

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет Информатики и Информационных Технологий
Кафедра Информационных технологий и безопасности компьютерных
систем

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и средства криптографической защиты информации

Образовательная программа
10.03.01 Информационная безопасность
Профиль подготовки

Безопасность компьютерных систем

Уровень высшего образования

Бакалавриат

Форма обучения

Очная, очно-заочная

Статус дисциплины: входит в обязательную часть ОПОП

Махачкала, 2021

Рабочая программа дисциплины **Методы и средства криптографической защиты информации** составлена в 2021 году в соответствии с требованиями ФГОС ВО - бакалавриат по направлению подготовки 10.03.01 – Информационная безопасность от 17 ноября 2020 г. №1427.

Разработчик: Ахмедова Написат Мурадовна, старший преподаватель кафедры информационных технологий и безопасности компьютерных систем.

Рабочая программа одобрена на заседании кафедры информационных технологий и безопасности компьютерных систем 28.06.2021 г., протокол № 11.

Зав. кафедрой Ахмедова З.Х. Ахмедова З.Х.

Рабочая программа одобрена на заседании Методической комиссии факультета информатики и информационных технологий

29.06.2021 г., протокол № 11.

Председатель методсовета факультета ИиИТ Бакмаев А.Ш.

Рабочая программа согласована с учебно-методическим управлением

09.07.2021 г., _____

Начальник УМУ Гасангаджиева А.Г. Гасангаджиева А.Г.

Аннотация рабочей программы дисциплины

Дисциплина **Методы и средства криптографической защиты информации** входит в обязательную часть ОПОП бакалавриата, по направлению 10.03.01 Информационная безопасность

Дисциплина реализуется на факультете ИиИТ кафедрой ИТиБКС.

Содержание дисциплины охватывает круг вопросов, связанных с защитой информации путем математических преобразований с помощью криптографических алгоритмов.

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональных – ОПК-7 ОПК-9.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: *лекции, практические занятия, лабораторные занятия, самостоятельная работа.*

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме - *контрольная работа, коллоквиум и пр.* и промежуточный контроль в форме - *экзамена.*

Объем дисциплины 4 зачетные единицы, в том числе 144 академических часа по видам учебных занятий

Очная форма обучения

Семестр	Учебные занятия							Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)	
	в том числе:								
	всего	Контактная работа обучающихся с преподавателем					СРС, в том числе экзамены		
		все го	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР			консультации
7	144	86	34	34	18		58	экзамен	

Очно-заочная форма обучения

Семестр	Учебные занятия							Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)	
	в том числе:								
	всего	Контактная работа обучающихся с преподавателем					СРС, в том числе экзамен		
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР			консультации
7	144	64	32	16	16		80	экзамен	

1. Цели освоения дисциплины

Целью освоения дисциплины **Методы и средства криптографической защиты информации** является изучение основных математических подходов к решению задач компьютерной безопасности и, прежде всего, к построению актуальных криптографических алгоритмов с учетом применения современных цифровых технологий.

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина **Методы и средства криптографической защиты информации** входит в базовую часть образовательной программы *бакалавриата*, по направлению 10.03.01 Информационная безопасность

Для освоения дисциплины необходимо знание курсов: «Математический анализ», «Алгебра и теория чисел», «Теория вероятности и математическая статистика», «Информатика», «Языки программирования», «Теория информации», «Теоретико-числовые методы криптографии». В результате изучения данной дисциплины студенты осваивают непростые математические принципы организации криптографической защиты информации, передаваемой и обрабатываемой техническими средствами, что является неотъемлемой составляющей подготовки учащихся по направлению 10.03.01 Информационная безопасность. Курс необходим для дисциплин компьютерной безопасности.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения).

Код и наименование компетенции из ОПОП	Код и наименование индикатора достижения компетенций (в соответствии с ОПОП)	Планируемые результаты обучения	Процедура освоения
ОПК-7 Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;	ИД1.ОПК-7.1.Знает основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий. ИД2.ОПК-7.2.Умеет применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий для автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и инф ИД3.ОПК-7.3.Имеет навыки программирования, отладки и тестирования прототипов программно-технических комплексов задач.	Знает основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий. Умеет применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий для автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ. Имеет навыки программирования, отладки и тестирования прототипов программно-технических комплексов задач.	Устный опрос, письменный опрос, практическая работа
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИД 1 ОПК-9.1.Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации ИД 2 ОПК-9.2. Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации ИД 3 ОПК-9.3. Владеет методами и средствами криптографической и технической защиты информации	Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации Владеет методами и средствами криптографической и технической защиты информации	Лабораторно-практические задания, к/р, тестовый контроль, устный и письменный опросы, доклады по темам

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 4 зачетные единицы, 144 академических часа.

4.2. Структура дисциплины.

4.2.1. Структура дисциплины в очной форме

№ п/п	Разделы и темы дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторны е занятия	Контроль самост. раб.		
	Модуль 1 Простые шифры								
1	Введение в криптографию	7		2		2		2	устный и письменный опросы
2	Краткая история криптографии	7		2		2		2	устный и письменный опросы, лабораторные работы.
3	Шифр Цезаря. простой замены.	7		2		2		2	устный и письменный опросы, лабораторные работы.
4	Шифр Виженера. Частотный анализ.	7		2	2	2			Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
5	Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ	7		2	2	2			Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
6	Шифры гаммирования. Композиции шифров	7		2	2	2			Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
	Итого по модулю 1:			12	6	12		6	
	Модуль 2 Шифрование с закрытым и открытым ключом								
1	Блочное шифрование. Сеть Фейстеля.	7		2		2		2	устный и письменный опросы, лабораторные работы.
2	DES/3DES	7		2	2	2			устный и письменный опросы, лабораторные работы.
3	AES	7		2		2		2	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
4	Шифрование с открытым ключом	7		2		2		2	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
5	Алгоритм Диффи- Хеллмана.	7		2	2	2			Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
6	Алгоритм RSA	7		2	2	2			Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
	Итого по модулю 2:			12	6	12		6	
	Модуль 3 Алгоритмы хеширования								
1	Схемы электронной подписи	7		2	2	2		2	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
2	Схемы построения хэш-функций	7		2	2	2		2	устный и письменный опросы, лаборат работы. орные

3	Base64/md5	7		2		2		2	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
4	Хеширование алгоритмом Sha 256/	7		2	2	2		2	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
5	Технология блокчейн	7		2		2		2	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
	<i>Итого по модулю 3:</i>			10	6	10		10	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
	Модуль 4								
	Экзамен (подготовка, сдача)							36	экзамен
	Итого:			34	18	34		58	

4.2.2. Структура дисциплины в очно-заочной форме

№ п/п	Разделы и темы дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные занятия	Контроль самост. раб.		
	Модуль 1 Простые шифры								
1	Введение в криптографию	7		2				4	устный и письменный опросы
2	Краткая история криптографии	7		2				4	устный и письменный опросы, лабораторные работы.
3	Шифр Цезаря. простой замены.	7		2				2	устный и письменный опросы, лабораторные работы.
4	Шифр Виженера. Частотный анализ.	7		2	2	2		2	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
5	Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ	7		2				2	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
6	Шифры гаммирования. Композиции шифров	7		2	2	2		2	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
	Итого по модулю 1:			12	4	4		16	
	Модуль 2 Шифрование с закрытым и открытым ключом								
1	Блочное шифрование. Сеть Фейстеля.	7		2				4	устный и письменный опросы, лабораторные работы.
2	DES/3DES/ AES	7		2	2	2		2	устный и письменный опросы, лабораторные работы.
3	Шифрование с открытым ключом	7		2				4	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
4	Алгоритм Диффи- Хеллмана.	7		2	2	2		2	Лабораторно-практические задания, к/р , устный и письменный опросы , доклады по темам
5	Алгоритм RSA	7		2	2	2		2	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
	Итого по модулю 2:			10	6	6		14	
	Модуль 3 Алгоритмы хеширования								
1	Схемы электронной подписи	7		2	2	2		2	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
2	Схемы построения хэш-функций	7		2	2	2		2	устный и письменный опросы, лаборат орные работы.
3	Base64/md5	7		2				4	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам

4	Хеширование алгоритмом Sha 256/	7		2	2	2		2	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
5	Технология блокчейн	7		2				4	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
	<i>Итого по модулю 3:</i>			10	6	6		14	Лабораторно-практические задания, к/р , устный и письменный опросы, доклады по темам
	Модуль 4								
	Экзамен (подготовка, сдача)							36	экзамен
	Итого:			32	16	16		80	

4.3. Содержание дисциплины, структурированное по темам (разделам).

4.3.1. Содержание лекционных занятий по дисциплине.

Модуль 1.

Тема 1. Введение в криптографию

Основные понятия криптографии. Введение в криптографию.
Криптографические атаки. Криптографический протокол.

Тема 2. Краткая история криптографии

Исторические шифры. Устройство. Эволюция шифров.

Тема 3. Шифр Цезаря.

Шифр Цезаря. Методы простой замены. Простейшие методы шифрования с закрытым ключом.

Тема 4. Шифр Виженера.

Таблица Виженера. Частотный анализ.

Тема 5. Классификация шифров перестановки.

Примеры шифров перестановки и их криптоанализ

Тема 6. Шифры гаммирования.

Гаммирование по модулю 2. Гаммирование по модулю n . Композиции шифров.

Модуль 2.

Тема 1. Блочное шифрование. Сеть Фейстеля.

Принципы построения блочных шифров с закрытым ключом. Режимы работы блочных шифров. Сеть Фейстеля.

Тема 2. DES/3DES

Алгоритмы шифрования DES и 3DES. Общие сведения. Шифрование и расшифрование.

Тема 3. AES

Алгоритмы шифрования AES. Общие сведения.

Тема 4. Шифрование с открытым ключом

Шифры с открытым ключом. Односторонние функции. Использование ассиметричных алгоритмов для шифрования.

Тема 5. Алгоритм Диффи-Хеллмана.

Тема 6. Алгоритм RSA

Алгоритм RSA. Основные сведения. Пример вычислений по алгоритму.

Практическое использование алгоритма RSA.

Модуль 3.

Тема 1. Схемы электронной подписи

Электронная цифровая подпись. Криптостойкость и имитостойкость шифров.

Тема 2. Схемы построения хэш-функций

Криптографические хеш-функции. Понятие хеш-функции. Обзор алгоритмов формирования хеш-функций

Тема 3. Base64/md5

Тема 4. Хеширование алгоритмом Sha 256

Хеширование алгоритмом sha 256

Тема 5. Технология блокчейн

Основные принципы и понятие блокчейна. Блокчейн как основа современной компьютерной безопасности.

4.3.2. Содержание лабораторно-практических занятий по дисциплине.

Модуль 1.

- 1) Шифрование с закрытым ключом незнакомого текста.
- 2) Программная реализация шифра Цезаря.
- 3) Одноалфавитная замена. Пропорциональные шифры.
- 4) Многоалфавитные подстановки, методы гаммирования.
- 5) Методы перестановки. Понятие композиционного шифра.
- 6) Программная реализация шифра Вижинера.

Модуль 2.

- 1) Поточные шифры.
- 2) DES-шифрование.
- 3) Использование алгоритма хеширования для сокрытия содержимого файла.
- 4) Использование алгоритма хеширования для подтверждения неизменности файла.
- 5) Base-64.
- 6) Кодирование бинарных зашифрованных файлов в base 64.

Модуль 3.

- 1) Создание цифровых сертификатов.
- 2) Применение электронной цифровой подписи для проверки авторства. неизменности файла.
- 3) Скрытие факта передачи шифрованного текста (стеганография).
- 4) С помощью готовых пакетов на python реализовать алгоритм sha 256
- 5) Реализовать сверку хеш-значений с помощью встроенных пакетов на python
- 6) Генерация ключей по протоколу Диффи-Хеллмана в среде Mathcad

5. Образовательные технологии

Предусмотрено сочетание традиционных видов учебной активности, таких как конспектирование лекций и контроль усвоения теоретического материала в виде коллоквиумов, так и интерактивных технологий, таких как собеседования, ситуационные игры на выбор методов защиты информации на практических занятиях.

Подготовка студентами докладов по темам, не входящим в план лекций, а также выполнение расчетных работ, позволяют расширить научный кругозор студентов, повысить навык работы с учебной и научной отечественной и зарубежной литературой, развить языковые навыки, повысить математическую подготовку, укрепить междисциплинарные связи, повысить навык программирования.

6. Учебно-методическое обеспечение самостоятельной работы студентов.

В соответствии с учебным планом предусмотрен экзамен в седьмом семестре.

Формы контроля: текущий контроль, промежуточный контроль по модулю, итоговый контроль по дисциплине.

Форма текущего контроля – выполнение семестровых заданий. В течение семестра студент выполняет задания, за каждой из которых получает соответствующие баллы. За выполнение задания студент получает определенное количество баллов.

Форма промежуточного контроля – контрольные, коллоквиум.

Форма итогового контроля, определенная учебным планом, - экзамен.

Темы для самостоятельного изучения:

Наименование темы:	Вид работы:	Примерная трудоемкость, а.ч.	
		очная	Очно-заочная
Инструментальные средства и библиотеки для реализации криптографических алгоритмов	Изучение функций библиотек GNU MP и GNU Crypto по технической документации	2	4
Теоретико –числовые методы в криптографии. Вычисления в простых полях и кольцах целых чисел	Изучение разделов дисциплины по учебной литературе, в том числе вопросов, не освещаемых на лекциях: Алгоритмические аспекты поиска больших простых чисел Подготовка к практическим занятиям	4	8
Создание цифровых сертификатов	Выполнение расчетного задания в виде компьютерной программы по темам	4	8
Сложность дискретного логарифмирования и наиболее быстрые алгоритмы.	Изучение разделов дисциплины по учебной литературе, в том числе вопросов, не освещаемых на лекциях. Подготовка к практическим занятиям	4	8
Возможные атаки на блокчейн и криптокошельки	Систематизировать и выявить основные способы борьбы с атаками Предложить рекомендации по защите криптокошельков	4	8
Теория секретных систем Шеннона и современные подходы к теоретико-информационной секретности	Выполнение расчетного задания в виде компьютерной программы по теме: реализация простейших омофонных кодов и их применение для построения идеальной криптосистемы для	4	8

	сообщений, порождаемых источником без памяти с неизвестной статистикой.		
Подготовка к экзамену	Подготовка к экзамену	36	36
	ИТОГО СРС	58	80

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

7.1. Типовые контрольные задания

ПЕРЕЧЕНЬ КОНТРОЛЬНЫХ ВОПРОСОВ ДЛЯ ПОДГОТОВКИ К ИТОГОВОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

1. Основные понятия и определения криптографии.
2. Виды криптосистем. Задачи, решаемые методами криптографии.
 3. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений.
4. История криптографии. Основные этапы становления науки криптографии.
 5. Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски.
 6. Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ.
7. Шифры гаммирования. Шифр Вернама. Подходы к его криптоанализу.
8. Композиции шифров. Enigma. Шифр Хейглина.
 9. Математическая модель шифра.
 10. Атаки и угрозы шифрам.
 11. Блочные шифры и их ключевая система. Замены и перестановки.
 12. Сеть Файстеля. Шифры DES, ГОСТ 28147-89.
 13. Шифр AES
 14. Шифр IDEA.
 15. Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ.
 16. Режимы шифрования.
 17. Многократное шифрование. Композиция блочных шифров.
 18. Совершенные шифры. Пример совершенного шифра.
 19. Энтропийные характеристики шифров. Идеальные шифры.
 20. Избыточность языка.
 21. Оценка числа ложных ключей и расстояние единственности.
 22. Безусловно стойкие и вычислительно стойкие шифры.
 23. Псевдослучайные последовательности (ПСП). Характеристики генераторов ПСП (ПСГ). Требования к криптографическим ПСП. Примеры ПСП и криптографических ПСП.

24. Поточные шифры. Общая схема поточного шифра. Синхронные и самосинхронизирующиеся шифры.
25. Регистры сдвига с обратной линейной связью (РСЛОС).
26. ПСГ на основе РСЛОС.
27. Шифр А5.
28. Нелинейные регистры сдвига.
29. Шифр RC4.
30. Теория имитостойкости Симмонса. Имитация и подмена сообщения. Характеристики имитостойкости. Совершенная имитостойкость.
31. Коды аутентификации сообщений.
32. Защитные контрольные суммы.
33. Криптографические хэш-функции и требования к ним.
34. Подходы к проектированию хэш-функций.
35. Хэш-функции на основе блочного шифра.
36. Ключевые хэш-функции.
37. Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях.
38. Криптосистема Диффи-Хэллмана. Пример.
39. Криптосистема RSA. Пример.
40. Криптосистема Эль-Гамала. Пример.
41. Криптосистема Рабина. Пример.
42. Криптосистема Гольдвассер-Микали. Пример.
43. Криптосистема Блюма-Гольдвассер. Пример.
44. Рюкзачные шифры. Криптосистема Меркла-Хэллмана.
45. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП.
46. Подпись RSA, Эль-Гамала.
47. Подпись Фиата-Шамира.
48. Подпись Онга-Шнорра-Шамира.
49. Неотрицаемая подпись Шаума-ван-Антверпена.
50. Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка.
51. Шифр Эль-Гамала на эллиптической кривой.
52. Технология блокчейн, как основа современной компьютерной безопасности
53. Хеширование алгоритмом Sha криптовалют

ПЕРЕЧЕНЬ ТЕМ РЕФЕРАТОВ

- 1) Криптография в Древнем мире.
- 2) Исторические методы стеганографии.
- 3) Криптография в Средние века и в Новое время.
- 4) Дисковые шифраторы.
- 5) Криптография на рубеже 19-20 вв.
- 6) История отечественной криптографии.
- 7) Шифрование аналогового сигнала.
- 8) Клод Шеннон и его вклад в криптографию.
- 9) Алан Тьюринг и его вклад в криптографию.
- 10) Лауреаты премии Алана Тьюринга.
- 11) Первый блочный шифр – Lucifer.
- 12) Современная стеганография – математические методы.
- 13) Электронные водяные знаки.
- 14) Ади Шамир и его вклад в криптографию.
- 15) Шифрование и аутентификация в современных беспроводных сетях связи.

- 16) Парольные схемы аутентификации.
- 17) Одноразовые пароли.
- 18) Протоколы с нулевым разглашением

7.2. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Общий результат выводится как интегральная оценка, складывающаяся из текущего контроля - _60___% и промежуточного контроля - _40___%.

Текущий контроль по дисциплине включает:

- посещение занятий - 10_ баллов,
- участие на практических занятиях - _10_ баллов,
- выполнение лабораторных заданий - _30_ баллов,
- выполнение домашних (аудиторных) контрольных работ - _10_ баллов.

Промежуточный контроль по дисциплине включает:

- устный опрос - _10_ баллов,
- письменная контрольная работа - _20___ баллов,
- тестирование - _10_ баллов.

Критерии оценивания ответов на экзамене

Основными критериями оценки уровня подготовки и сформированности соответствующих компетенций студента при проведении государственного экзамена являются:

- степень владения профессиональной терминологией;
- уровень усвоения студентом теоретических знаний и умение использовать их для решения профессиональных задач;
- ориентирование в научной и иной специальной литературе;
- логичность, обоснованность, четкость ответа;
- культура ответа;
- готовность отвечать на дополнительные вопросы по существу экзаменационного билета.

Критерии оценок:

-86-100 баллов – студент демонстрирует: свободное владение профессиональной терминологией; высокий уровень теоретических знаний и умение использовать их для решения профессиональных задач; исчерпывающее последовательное, обоснованное и логически стройное изложение ответа, без ошибок. Студент без затруднений ориентируется в нормативных правовых актах, научной и иной специальной литературе. Речь студента грамотная, лаконичная, с правильной расстановкой акцентов. Студент готов отвечать на дополнительные вопросы.

- 66 - 85 баллов - Студент демонстрирует: владение профессиональной терминологией на достаточном уровне; достаточный уровень теоретических знаний и умение использовать их для решения профессиональных задач; грамотное и логичное изложение ответа, без существенных ошибок, но изложение недостаточно систематизировано и последовательно. Студент с некоторыми затруднениями ориентируется в нормативных правовых актах, научной и иной специальной литературе. Речь студента грамотная, лаконичная, с правильной расстановкой акцентов. Студент испытывает затруднения при ответе на дополнительные вопросы.

- 51 – 65 баллов - Студент демонстрирует: владение профессиональной терминологией на минимальном уровне; низкий пороговый уровень теоретических знаний, усвоил только основной программный материал без знания отдельных особенностей; при ответе допускает неточности, материал недостаточно систематизирован. Студент с затруднениями ориентируется в нормативных правовых актах, научной и иной специальной литературе. Речь студента в основном грамотная, но не демонстрируется уверенное владение материалом. Студент с трудом отвечает на дополнительные вопросы.

- 0 - 50 баллов - Студент не владеет профессиональной терминологией, демонстрирует низкий уровень теоретических знаний и умения использовать их для решения профессиональных задач. Студент не знает значительной части программного материала, допускает существенные грубые ошибки, не ориентируется в нормативных правовых актах, научной и иной специальной литературе. Речь недостаточно грамотная. Студент не может ответить на дополнительные вопросы.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

а) основная литература:

- 1) **Иванов, Михаил Александрович.** Методы и средства криптографической защиты информации в компьютерных системах и сетях. - М. : КУДРИЦ-ОБРАЗ, 2001. - 363 с. - ISBN 5-93378- 021-9 : 0-0..
- 2) **Торстейнсон, Питер.** Криптография и безопасность в технологии .NET / пер. с англ. В.Д.Хорева; под ред. С.М.Моляко. - М. : БИНОМ. Лаб. знаний, 2007. - 479 с. : ил. - (Программисту). - Предм. указ.: с. 448-472. - ISBN 978-5-94774-312-8 : 380-00
- 3) **Кирпичников А.П.** Криптографические методы защиты компьютерной информации [Электронный ресурс]: учебное пособие / А.П. Кирпичников, З.М. Хайбуллина. — Электрон. текстовые данные. — Казань: Казанский национальный исследовательский технологический университет, 2016. — 100 с. — 978-5-7882-2052-9. — Режим доступа: <http://www.iprbookshop.ru/79313.html>
- 4) **Лоран Л.** Блокчейн от А до Я; Все о технологии десятилетия. М: Бомбора, 2017. – 376с. – ISBN 978-5-699-98942-3

б) дополнительная литература:

1. **Калмыков И.А.** Методы и средства криптографической защиты информации [Электронный ресурс] : лабораторный практикум / И.А. Калмыков, Д.О. Науменко, Т.А. Гиш. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 109 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/63099.html>
2. Практикум по выполнению лабораторных работ по дисциплине Методы и средства криптографической защиты информации [Электронный ресурс] / . — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2015. — 67 с. — 2227- 8397. — Режим доступа: <http://www.iprbookshop.ru/61738.html>
3. Учебно-методическое пособие по выполнению курсовой работы по дисциплине Методы и средства криптографической защиты информации [Электронный ресурс] / . — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2015. — 28 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/63335.html>
4. **Табернакулов А., Койфманн Я.** Блокчейн на практике. М.: Альпина Паблишер, 2019, 260 с. - ISBN 978-5-9614-2382-2

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

- 1) eLIBRARY.RU [Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва, 1999 — . Режим доступа: <http://elibrary.ru/defaultx.asp> (дата обращения: 01.02.2020). — Яз. рус., англ.
- 2) Moodle [Электронный ресурс]: система виртуального обучения: [база данных] / Даг. гос. ун-т. — Махачкала, г. — Доступ из сети ДГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. — URL: <http://moodle.dgu.ru/> (дата обращения: 22.03.2020).
- 3) Электронный каталог НБ ДГУ [Электронный ресурс]: база данных содержит сведения о всех видах лит, поступающих в фонд НБ ДГУ/Дагестанский гос. ун-т. — Махачкала, 2010 — Режим доступа: <http://elib.dgu.ru>, свободный (дата обращения: 21.03.2020).
- 4) Информационный портал по безопасности **SecurityLab.ru**, новости, статьи, обзор уязвимостей, вирусов и мнения аналитиков.
- 5) Алгоритмы хеширования криптовалют в 2020 году — Режим доступа: <https://www.developcoins.com/cryptocurrency-hashing-algorithms> - (Дата обращения: 28.06.2021).
- 6) Secure Hash Algorithms — Режим доступа: <https://brilliant.org/wiki/secure-hashing-algorithms/> - (Дата обращения: 28.06.2021).

10. Методические указания для обучающихся по освоению дисциплины.

Практические занятия по дисциплине «Методы и средства криптографической защиты информации» служат для получения практических навыков по применению теоретических знаний, полученных студентами на лекциях, для решения конкретных задач в профессиональной сфере специалистов в области защиты информации.

Решения задач фиксируются с помощью реализованных программ на современных языках программирования, с использованием системы контроля версий GIT.

Для более полного понимания целей, задач и практических результатов теории систем следует: 1) Ознакомиться с дополнительной литературой, особенно с трудами основоположников. 2) Выполнять самостоятельную работу 3) Попытаться в рамках практических и лабораторных занятий полностью выполнить все задания.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

Учебная аудитория, оборудованная мультимедиа проектором. Компьютер под управлением операционной системы Windows 7, 8.0, 8.1, 10, имеющий установленный пакет офисных программ MSOffice и Microsoft Visual Studio.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

- а) Мультимедийная аудитория - для лекций;
- б) Компьютерный класс, оборудованный для проведения практических работ средствами оргтехники, персональными компьютерами, объединенными в сеть с выходом в Интернет – для практических занятий.

Для проведения лекционных занятий требуется аудитория на курс, оборудованная интерактивной доской, мультимедийным проектором с экраном, ПЭВМ с установленным ПО: Miro, Zoom, Trello.

Для проведения практических занятий требуется аудитория на группу студентов, оборудованная интерактивной доской, мультимедийным проектором с экраном.

Для проведения лабораторных занятий на ПЭВМ требуется компьютерный класс с установленной на ПЭВМ: 1. Microsoft Office 2. Microsoft Visual Studio. 3. Pycharm. 4.

Браузер с выходом в интернет. 5. Mathcad