....	9
3.2.3. Аттестационная контрольная работа №3 .....	9

## **1. Область применения, цели и задачи фонда оценочных средств**

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Инфраструктура открытых ключей в СЗИ» 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 «Инфраструктура открытых ключей в СЗИ» предусмотрено формирование следующих компетенций:

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
- 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 <sup>1</sup>
ОПК-10 - Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1.1 - знает принципы организации и структуру систем защиты информации современных операционных систем	<p>знать: концепцию, назначение, организационно-технические аспекты использования РКІ; основные криптографические методы защиты информации; особенности использования ЭП/ЭЦП и РКІ в корпоративных информационных системах; что представляют собой сертификаты открытых ключей, ключевые носители и средства ЭП/ЭЦП; варианты настроек программных компонентов Microsoft Windows Server 2016/2019 и Windows 10 для реализации типовых регламентов оказания услуг.</p> <p>уметь: проектировать иерархию удостоверяющих центров (Certification Authority, CA), удовлетворяющую бизнес-требованиям; устанавливать службу Certificate Services для формирования иерархии CA; выполнять текущие задачи по управлению сертификатами и удостоверяющими центрами, формировать план аварийного восстановления службы Certificate Services; создавать и публиковать шаблоны</p>	
	ОПК-10.2.1 - умеет конфигурировать параметры системы защиты информации современных операционных систем		
	ОПК-10.1.3 - знает основные протоколы, используемые для защиты информации в вычислительных сетях		

<sup>1</sup> Наименования разделов и тем должен соответствовать рабочей программе дисциплины.

		сертификатов, шаблоны сертификатов; выпускать сертификаты вручную и автоматически, выпускать сертификаты для смарт-карт; внедрять ручное и автоматическое архивирование и восстановление ключей в Windows Server 2016/2019 PKI; устанавливать доверительные отношения между организациями, квалифицированное подчинение; внедрять смарт-карты в операционной среде Windows; настраивать защиту операционной среды Web с использованием SSL/TLS и аутентификации с использованием сертификатов для Web-приложений.	
--	--	---	--

### 2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине Инфраструктура открытых ключей в СЗИ 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-10 - Способен	ОПК-10.1.1 - знает принципы организации и	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена

использовать средства криптографической защиты информации при решении задач профессиональной деятельности	структуру систем защиты информации современных операционных систем						
	ОПК-10.2.1 - умеет конфигурировать параметры системы защиты информации современных операционных систем	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
	ОПК-10.1.3 - знает основные протоколы, используемые для защиты информации в вычислительных сетях	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 Инфраструктура открытых ключей в СЗИ 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.	Обучающимся усвоена взаимосвязь основных понятий дисциплины, в том числе для решения профессиональных задач. Ответы на вопросы оценочных средств самостоятельны,

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
	Даны развернутые ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции	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 материала 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 и навыков	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 пятибалльная, двадцатибалльная и стобальная шкалы знаний, умений, навыков.

Шкалы оценивания			Критерии оценивания
пятибалльная	двадцатибалльная	стобальная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 – 100 баллов	Показывает высокий уровень сформированности компетенций, т.е.: <ul style="list-style-type: none"> <li>- продемонстрирует глубокое и прочное усвоение материала;</li> <li>- исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал;</li> <li>- правильно формирует определения;</li> <li>- демонстрирует умения самостоятельной работы с нормативно-правовой литературой;</li> <li>- умеет делать выводы по излагаемому материалу.</li> </ul>
«Хорошо» - 4 баллов	«Хорошо» - 15 - 17 баллов	«Хорошо» - 70 - 84 баллов	Показывает достаточный уровень сформированности компетенций, т.е.: <ul style="list-style-type: none"> <li>- демонстрирует достаточно полное знание материала, основных теоретических положений;</li> <li>- достаточно последовательно, грамотно логически стройно излагает материал;</li> <li>- демонстрирует умения ориентироваться в нормальной литературе;</li> <li>- умеет делать достаточно обоснованные выводы по излагаемому материалу.</li> </ul>
«Удовлетворительно» - 3 баллов	«Удовлетворительно» - 12 - 14 баллов	«Удовлетворительно» - 56 – 69 баллов	Показывает пороговый уровень сформированности компетенций, т.е.: <ul style="list-style-type: none"> <li>- демонстрирует общее знание изучаемого материала;</li> <li>- испытывает серьезные затруднения при ответах на дополнительные вопросы;</li> <li>- знает основную рекомендуемую литературу;</li> <li>- умеет строить ответ в соответствии со структурой излагаемого материала.</li> </ul>
«Неудовлетворительно» - 2 баллов	«Неудовлетворительно» - 1-11 баллов	«Неудовлетворительно» - 1-55 баллов	Ставится в случае: <ul style="list-style-type: none"> <li>- незнания значительной части программного материала;</li> <li>- не владения понятийным аппаратом дисциплины;</li> <li>- допущения существенных ошибок при изложении учебного материала;</li> <li>- неумение строить ответ в соответствии со структурой излагаемого вопроса;</li> <li>- неумение делать выводы по излагаемому материалу.</li> </ul>



### **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. Аттестационная контрольная работа №1**

1. Обзор инфраструктуры открытых ключей (PKI)
2. Российские криптоалгоритмы. КриптоПро CSP. Сертификаты и удостоверяющие центры.
3. Планирование иерархии удостоверяющих центров.
4. Требования, влияющие на структуру иерархии удостоверяющих центров.
5. Типовые решения иерархии удостоверяющих центров.
6. Планирование иерархии удостоверяющих центров
7. Защита службы управления ключами на удостоверяющем управлении Windows Server 2016/2019 при помощи ПАКМ «КриптоПро HSM».
8. Создание иерархии удостоверяющих центров.
9. Создание удостоверяющего центра, отключенного от сети.
10. Проверка запросов на сертификат.
11. Создание иерархии удостоверяющих центров.
12. Планирование публикации списков отозванных сертификатов.
13. Установка подчиненного удостоверяющего центра.

##### **3.2.2. Аттестационная контрольная работа №2**

1. Управление инфраструктурой открытых ключей
2. Управление PKI. Управление сертификатами. Списки отозванных сертификатов.
3. Управление инфраструктурой открытых ключей
4. Протокол OCSP. Сетевой ответчик. Особенности применения КриптоПро OCSP. Управление удостоверяющими центрами.
5. Планирование аварийного восстановления.
6. Настройка шаблонов сертификатов.
7. Шаблоны сертификатов. Разработка и создание шаблона сертификатов.
8. Публикация шаблона сертификатов.
9. Управление изменениями в шаблонах сертификатов.
10. Настройка выпуска сертификатов
11. Выпуск сертификатов. Ручной выпуск сертификатов. Автоматический выпуск сертификатов.

##### **3.2.3. Аттестационная контрольная работа №3**

1. Настройка архивирования и восстановления ключей
2. Архивирование и восстановление ключей.
3. Внедрение ручного архивирования и восстановления ключей.
4. Внедрение автоматического архивирования и восстановления ключей.
5. Обеспечение конфиденциальности данных

6. Архитектура EFS. Шифрование данных с помощью EFS.
7. Особенности применения КриптоПро EFS.
8. Обеспечение конфиденциальности данных

### **Список вопросов к зачету**

1. Обзор инфраструктуры открытых ключей (PKI)
2. Российские криптоалгоритмы. КриптоПро CSP. Сертификаты и удостоверяющие центры.
3. Планирование иерархии удостоверяющих центров.
4. Требования, влияющие на структуру иерархии удостоверяющих центров.
5. Типовые решения иерархии удостоверяющих центров.
6. Планирование иерархии удостоверяющих центров
7. Защита службы управления ключами на удостоверяющем управлении Windows Server 2016/2019 при помощи ПАКМ «КриптоПро HSM».
8. Создание иерархии удостоверяющих центров.
9. Создание удостоверяющего центра, отключенного от сети.
10. Проверка запросов на сертификат.
11. Создание иерархии удостоверяющих центров.
12. Планирование публикации списков отозванных сертификатов.
13. Установка подчиненного удостоверяющего центра.
14. Управление инфраструктурой открытых ключей
15. Управление PKI. Управление сертификатами. Списки отозванных сертификатов.
16. Управление инфраструктурой открытых ключей
17. Протокол OCSP. Сетевой ответчик. Особенности применения КриптоПро OCSP. Управление удостоверяющими центрами.
18. Планирование аварийного восстановления.
19. Настройка шаблонов сертификатов.
20. Шаблоны сертификатов. Разработка и создание шаблона сертификатов.
21. Публикация шаблона сертификатов.
22. Управление изменениями в шаблонах сертификатов.
23. Настройка выпуска сертификатов
24. Выпуск сертификатов. Ручной выпуск сертификатов. Автоматический выпуск сертификатов.
25. Настройка архивирования и восстановления ключей
26. Архивирование и восстановление ключей.
27. Внедрение ручного архивирования и восстановления ключей.
28. Внедрение автоматического архивирования и восстановления ключей.
29. Обеспечение конфиденциальности данных
30. Архитектура EFS. Шифрование данных с помощью EFS.
31. Особенности применения КриптоПро EFS.
32. Обеспечение конфиденциальности данных
33. Обеспечение конфиденциальности данных. Архитектура EFS.
34. Шифрование данных с помощью EFS. Особенности применения КриптоПро EFS.
35. Настройка доверия между организациями
36. Дополнительные вопросы, связанные с иерархией удостоверяющих центров.
37. Настройка ограничений в файле Policy.inf.
38. Возможности квалифицированного подчинения.
39. Введение в смарт-карты. Выпуск сертификатов для смарт-карт.
40. Внедрение смарт-карт. Применение биометрической идентификации в смарт-картах. Особенности применения КриптоПро WinLogon.

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.

## Форма экзаменационного билета (пример оформления)

<p><u>Министерство науки и высшего образования РФ</u> <u>ФГБОУ ВО "Дагестанский государственный технический университет"</u> Дисциплина (модуль) <u>Защита информации от утечки по техническим каналам</u> Код, специальность <u>10.05.03 Информационная безопасность автоматизированных систем .....</u> Специализация <u>Безопасность открытых информационных систем</u> Кафедра ИБ Курс 4 Семестр 8 Форма обучения – <u>очная</u></p> <p style="text-align: center;"><b>ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1.</b></p> <p>1. Представление сил и средств защиты информации в виде системы. 2. 2 . Комплекс технических средств охраны.</p> <p>Экзаменатор.....Качаева Г.И.</p> <p>Утвержден на заседании кафедры (протокол №__ от _____ 20__ г.)</p> <p>Зав. кафедрой (название) .....Качаева Г.И.</p>
---

*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).