

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Баламирзоев Назим Лиодинович
Должность: Ректор
Дата подписания: 2024.11.04
Уникальный программный ключ:
5cf0d6f89e80f49a334f6a4ba58e91f3326b9926

Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина «Инфраструктура открытых ключей в СЗИ»

наименование дисциплины по ОПОП

для специальности 10.05.03 Информационная безопасность автоматизированных систем

код и полное наименование направления (специальности)

по специализации Безопасность открытых информационных систем,

факультет Компьютерных технологий и энергетики,

наименование факультета, где ведется дисциплина

кафедра Информационная безопасность.

наименование кафедры, за которой закреплена дисциплина

Форма обучения очная, курс 4, семестр (ы) 8.

очная, очно-заочная, заочная

г. Махачкала 2024

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем с учетом рекомендаций и ОПОП ВО по специализации Безопасность открытых информационных систем

/Разработчик  Алтухов А.А. старший преподаватель кафедры защиты информации МФТИ, начальник отдела разработки программного обеспечения средств доверенной загрузки (ПО СДЗ) "ОКБ САПР"
подпись (ФИО уч. степень, уч. звание)

«27» сентября 2024г.

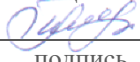
Зав. кафедрой, за которой закреплена дисциплина (модуль) ТПЗАС

 Качаева Г. И., к.э.н., доцент
подпись (ФИО уч. степень, уч. звание)

«27» сентября 2024г.

Программа одобрена на заседании выпускающей кафедры Информационная безопасность от 15 октября 2024года, протокол № 3.

Зав. выпускающей кафедрой по данному направлению (специальности, профилю)

 Качаева Г. И., к.э.н., доцент
подпись (ФИО уч. степень, уч. звание)

«15» октября 2024 г.

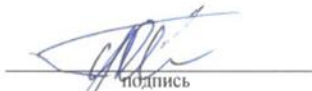
Программа одобрена на заседании Методического Совета факультета компьютерных технологий и энергетики от 17 октября 2024года, протокол № 2.

Председатель Методического совета факультета КТиЭ


подпись

Т.И. Исабекова, к.ф.-м.н., доцент
(ФИО уч. степень, уч. звание)

Декан факультета


подпись

Т.А. Рагимова
ФИО

Начальник УО


подпись

М.Т. Муталибов
ФИО

Проректор по УР


подпись

А.Ф. Демирова
ФИО

1. Цели и задачи освоения дисциплины.

В основе курса «Инфраструктура открытых ключей в СЗИ» лежит инженерная, прикладная криптография, что позволяет реализовать подход, ориентированный на понимание условий, при которых математические построения обеспечивают достаточный уровень защищенности информации. Инфраструктура открытых ключей рассматривается в применении к средствам защиты информации, а также через техническую реализацию СКЗИ. Целями освоения дисциплины являются изучение принципов и технологий построения и использования инфраструктуры открытых ключей в системах защиты информации.

Задачи дисциплины:

- получение представлений о подходах к использованию средств защиты информации и разработке систем защиты информации;
- ознакомление с особенностями и ограничениями применения инфраструктуры открытых ключей в контексте ее применения в средствах защиты информации;
- изучение аппаратной базы средств криптографической защиты информации.

2. Место дисциплины в структуре ОПОП

Дисциплина относится к части, формируемой участниками образовательных отношений.

Дисциплина базируется на следующих дисциплинах ОПОП:

- Основы информационной безопасности;
- Операционные системы;
- Алгоритмы и структуры данных;
- Введение в программирование и алгоритмы;
- Основы IT-технологий;
- Криптографические протоколы.

Требования к «входным» знаниям, умениям и готовностям, необходимым при освоении дисциплины и приобретенным в результате освоения предшествующих дисциплин:

- знание базовых понятий области обеспечения информационной безопасности;
- знание базовых понятий операционных систем различных видов;
- знание базовых понятий компьютерной безопасности;
- знание основных криптографических протоколов;
- знание порядка осуществления аутентификации взаимодействующих объектов, проверки подлинности отправителя и целостности передаваемых данных;
- готовность совершенствовать полученные умения по работе с операционными системами различных видов для установки, настройки и администрирования программно-аппаратных СЗИ.

Дисциплина предшествует изучению следующих дисциплин ОПОП:

- Программно-аппаратные средства обеспечения информационной безопасности;
- Открытые информационные системы;
- Технология построения защищенных автоматизированных систем;
- Аудит защищенности информации в автоматизированных системах;
- Комплексное обеспечение информационной безопасности автоматизированных систем;
- Безопасность операционных систем.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины «Инфраструктура открытых ключей в СЗИ» студент должен овладеть следующими компетенциями:

Код компетенции	Наименование компетенции	Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.5 - умеет критически анализировать проблемные ситуации и вырабатывать стратегию действий в ходе решения профессиональных задач
ОПК-7	Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ОПК-7.9 - умеет применять известные методы программирования и возможности базового языка программирования для решения - типовых профессиональных задач
ОПК 4.3	Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.1. Знает принципы устройства и функционирования программных, программно-аппаратных и технических средств защиты информации. ОПК-4.3.1. Умеет использовать программные, программно-аппаратные (в том числе криптографические) и технические средства для защиты информации в автоматизированных системах. ОПК-4.3.1. Владеет методами установки и настройки программных, программно-аппаратных и технических средств защиты информации..
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности.	ОПК-8.4 - умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.4 - умеет использовать СКЗИ для решения задач профессиональной деятельности
ОПК-10.	Способен в качестве	ОПК-10.2 - умеет

	технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности
--	--	---

4. Объем и содержание дисциплины (модуля)

Форма обучения	очная	очно-заочная	заочная
Общая трудоемкость по дисциплине (ЗЕТ/ в часах)	3/108	3/108	—
Семестр	5	5	—
Лекции, час	17	9	—
Практические занятия, час	—	—	—
Лабораторные занятия, час	17	9	—
Самостоятельная работа, час	74	108	—
Курсовой проект (работа), РГР, семестр	—	—	—
Зачет (при заочной форме 4 часа отводится на контроль)	+	+	—
Часы на экзамен (при очной, очно-заочной формах 1 ЗЕТ – 36 часов , при заочной форме 9 часов отводится на контроль)	—	—	—

4.1.Содержание дисциплины (модуля)

№ п/п	Раздел дисциплины, тема лекции и вопросы	Очная форма				Очно-заочная форма				Заочная форма			
		ЛК	ПЗ	ЛБ	СР	ЛК	ПЗ	ЛБ	СР	ЛК	ПЗ	ЛБ	СР
Раздел 1. Введение в предметную область. Базовые понятия криптографии													
1	Социальная функция электронной подписи. Основные понятия криптографии и задачи криптографических методов защиты информации. Симметричное и асимметричное шифрование. Открытые и закрытые ключи. Криптографические методы с открытым ключом: электронная подпись, шифрование, аутентификация	1	–	–	8	1	–	1	8	–	–	–	–
Раздел 2. Условия безопасного применения криптографических механизмов													
2	Уязвимости криптографических систем и атаки на них. Криптосистема Эль-Гамала. Обоснование аппаратной реализации. Атака Грунтовича. Управление ключевой системой. Ключ как объект атаки. Защищенность ключа. Математические ограничения криптографических систем. Реализация и проблемы реализации криптографических систем. Угрозы со стороны среды исполнения криптографических систем.	1	–	–	4	–	–	–	8	–	–	–	–
Раздел 3. Системы и решения с использованием криптографических систем с открытым ключом													
3	Изучение принципов использования криптографических систем с открытым ключом на примере SSH, пакетный менеджер, почта. Анализ безопасности рассмотренных решений	1	–	2	4	1	–	1	8	–	–	–	–
Раздел 4. Доверенная среда													

4	Организация доверенной среды и резидентный компонент безопасности. Среда функционирования криптографии. Случайные числа. Датчик случайных чисел. Генератор случайных чисел	1	–	2	6	–	–	–	8	–	–	–	–
<i>Раздел 5. Отчуждаемые ключевые хранилища</i>													
5	Отчуждаемые ключевые хранилища: смарт-карты, USB-ключи. Цели и задачи данного класса решений, принципы их устройства. Принципиальные ограничения использования данных решений. Использование смарт-карт и USB-ключей при разработке СЗИ на примере стандартов PKCS#11	1	–	–	4	1	–	1	8	–	–	–	–
<i>Раздел 6. Криптографические системы с открытым ключом в СЗИ</i>													
6	Защита канала, подпись документов. Организация системы безопасного обновления на примере модулей расширения m-TrusT. Организация доверенной загрузки в UEFI системах с TPM (Secure Boot). Аутентификация пользователя	1	–	5	4	–	–	–	8	–	–	–	–
<i>Раздел 7. Управление ключами</i>													
7	Создание, хранение, обработка, удаление и учет ключей. Сертификат открытого ключа	1	–	2	6	1	1	–	6	–	–	–	–
<i>Раздел 8. Инфраструктуры открытых ключей (PKI)</i>													
8	Цели, принципы и основные задачи инфраструктуры открытых ключей. Центр сертификации (CA), сертификаты и цепочки сертификации	1	–	–	4	1	1	–	6	–	–	–	–
9	Инфраструктура открытых ключей как объект защиты и компонент СЗИ	1	–	–	6	1	1	–	6	–	–	–	–

10	Проектирование и внедрение инфраструктуры открытых ключей. Применение инфраструктуры открытых ключей в современных системах. Защита электронной почты. Использование в веб-приложениях	1	–	2	4	–	–	–	6	–	–	–	–
<i>Раздел 9. Безопасность и угрозы РКІ</i>													
11	Уязвимости инфраструктуры открытых ключей. Меры безопасности и защита от угроз.	1	–	–	4	1	–	1	8	–	–	–	–
12	Роль аппаратных средств защиты информации в обеспечении защиты инфраструктуры открытых ключей. Неизвлекаемые ключи	1	–	–	6	–	–	–	6	–	–	–	–
<i>Раздел 10. Защита ГИС, ИСПДн и КИИ</i>													
13	Проблемы интеграции СЗИ и корпоративных инфраструктур открытых ключей при обеспечении защиты ГИС, ИСПДн и КИИ	1	–	1	6	1	–	1	8	–	–	–	–
<i>Раздел 11. Альтернативные решения</i>													
14	Альтернативы инфраструктуре открытых ключей	2	–	1	5	–	–	–	6	–	–	–	–
<i>Раздел 12. Атаки на микроконтроллеры и аппаратные СЗИ</i>													
15	Инвазивные атаки, glitch-атаки, атаки по стороннему каналу. Подходы к организации защищенного хранения и обработки ключей. Защищенная инфраструктура открытых ключей для СЗИ. Неизвлекаемые ключи. Хранилища ключей. Ключевое хранилище на основе закона Клайперсона-Менделеева	2	–	2	4	1	–	1	8	–	–	–	–

Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре)	Входной контроль 1 аттестация 1-4 тема – комплексная теоретико-практическая задача № 1 2 аттестация 5-9 тема – комплексная теоретико-практическая задача № 2 3 аттестация 10-15 тема – комплексная теоретико-практическая задача № 3				Входной контроль 1 аттестация 1-4 тема – комплексная теоретико-практическая задача № 1 2 аттестация 5-9 тема – комплексная теоретико-практическая задача № 2 3 аттестация 10-15 тема – комплексная теоретико-практическая задача № 3				—			
Форма промежуточной аттестации (по семестрам)	Зачет				Зачет				Зачет/зачет с оценкой/экзамен			
Итого	17	—	17	74	9		9	108				

4.2. Содержание лабораторных (практических) занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного (практического, семинарского) занятия	Количество часов			Рекомендуемая литература и методические разработки (№ источника из списка литературы)
			Очно	Очно-заочно	Заочно	
1	2	3	4	5	6	7
1	3	Применение криптографических систем с открытым ключом: SSH, пакетный менеджер	2	1	—	6
2	4	Генераторы случайных чисел	2	1	—	4
3	6	Организация системы безопасного обновления на примере модулей расширения m-Trust	3	1	—	11, 13
4	6	Организация доверенной загрузки в UEFI системах с TPM (Secure Boot)	2	1	—	5
5	7	Жизненный цикл криптографических ключей	2	1	—	1
6	11	Защита электронной почты с использованием инфраструктуры открытых ключей	2	2	—	6
7	15	Средства реализации инвазивных атак по стороннему каналу	4	2	—	6
ИТОГО			17	9	—	

4.3. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Количество часов из содержания дисциплины			Рекомендуемая литература и источники информации	Формы контроля СРС
		Очно	Очно-заочно	Заочно		
1	2	3	4	5	6	7
1	Основные понятия криптографии	8	12	–	1, 2	Устный опрос
2	Виды шифрования	8	12	–	1,2	Устный опрос
3	Цифровой сертификат Х. 509	8	12	–	1, 6	Устный опрос
4	ГОСТ, ГОСТ Р ИСО/МЭК 7816-3-2013 основные положения	8	12	–	3, 5	Устный опрос
5	Доверенные информационные технологии	8	12	–	5	Устный опрос
6	Автономность и независимость РКБ от защищаемой среды	8	12	–	4, 9, 12	Устный опрос
7	Изучение стандарта PKCS#11	8	12	–		Устный опрос
8	Криптографическая защита КИИ	8	12	–	5, 10, 11	Устный опрос
9	Криптографическая защита информационного взаимодействия объектов КИИ на базе платформы m-Trust	10	12	–	5, 10, 11, 13	Устный опрос
ИТОГО		74	108	–	–	Зачет

5. Образовательные технологии

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю):

- дистанционные образовательные технологии;
- электронные средства обучения;
- мастер-классы;
- мультимедийные технологии.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

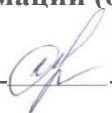
В рамках дисциплины (модуля) предусмотрено аттестации текущего контроля успеваемости и промежуточная аттестация.

Каждый текущий контроль успеваемости представляет собой контрольную работу в форме выполнения решения комплексной теоретико-практической задачи с письменным отчетом и устным опросом. Выполнение СРС контролируется путем подготовки небольшого доклада и устного опроса по изученному материалу. В течение семестра предусмотрено одно эссе по одной из тем о состоянии изучаемых областей информационной безопасности и перспективы ее развития.

Рефераты и курсовые работы в рамках дисциплины (модуля) не предусмотрены.

Фонд оценочных средств приведен в Приложении А к настоящей РПД.

7. Учебно-методическое и информационное обеспечение дисциплины
Рекомендуемая литература и источники информации (основная и дополнительная)

Зав. библиотекой _____  _____ Сулейманова О.Ш.

№ п/п	Виды занятий	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение, электронно- библиотечные и Интернет ресурсы	Автор(ы)	Издательс тво и год издания	Количество изданий	
					В библиотеке	
1	2	3	4	5	6	7
Основная литература						
1	ЛК, ЛБ, СР	Основы криптографии	Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.	Гелиос АПВ, 2005	URL: https://e.lanbook.com/book/162235	
2	ЛК, СР	Криптографические методы и средства защиты информации: учеб. пособие	Бутакова Н.Г.	ИЦ «Интерме дия», 2019	URL: https://e.lanbook.com/book/216491	
3	ЛК, СР	Электронная подпись. Просто о сложном	Шадур А.А., Гущин Е.Е.	Ridero, 2019	URL: https://e.lanbook.com/book/176563	
4	ЛК, ЛБ, СР	Теория, применение и оценка качества генераторов псевдослучайных последовательностей	Иванов М.А., Чугунков И.В.	КУДИЦ- ОБРАЗ 2003	URL: https://e.lanbook.com/book/118230	
5	ЛК, СР	Доверенные информационные технологии: от архитектуры к системам и средствам, 2-е изд.	Конявский В.А., Конявская С.В.	URSS, 2021	URL: https://e.lanbook.com/book/182252	
Дополнительная литература						
6	ЛК, ЛБ, СР	Прикладная криптография: протоколы, алгоритмы и исходные коды на языке С	Шнайер Б.	Альфа- книга, 2017	URL: https://e.lanbook.com/book/118990	
7	ЛК	Инфраструктуры открытых ключей	Полянская О.Ю., Горбатов В.С.	Просвеще ние/Бином , 2013	URL: https://e.lanbook.com/book/187652	

8	ЛК	Теоретико-числовые методы в криптографии.	Рожков А.В., Ниссенбаум О.В.	Изд-во Тюменско го гос. Ун- та, 2007	https://studizba.com/how/1127102-1-av-rozhkov-ov-nissenbaum-teoretiko.html
9	ЛК, СР	Основы технологии РКІ	Горбатов В.С., Полянская О.Ю.	Горячая линия-Телеком, 2011	
10	ЛК, СР	Мантра о неизвлекаемом ключе. Криптографическая защита в КИИ	Конявская С.В.	Information Security /Информационная безопасность. М., 2023. № 6. С.56-57	
11	ЛК, ЛБ, СР	Решения для криптографической защиты сетевого взаимодействия объектов КИИ на базе платформы m-TrusT	Конявская С.В.	Information Security /Информационная безопасность. М., 2023. № 6. С.51	10
12	ЛК, СР	Платформенные решения ОКБ САПР как основа построения защищенных ИС. /	Каннер Т.М.	Медиа Группа «Авангард», 2020	URL: https://www.okbsapr.ru/library/publications/platformennye-resheniya-okb-sapr-kak-osnova-postroeniya-zashchishchennykh-is1
13	ЛК, ЛБ, СР	Сайт производителя программно-аппаратных комплексов СЗИ:			URL: https://www.okbsapr.ru

7. Материально-техническое обеспечение дисциплины (модуля)_____

Учебная аудитория дисциплины (модуля) «Инфраструктура открытых ключей в СЗИ» оснащена следующим учебно-лабораторным оборудованием:

- ПК преподавателя с ОС Windows с установленной программой просмотра документов в формате pdf (например, Adobe Acrobat Reader DC) и программой виртуализации (например, VirtualBox), средствами организации дистанционного обучения;
- мультимедийное оборудование, доска;
- ПК студентов с ОС Windows с установленной программой просмотра документов в формате pdf (например, Adobe Acrobat Reader DC) и программой виртуализации (например, VirtualBox);

Специальные условия инвалидам и лицам с ограниченными возможностями здоровья (ОВЗ)

Специальные условия обучения и направления работы с инвалидами и лицами с ОВЗ определены на основании:

- Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;
- Федерального закона от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;
- приказа Минобрнауки России от 05.04.2017 № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;
- методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утвержденных Минобрнауки России 08.04.2014 № АК-44/05вн).

Под специальными условиями для получения образования обучающихся с ОВЗ понимаются условия обучения, воспитания и развития, включающие в себя использование при необходимости адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего необходимую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания ДГТУ и другие условия, без которых невозможно или затруднено освоение ОПОП обучающихся с ОВЗ.

Обучение в рамках учебной дисциплины обучающихся с ОВЗ осуществляется ДГТУ с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение по учебной дисциплине обучающихся с ОВЗ может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

В целях доступности обучения по дисциплине обеспечивается:

- 1) для лиц с ограниченными возможностями здоровья по зрению:
 - наличие альтернативной версии официального сайта ДГТУ в сети «Интернет» для слабовидящих;
 - весь необходимый для изучения материал, согласно учебному плану (в том числе, для обучающихся по индивидуальным учебным планам) предоставляется в электронном виде на диске.
 - индивидуальное равномерное освещение не менее 300 люкс;
 - присутствие ассистента, оказывающего обучающемуся необходимую помощь;
 - обеспечение возможности выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);
 - обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию ДГТУ.
- 2) для лиц с ОВЗ по слуху:
 - наличие микрофонов и звукоусиливающей аппаратуры коллективного пользования (аудиоколонки);
- 3) для лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и других приспособлений).

Перед началом обучения могут проводиться консультативные занятия, позволяющие студентам с ОВЗ адаптироваться к учебному процессу.

В процессе ведения учебной дисциплины научно-педагогическим работникам рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи обучающимся с ОВЗ в установлении полноценных межличностных отношений с другими обучающимися, создании комфортного психологического климата в учебной группе.

Особенности проведения текущей и промежуточной аттестации по дисциплине для обучающихся с ОВЗ устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и др.). При необходимости предоставляется дополнительное время для подготовки ответа на зачете или экзамене.

9. Лист изменений и дополнений к рабочей программе

Дополнения и изменения в рабочей программе на 20___/20___ учебный год.

В рабочую программу вносятся следующие изменения:

1.;
2.;
3.;
4.;
5.

или делается отметка о нецелесообразности внесения каких-либо изменений или дополнений на данный учебный год.

Рабочая программа пересмотрена и одобрена на заседании кафедры _____
от _____ года, протокол № _____.

Заведующий кафедрой _____
(название кафедры) (подпись, дата) (ФИО, уч. степень, уч. звание)

Согласовано:

Декан (директор) _____
(подпись, дата) (ФИО, уч. степень, уч. звание)

Председатель МС факультета _____
(подпись, дата) (ФИО, уч. степень, уч. звание)

(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

бакалавриат

(бакалавриат/магистратура/специалитет)

Направление подготовки
бакалавриата/магистратуры/специальность

10.03.01 Информационная безопасность

(код, наименование направления подготовки/специальности)

Профиль направления
подготовки/специализация

**Безопасность автоматизированных систем (по
отрасли или в сфере профессиональной
деятельности)**

(наименование)

Разработчик

подпись

(ФИО уч. степень, уч. звание)

Фонд оценочных средств обсужден на заседании кафедры Информационная
безопасность « » 20 г., протокол №

Зав. кафедрой

подпись

Качаева Г.И. к.э.н., доцент

(ФИО уч. степень, уч. звание)

г. Махачкала 2024

СОДЕРЖАНИЕ

1. Область применения, цели и задачи фонда оценочных средств
2. Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля)
 - 2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП
 - 2.1.2. Этапы формирования компетенций
 - 2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания
 - 2.2.1. Показатели уровней сформированности компетенций на этапах их формирования
 - 2.2.2. Описание шкал оценивания
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
 - 3.2. Оценочные средства и критерии сформированности компетенций
 - 3.3. Задания для промежуточной аттестации (зачета и (или) экзамена)

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 направлению подготовки/специальности 10.03.01 Информационная безопасность.

Рабочей программой дисциплины «Инфраструктура открытых ключей в СЗИ» предусмотрено формирование следующих компетенций:

- 1) УК-1 – способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
- 2) ОПК-7– Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности
- 3) ОПК 4.3– Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем
- 5) ОПК-8 – Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности.
- 4) ОПК-9 – Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности
- 5) ОПК-10 – Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

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.

При освоении дисциплины используются следующие оценочные средства:

- Комплексные теоретико-практические задачи (КТПЗ) №1, №2, №3.
- Устные опросы (для контроля СРС).
- Теоретико-практическая задача и список смежных вопросов (для проведения зачета).

2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП

В результате освоения дисциплины «Инфраструктура открытых ключей в СЗИ» студент должен овладеть следующими компетенциями:

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-1.5 - умеет критически анализировать проблемные ситуации и вырабатывать стратегию действий в ходе решения профессиональных задач	- способен выработать критерии и требования к продуктам и проектным решения для решения практической бизнес задачи - умеет осуществлять поиск и подбор СЗИ, технически и проектные решения под заданные критерии - умеет анализировать ограничения и проблемы существующих решений и методов их использования - способен получить данных об актуальных уязвимостях и проблемах безопасности применяемых решений	Раздел 1. Введение в предметную область. Базовые понятия криптографии Раздел 2. Условия безопасного применения криптографических механизмов Раздел 9. Безопасность и угрозы РКІ Раздел 12. Атаки на микроконтроллеры и аппаратные СЗИ
ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной	ОПК-7.9 - умеет применять известные методы программирования и возможности базового языка программирования для решения - типовых профессиональных задач	- может применять языки программирования и средства разработки для решения прикладной задачи - может подобрать для решения прикладной задачи наиболее подходящие средства	Раздел 3. Системы и решения с использованием криптографических систем с открытым ключом Раздел 4. Доверенная среда Раздел 5. Отчуждаемые ключевые хранилища

¹ Наименования разделов и тем должен соответствовать рабочей программе дисциплины.

деятельности		- способе использовать незнакомы языки программирования для прототипирования и оценки возможности применения языка для решения практической задачи	Раздел 7. Управление ключами Раздел 8. Инфраструктуры открытых ключей (PKI) Раздел 10. Защита ГИС, ИСПДн и КИИ
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно- технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.4 - умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности	- может подбирать актуальные материалы научных статей по заданной теме для поиска перспективных проектных решений поставленной задачи - умеет анализировать подобранные материалы с целью поиска новых технологий и подход по решению задачи. - умеет подбирать материалы с целью поиска существующих решений поставленных задач	Раздел 4. Доверенная среда Раздел 5. Отчуждаемые ключевые хранилища Раздел 11. Альтернативные решения Раздел 12. Атаки на микроконтроллеры и аппаратные СЗИ
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.4 - умеет использовать СКЗИ для решения задач профессиональной деятельности	- способен настраивать средства использующие технологию открытых ключей - способен использовать существующие продукты и технологии для решения поставленных задач - понимает принцип и ограничения существующих средствах на базе технологии открытых ключей	Раздел 3. Системы и решения с использованием криптографических систем с открытым ключом Раздел 7. Управление ключами Раздел 8. Инфраструктуры открытых ключей (PKI)
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение	ОПК-10.2 - умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	- способен составить список организационных требований для конкретного технического решения или продукта с целью реализации политики безопасности - способен реализовать отдельные положения политик безопасности	Раздел 3. Системы и решения с использованием Раздел 9. Безопасность и угрозы PKI Раздел 10. Защита ГИС, ИСПДн и КИИ

комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты		используя настройки конкретных продуктов - способен выявить ограничения технических решений для реализации отдельных требований политики безопасности. - способе описать правила	
ОПК 4.3. -Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.1. Знает принципы устройства и функционирования программных, программно-аппаратных и технических средств защиты информации.	- способен понимать ограничения применяемых средств защиты для решения реальных задач, основываясь на понимании внутренних принципов работы СЗИ - способен выставлять дополнительные требования по улучшению СЗИ для решения поставленной задачи	Раздел 4. Доверенная среда Раздел 5. Отчуждаемые ключевые хранилища Раздел 6. Криптографические системы с открытым ключом в СЗИ
	ОПК-4.3.2. Умеет использовать программные, программно-аппаратные (в том числе криптографические) и технические средства для защиты информации в автоматизированных системах.	- умеет настраивать СЗИ - умеет тестировать и оценивать функциональную полноту не знакомых и ранее не знакомых средств защиты информации - оценивать полноту документации по настройке и использованию СЗИ	Раздел 3. Системы и решения с использованием криптографических систем с открытым ключом Раздел 4. Доверенная среда Раздел 5. Отчуждаемые ключевые хранилища
	ОПК-4.3.3. Владеет методами установки и настройки программных, программно-аппаратных и технических средств защиты информации.	- внедрять СЗИ в существующие системы - организовывать процесс интеграции СЗИ	Раздел 3. Системы и решения с использованием криптографических систем с открытым ключом Раздел 4. Доверенная среда Раздел 5. Отчуждаемые ключевые хранилища

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Инфраструктура открытых ключей в СЗИ» определяется на следующих этапах:

1. Этап текущих аттестаций

- Контрольные работы в виде тестов: КТПЗ №1, КТПЗ №2, КТПЗ №3.
- Устные опросы по результатам СРС.

2. Этап промежуточных аттестаций

- Теоретико-практическая задача и и устный опрос.

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	Эссе	СРС	КР/КП	Промежуточная аттестация
1		2	3	4	5	6	7	8
УК – 1	УК-1.5 - умеет критически анализировать проблемные ситуации и вырабатывать стратегию действий в ходе решения профессиональных задач	КТПЗ №1	КТПЗ №2	КТПЗ №3	Эссе	Устный опрос	-	Теоретико-практическая задача
ОПК-4.3	ОПК-4.3.1 Знает принципы устройства и функционирования программных, программно-аппаратных и технических средств защиты информации.		КТПЗ №2			Устный опрос		
	ОПК-4.3.2. Умеет использовать							

	программные, программно-аппаратные (в том числе криптографические) и технические средства для защиты информации в автоматизированных системах							
	ОПК-4.3.3. Владеет методами установки и настройки программных, программно-аппаратных и технических средств защиты информации.							
ОПК-7	ОПК-7.9 - умеет применять известные методы программирования и возможности базового языка программирования для решения - типовых профессиональных задач		КТПЗ №2	КТПЗ №3		Устный опрос		
ОПК-8	ОПК-8.4 - умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности			КТПЗ №3		Устный опрос		
ОПК-9	ОПК-9.4 - умеет использовать СКЗИ для решения задач профессиональной деятельности	КТПЗ №1		КТПЗ №3		Устный опрос		
ОПК-10	ОПК-10.2 - умеет конфигурировать программно-аппаратные	КТПЗ №1	КТПЗ №2			Устный опрос		

	средства защиты информации в соответствии с заданными политиками безопасности							
--	---	--	--	--	--	--	--	--

СРС – самостоятельная работа студентов;

КР – курсовая работа;

КП – курсовой проект.

КТПЗ – комплексные теоретико-практическая задачи

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. Продemonстрированные умение применять практические навыки для решения. Ответы на вопросы оценочных средств полные и верные. Даны развернутые ответы на дополнительные вопросы по предложенным решениям 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. Есть общие подходы и понимания решения практических задач. В ответах на вопросы/задания оценочных средств изложено понимание вопроса, дано достаточно	Сформированы в целом системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные, грамотные. Продemonстрирован повышенный уровень владения практическими умениями и навыками.

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
	подробное описание ответа, приведены и раскрыты в тезисной форме основные понятия. Ответ отражает основное знание материала, а также наличие, с незначительными пробелами, умений и навыков по изучаемой дисциплине. Допустимы единичные негрубые ошибки. Обучающимся продемонстрирован повышенный уровень освоения компетенции	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. Есть понимания решения индивидуальной практической задачи. Обучающимся продемонстрирован базовый уровень освоения компетенции	Обучающийся владеет знаниями основного материал на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продemonстрирован 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	

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

Примеры типовых вопросов для входного контроля:

1. Базовые понятия в области обеспечения информационной безопасности.
2. Базовые понятия операционных систем различных видов.
3. Базовые понятия компьютерной безопасности.
4. Базовые навыки основ программирования.
5. Базовые навыки владения IT-технологиями.
6. Базовые понятия сетевых технологий.
7. Базовые понятия основ цифровой электроники.

Входной контроль осуществляется путем устного опроса обучающихся в соответствии с типовыми вопросами входного контроля.

Критерии оценки уровня сформированности компетенций при проведении входного контроля:

- оценка «отлично»: обучающимся дан полный, развернутый ответ на поставленный вопрос; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Обучающийся владеет терминологией, способен приводить примеры, высказывает свою точку зрения с опорой на знания и опыт;

- оценка «хорошо»: обучающимся дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ логичен, выстроен, но совершены единичные ошибки. Не в полной мере владеет знаниями по предшествующим дисциплинам. Даны ответы на дополнительные, поясняющие вопросы;

- оценка «удовлетворительно»: ответ на вопрос не полный, с ошибками. Обучающийся путается в деталях, с затруднением пользуется профессиональной терминологией. Есть замечания к построению ответа, к логике и последовательности изложения. Не отвечает на дополнительные вопросы;

- оценка «неудовлетворительно»: ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствует фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса с другими объектами предшествующих дисциплин, речь неграмотная, не используется профессиональная терминология. Ответы на дополнительные вопросы не даны или неверные.

3.2. Оценочные средства и критерии сформированности компетенций

Примеры индивидуальных комплексных теоретико-практических задач (КТПЗ) № 1 по разделу 1 «Введение в предметную область. Базовые понятия криптографии», разделу 2 «Условия безопасного применения криптографических механизмов», разделу 3 «Системы и решения с использованием криптографических систем с открытым ключом» и разделу 4 «Доверенная среда»

- Время выполнения 80 мин.
- Форма работы – самостоятельная, индивидуальная.

Примеры задач:

1. Спроектируйте решение для безопасного обновления BIOS компьютера.

- Опишите потенциальные проблемы, связанные с обеспечением конфиденциальности данных на рабочем ноутбуке сотрудника с использованием шифрования.
- Спроектируйте систему для защищенного выставления оценок в типовой школе с использованием криптографических средств.
- Предложите комплекс программных и аппаратных мер для обеспечения безопасности интернет-банкинга.
- Создайте приложение для проверки подлинности передаваемых сообщений.
- Разработайте способ организации удаленного доступа сотрудников с использованием подхода доверенного сеанса связи.
- Организуите безопасное удаленное подключение к ЭВМ на ОС Астра Linux

Критерии оценки уровня сформированности компетенций при выполнении теста:

Оценка	Показатели*
Отлично	Предложено полное решение задачи с детальными ответами на три или более уточняющих вопроса, касающихся обсуждаемых тем. Продемонстрировано глубокое понимание возможных ограничений и недостатков предлагаемого решения
Хорошо	Представлено техническое решение или полное письменное решение на теоретический вопрос, однако отсутствуют ответы на уточняющие вопросы в рамках тем работы. Либо предложено неполное практическое или письменное решение, но даны ответы как минимум на три уточняющих вопроса.
Удовлетворительно	Предложено общее примерное решение задачи. Даны ответы как минимум на два базовых общих вопроса по теме задачи.
Неудовлетворительно	Решение задачи не предложено. Не дано хотя бы 2 полных ответов на базовые общие вопросы

Примеры индивидуальных комплексных теоретико-практических задач (КТПЗ) № 2 по разделу 5 «Отчуждаемые ключевые хранилища», разделу 6 «Криптографические системы с открытым ключом в СЗИ», разделу 7 «Управление ключами», разделу 8 «Инфраструктура открытых ключей (PKI)» и разделу 9 «Безопасность и угрозы PKI»

- Время выполнения 80мин.
- Форма работы – самостоятельная, индивидуальная.

Примеры задач:

- Напишите приложение получения случайных чисел со смарт-карточки
- Сгенерируйте ключевую пару для алгоритма подписи на токене. В чем недостаток этого решения
- Создайте решение по автоматической генерации сертификатов пользователя для небольшой организации
- Настройте идентификацию-аутентификацию в ОС Astra Linux по смарт-карте/токене.

5. Опишите возможные последствия для организации утери USB-токена с ключами для ЭП.

Критерии оценки уровня сформированности компетенций при выполнении теста:

Оценка	Показатели*
Отлично	Предложено полное решение задачи с детальными ответами на три или более уточняющих вопроса, касающихся обсуждаемых тем. Продemonстрировано глубокое понимание возможных ограничений и недостатков предлагаемого решения
Хорошо	Представлено техническое решение или полное письменное решение на теоретический вопрос, однако отсутствуют ответы на уточняющие вопросы в рамках тем работы. Либо предложено неполное практическое или письменное решение, но даны ответы как минимум на три уточняющих вопроса.
Удовлетворительно	Предложено общее примерное решение задачи. Даны ответы как минимум на два базовых общих вопроса по теме задачи.
Неудовлетворительно	Решение задачи не предложено. Не дано хотя бы 2 полных ответов на базовые общие вопросы

Примеры индивидуальных комплексных теоретико-практических задач (КТПЗ) № 3 по разделу 10 «Защита ГИС, ИСПДн и КИИ», разделу 11 «Альтернативные решения» и разделу 12 «Атаки на микроконтроллеры и аппаратные СЗИ»

- Время выполнения 80мин.
 - Форма работы – самостоятельная, индивидуальная.
- Примеры задач:

1. Спроектируйте решение по безопасные обновления ПО на ЭВМ, демонстрирующем уличную рекламу на базе ОС Linux.
2. Опишите комплекс атак на типовой АРМ, на котором осуществляется электронная подпись документов.
3. Составить список угроз системы обновления ПО для ОС Linux на примере Debian.
4. Подготовьте пакет обновления для ОС RedOS демонстрационного приложения.
5. Опишите решение по защите от инвазивных атак на ключ.

Критерии оценки уровня сформированности компетенций при выполнении теста:

Оценка	Показатели*
Отлично	Предложено полное решение задачи с детальными ответами на три или более уточняющих вопроса, касающихся обсуждаемых тем. Продemonстрировано

	глубокое понимание возможных ограничений и недостатков предлагаемого решения
Хорошо	Представлено техническое решение или полное письменное решение на теоретический вопрос, однако отсутствуют ответы на уточняющие вопросы в рамках тем работы. Либо предложено неполное практическое или письменное решение, но даны ответы как минимум на три уточняющих вопроса.
Удовлетворительно	Предложено общее примерное решение задачи. Даны ответы как минимум на два базовых общих вопроса по теме задачи.
Неудовлетворительно	Решение задачи не предложено. Не дано хотя бы 2 полных ответов на базовые общие вопросы

Устный опрос по разделу 1 «Введение в предметную область. Базовые понятия криптографии»

- Форма опроса – фронтальный.

Пример заданий к устному опросу.

1. Социальная функция электронной подписи.
2. Основные понятия криптографии и задачи криптографических методов защиты информации.
3. Симметричное и асимметричное шифрование.
4. Организация доверенной среды и резидентный компонент безопасности.
5. Открытые и закрытые ключи.
6. Криптографические методы с открытым ключом: электронная подпись, шифрование, аутентификация.

Критерии оценки уровня сформированности компетенций для устного опроса:

- оценка «отлично»: обучающимся дан полный, развернутый ответ на поставленный вопрос; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание по дисциплине демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей. Обучающийся владеет терминологией, способен приводить примеры, высказывает свою точку зрения с опорой на знания и опыт;

- оценка «хорошо»: обучающимся дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ логичен, выстроен, но совершены единичные ошибки. Не в полной мере владеет знаниями по всей дисциплине. Даны ответы на дополнительные, поясняющие вопросы;

- оценка «удовлетворительно»: ответ на вопрос не полный, с ошибками. Обучающийся путается в деталях, с затруднением пользуется профессиональной терминологией. Есть замечания к построению ответа, к логике и последовательности изложения. Не отвечает на дополнительные вопросы;

- оценка «неудовлетворительно»: ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствует фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса с другими объектами

дисциплины, речь неграмотная, не используется профессиональная терминология. Ответы на дополнительные вопросы не даны или неверные.

Устный опрос по разделу 2 «Условия безопасного применения криптографических механизмов»

- Содержит 6 вопросов.
- Форма опроса – фронтальный.

Пример заданий к устному опросу.

1. Уязвимости криптографических систем и атаки на них.
2. Криптосистема Эль-Гамала. Обоснование аппаратной реализации. Атака Грунговича.
3. Управление ключевой системой. Ключ как объект атаки. Защищенность ключа.
4. Математические ограничения криптографических систем.
5. Реализация и проблемы реализации криптографических систем.
6. Угрозы со стороны среды исполнения криптографических систем.

Критерии оценки уровня сформированности компетенций для устного опроса:

- оценка «отлично»: обучающимся дан полный, развернутый ответ на поставленный вопрос; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание по дисциплине демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей. Обучающийся владеет терминологией, способен приводить примеры, высказывает свою точку зрения с опорой на знания и опыт;

- оценка «хорошо»: обучающимся дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ логичен, выстроен, но совершены единичные ошибки. Не в полной мере владеет знаниями по всей дисциплине. Даны ответы на дополнительные, поясняющие вопросы;

- оценка «удовлетворительно»: ответ на вопрос не полный, с ошибками. Обучающийся путается в деталях, с затруднением пользуется профессиональной терминологией. Есть замечания к построению ответа, к логике и последовательности изложения. Не отвечает на дополнительные вопросы;

- оценка «неудовлетворительно»: ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствует фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса с другими объектами дисциплины, речь неграмотная, не используется профессиональная терминология. Ответы на дополнительные вопросы не даны или неверные.

Устный опрос по разделу 3 «Системы и решения с использованием криптографических систем с открытым ключом»

- Форма опроса – фронтальный.

Пример заданий к устному опросу.

1. Базовые настройки безопасности для SSH сервера.
2. Основные угрозы пакетного менеджера apt.
3. Приведите пример решения задачи с использованием технологии PGP
4. В чем недостаток использования паролей при удаленном подключении по ssh?

Критерии оценки уровня сформированности компетенций для устного опроса:

- оценка «отлично»: обучающимся дан полный, развернутый ответ на поставленный вопрос; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание по дисциплине демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей. Обучающийся владеет терминологией, способен приводить примеры, высказывает свою точку зрения с опорой на знания и опыт;

- оценка «хорошо»: обучающимся дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ логичен, выстроен, но совершены единичные ошибки. Не в полной мере владеет знаниями по всей дисциплине. Даны ответы на дополнительные, поясняющие вопросы;

- оценка «удовлетворительно»: ответ на вопрос не полный, с ошибками. Обучающийся путается в деталях, с затруднением пользуется профессиональной терминологией. Есть замечания к построению ответа, к логике и последовательности изложения. Не отвечает на дополнительные вопросы;

- оценка «неудовлетворительно»: ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствует фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса с другими объектами дисциплины, речь неграмотная, не используется профессиональная терминология. Ответы на дополнительные вопросы не даны или неверные.

Устный опрос по разделу 4 «Доверенная среда»

• Форма опроса – фронтальный.

Пример заданий к устному опросу.

1. Что такое среда функционирования криптографии? Для каких бизнес задач она может потребоваться?
2. Что такое резидентный компонент безопасности?
3. Что такое датчик случайных чисел?
4. Какие бывают датчики случайных чисел?
5. Как понять, что последовательность случайная?
6. Плюсы и минусы использования аппаратных и программных ДСЧ?
7. Какие атаки можно провести на средства криптографической защиты?

Критерии оценки уровня сформированности компетенций для устного опроса:

- оценка «отлично»: обучающимся дан полный, развернутый ответ на поставленный вопрос; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание по дисциплине демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей. Обучающийся владеет терминологией, способен приводить примеры, высказывает свою точку зрения с опорой на знания и опыт;

- оценка «хорошо»: обучающимся дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ логичен, выстроен, но совершены единичные ошибки. Не в полной мере владеет знаниями по всей дисциплине. Даны ответы на дополнительные, поясняющие вопросы;

- оценка «удовлетворительно»: ответ на вопрос не полный, с ошибками. Обучающийся путается в деталях, с затруднением пользуется профессиональной терминологией. Есть замечания к построению ответа, к логике и последовательности изложения. Не отвечает на дополнительные вопросы;

- оценка «неудовлетворительно»: ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствует фрагментарность, нелогичность

изложения. Обучающийся не осознает связь обсуждаемого вопроса с другими объектами дисциплины, речь неграмотная, не используется профессиональная терминология. Ответы на дополнительные вопросы не даны или неверные.

Устный опрос по разделу по разделу 5 «Отчуждаемые ключевые хранилища»

- Форма опроса – фронтальный.

Пример заданий к устному опросу

1. Что такое смарт-карта и чем она отличается от USB-токена?
2. В чем принципиальные ограничения использования отчуждаемых ключевых хранилищ типа смарт-карт?
3. Какие существуют интерфейсы взаимодействия со смарт-картами?
4. Что такое технология NFC? В чем ее плюсы и минусы
5. Зачем могут использовать не отчуждаемые ключевые хранилища?

Критерии оценки уровня сформированности компетенций для устного опроса:

- оценка «отлично»: обучающимся дан полный, развернутый ответ на поставленный вопрос; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание по дисциплине демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей. Обучающийся владеет терминологией, способен приводить примеры, высказывает свою точку зрения с опорой на знания и опыт;

- оценка «хорошо»: обучающимся дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ логичен, выстроен, но совершены единичные ошибки. Не в полной мере владеет знаниями по всей дисциплине. Даны ответы на дополнительные, поясняющие вопросы;

- оценка «удовлетворительно»: ответ на вопрос не полный, с ошибками. Обучающийся путается в деталях, с затруднением пользуется профессиональной терминологией. Есть замечания к построению ответа, к логике и последовательности изложения. Не отвечает на дополнительные вопросы;

- оценка «неудовлетворительно»: ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствует фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса с другими объектами дисциплины, речь неграмотная, не используется профессиональная терминология. Ответы на дополнительные вопросы не даны или неверные.

Устный опрос по разделу по разделу 6 «Криптографические системы с открытым ключом в СЗИ»

- Форма опроса – фронтальный.

Пример заданий к устному опросу

1. Приведите примеры криптографических алгоритмов, которые возможно использовать для решения задачи ЭП.
2. Приведите пример использования механизма ЭП для защиты ПО.
3. Приведите пример решений продуктов, в которых используется аутентификация с используем ключей
4. Какие есть плюсы аутентификации по ключу перед паролем аутентификацией?

Критерии оценки уровня сформированности компетенций для устного опроса:

- оценка «отлично»: обучающимся дан полный, развернутый ответ на поставленный вопрос; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание по дисциплине демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей. Обучающийся владеет терминологией, способен приводить примеры, высказывает свою точку зрения с опорой на знания и опыт;

- оценка «хорошо»: обучающимся дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ логичен, выстроен, но совершены единичные ошибки. Не в полной мере владеет знаниями по всей дисциплине. Даны ответы на дополнительные, поясняющие вопросы;

- оценка «удовлетворительно»: ответ на вопрос не полный, с ошибками. Обучающийся путается в деталях, с затруднением пользуется профессиональной терминологией. Есть замечания к построению ответа, к логике и последовательности изложения. Не отвечает на дополнительные вопросы;

- оценка «неудовлетворительно»: ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствует фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса с другими объектами дисциплины, речь неграмотная, не используется профессиональная терминология. Ответы на дополнительные вопросы не даны или неверные.

Устный опрос по разделу 7 «Управление ключами»

- Форма опроса – фронтальный.

Пример заданий к устному опросу

1. Опишите жизненный цикл ключа.
2. Как осуществляется уничтожение ключей и ключевой информации?
3. Необходимо ли держать открытой ключ в секрет?
4. Должен ли пользователь средства ЭП иметь доступ к ключу?

Критерии оценки уровня сформированности компетенций для устного опроса:

- оценка «отлично»: обучающимся дан полный, развернутый ответ на поставленный вопрос; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание по дисциплине демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей. Обучающийся владеет терминологией, способен приводить примеры, высказывает свою точку зрения с опорой на знания и опыт;

- оценка «хорошо»: обучающимся дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ логичен, выстроен, но совершены единичные ошибки. Не в полной мере владеет знаниями по всей дисциплине. Даны ответы на дополнительные, поясняющие вопросы;

- оценка «удовлетворительно»: ответ на вопрос не полный, с ошибками. Обучающийся путается в деталях, с затруднением пользуется профессиональной терминологией. Есть замечания к построению ответа, к логике и последовательности изложения. Не отвечает на дополнительные вопросы;

- оценка «неудовлетворительно»: ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствует фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса с другими объектами дисциплины, речь неграмотная, не используется профессиональная терминология. Ответы на дополнительные вопросы не даны или неверные.

Устный опрос по разделу 8 «Инфраструктуры открытых ключей (PKI)»

• Форма опроса – фронтальный.

1. Что такое сертификат?
2. Допустимо ли использовать самоподписанный сертификат? В каких условиях?
3. Что такое сеть доверия?
4. Как происходит процесс взаимной аутентификации при подключении к веб-серверу?

Критерии оценки уровня сформированности компетенций для устного опроса:

- оценка «отлично»: обучающимся дан полный, развернутый ответ на поставленный вопрос; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание по дисциплине демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей. Обучающийся владеет терминологией, способен приводить примеры, высказывает свою точку зрения с опорой на знания и опыт;

- оценка «хорошо»: обучающимся дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ логичен, выстроен, но совершены единичные ошибки. Не в полной мере владеет знаниями по всей дисциплине. Даны ответы на дополнительные, поясняющие вопросы;

- оценка «удовлетворительно»: ответ на вопрос не полный, с ошибками. Обучающийся путается в деталях, с затруднением пользуется профессиональной терминологией. Есть замечания к построению ответа, к логике и последовательности изложения. Не отвечает на дополнительные вопросы;

- оценка «неудовлетворительно»: ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствует фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса с другими объектами дисциплины, речь неграмотная, не используется профессиональная терминология. Ответы на дополнительные вопросы не даны или неверные.

Устный опрос по разделу 9 «Безопасность и угрозы PKI »

• Форма опроса – фронтальный.

Примеры вопросов.

1. Приведите примеры уязвимостей инфраструктуры открытых ключей.
2. Приведите типовые меры защиты инфраструктуры открытых ключей.
3. Роль аппаратных средств защиты информации в обеспечении защиты инфраструктуры открытых ключей.
4. Проблема обеспечения неизвлекаемости ключа.

Критерии оценки уровня сформированности компетенций для устного опроса:

- оценка «отлично»: обучающимся дан полный, развернутый ответ на поставленный вопрос; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание по дисциплине демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей. Обучающийся владеет терминологией, способен приводить примеры, высказывает свою точку зрения с опорой на знания и опыт;

- оценка «хорошо»: обучающимся дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ логичен, выстроен, но совершены единичные ошибки. Не в полной

мере владеет знаниями по всей дисциплине. Даны ответы на дополнительные, поясняющие вопросы;

- оценка «удовлетворительно»: ответ на вопрос не полный, с ошибками. Обучающийся путается в деталях, с затруднением пользуется профессиональной терминологией. Есть замечания к построению ответа, к логике и последовательности изложения. Не отвечает на дополнительные вопросы;

- оценка «неудовлетворительно»: ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствует фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса с другими объектами дисциплины, речь неграмотная, не используется профессиональная терминология. Ответы на дополнительные вопросы не даны или неверные.

Устный опрос по разделу 10 «Защита ГИС, ИСПДн и КИИ»

- Форма опроса – фронтальный.

Пример заданий к устному опросу

1. Какие основные проблемы возникают при интеграции СЗИ и корпоративных инфраструктур открытых ключей в контексте защиты ГИС?
2. Каковы преимущества и недостатки использования единых инфраструктур открытых ключей для защиты различных типов информационных систем?
3. Какие технологические и организационные барьеры могут препятствовать успешной интеграции РКІ?

Критерии оценки уровня сформированности компетенций для устного опроса:

- оценка «отлично»: обучающимся дан полный, развернутый ответ на поставленный вопрос; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание по дисциплине демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей. Обучающийся владеет терминологией, способен приводить примеры, высказывает свою точку зрения с опорой на знания и опыт;

- оценка «хорошо»: обучающимся дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ логичен, выстроен, но совершены единичные ошибки. Не в полной мере владеет знаниями по всей дисциплине. Даны ответы на дополнительные, поясняющие вопросы;

- оценка «удовлетворительно»: ответ на вопрос не полный, с ошибками. Обучающийся путается в деталях, с затруднением пользуется профессиональной терминологией. Есть замечания к построению ответа, к логике и последовательности изложения. Не отвечает на дополнительные вопросы;

- оценка «неудовлетворительно»: ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствует фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса с другими объектами дисциплины, речь неграмотная, не используется профессиональная терминология. Ответы на дополнительные вопросы не даны или неверные.

Устный опрос по разделу 11 «Альтернативные решения»

- Форма опроса – фронтальный.

Пример заданий к устному опросу

1. Особенности организации систем управления ключами в распределённых реестрах
2. Какие недостатки существуют в использовании блокчейна для организации распределённых реестров?

Критерии оценки уровня сформированности компетенций для устного опроса:

- оценка «отлично»: обучающимся дан полный, развернутый ответ на поставленный вопрос; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание по дисциплине демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей. Обучающийся владеет терминологией, способен приводить примеры, высказывает свою точку зрения с опорой на знания и опыт;

- оценка «хорошо»: обучающимся дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ логичен, выстроен, но совершены единичные ошибки. Не в полной мере владеет знаниями по всей дисциплине. Даны ответы на дополнительные, поясняющие вопросы;

- оценка «удовлетворительно»: ответ на вопрос не полный, с ошибками. Обучающийся путается в деталях, с затруднением пользуется профессиональной терминологией. Есть замечания к построению ответа, к логике и последовательности изложения. Не отвечает на дополнительные вопросы;

- оценка «неудовлетворительно»: ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствует фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса с другими объектами дисциплины, речь неграмотная, не используется профессиональная терминология. Ответы на дополнительные вопросы не даны или неверные.

Устный опрос по разделу 12 «Атаки на микроконтроллеры и аппаратные СЗИ »

- Форма опроса – фронтальный.

Задания к устному опросу (*названия тем*)

1. Приведите примеры инвазивных атак
2. Что такое glitch-атаки?
3. Приведите примеры атаки по стороннему каналу.

Критерии оценки уровня сформированности компетенций для устного опроса:

- оценка «отлично»: обучающимся дан полный, развернутый ответ на поставленный вопрос; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание по дисциплине демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей. Обучающийся владеет терминологией, способен приводить примеры, высказывает свою точку зрения с опорой на знания и опыт;

- оценка «хорошо»: обучающимся дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ логичен, выстроен, но совершены единичные ошибки. Не в полной мере владеет знаниями по всей дисциплине. Даны ответы на дополнительные, поясняющие вопросы;

- оценка «удовлетворительно»: ответ на вопрос не полный, с ошибками. Обучающийся путается в деталях, с затруднением пользуется профессиональной терминологией. Есть замечания к построению ответа, к логике и последовательности изложения. Не отвечает на дополнительные вопросы;

- оценка «неудовлетворительно»: ответ представляет собой разрозненные знания с существенными ошибками по вопросу, присутствует фрагментарность, нелогичность изложения. Обучающийся не осознает связь обсуждаемого вопроса с другими объектами дисциплины, речь неграмотная, не используется профессиональная терминология. Ответы на дополнительные вопросы не даны или неверные.

Примеры тем эссе.

1. Постквантовая криптография. Перспективы и положения дел.
2. Особенности использования биологического датчика случайных чисел.
3. Перспективы использования смарт-карт для хранения ключей.
4. Перспективные задачи защиты приватных ключей.

3.3. Задания для промежуточной аттестации (зачета)

Пример зада к зачету

5. Настроить аутентификацию по смарт-карте в ОС Linux
6. Разработать систему защищенной передачи данных
7. Настроить систему доверенного загрузки модулей ядра в ОС Linux
8. Разработать ПО с возможностью доверенного обновления.
9. Продемонстрировать угрозу использования программного средства электронной подписи в незащищенной среде

Для подготовки к зачету обучающимся после индивидуального обсуждения выдается практическая задача. В процессе зачета студент должен предложить решение и ответить на 2-3 вопроса по предложенному решению.

Зачет проводится в практически и письменной форме с устным дополнением ответа. Зачет служит формой проверки качества выполнения студентами лабораторных работ и усвоения семестрового учебного материала по дисциплине, а также является часть процесса обучения и закрепления полученных знаний в семестре.

По итогам зачета, в соответствии с модульно – рейтинговой системой университета, выставляются баллы с последующим переходом по шкале баллы – оценки за зачет, выставляемый по наименованию «зачтено» или «не зачтено».

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.