МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

УТВЕРЖДАЮ
Директор Пятигорского института (филиал) СКФУ
_____ Т.А. Шебзухова
«__» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Методы и средства криптографической защиты информации

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Направление подготовки/специальность 10.03.01 Информационная безопасность
Квалификация выпускника: бакалавр
Форма обучения очная
Год начала обучения 2021
Изучается в 5-6 семестре

г. Пятигорск 20__ **г.**

Цель и задачи освоения дисциплины

Цель изучения дисциплины «Криптографические методы защиты информации»: теоретическая и практическая подготовка студентов к изучению методов и средств защиты информации и их применение для решения задач обеспечения криптостойкости современных систем шифрования, основанных на методах симметричного и асимметричного криптографического сокрытия семантического смысла передаваемой информации.

В соответствии с указанной целью при изучении данной дисциплины ставятся следующие задачи:

−ознакомить студентов с современными системами шифрования на основе симметричных и асимметричных алгоритмов;

−научить выбирать параметры псевдослучайных последовательностей для генерирования криптостойких ключей;

−изучить стандарты систем шифрования;

−изучить криптографические протоколы.

1. Место дисциплины в структуре ОП

Дисциплина относится к базовой части блока Б1, её освоение происходит в 5 и 6 семестрах.

2. Связь с предшествующими дисциплинами

Пререквизитами являются дисциплины: «Математические основы криптологии», «Введение в спектрально-корреляционный анализ случайных процессов», «Методы проверки статистических гипотез в обработке информации».

3. Связь с последующими дисциплинами

Кореквизитами являются дисциплины:«Защита информационных процессов в компьютерных системах», а также подготовкак сдаче и сдача государственного экзамена, защита ВКР, включая подготовку к процедуре защиты и процедуру защиты.

4. Компетенции обучающегося, формируемые в результате изучения дисциплины

4.1 Наименование компетенции

Индекс	Формулировка:
ОПК-2	Способность применять соответствующий математический аппарат для решения профессиональных задач.
ОПК-4	Способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для обработки информации.
ПК-1	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

4.2 Знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенции

Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: – основные задачи и понятия криптографии;	ОПК-2

– модели шифров и математические методы их исследования;	
Уметь: – применять математический аппарат для решения профессиональных задач;	ОПК-2
Владеть: – криптографической терминологией; – навыками применения математического аппарата при реализации типовых криптографических алгоритмов и оценке их криптостойкости;	ОПК-2
Знать: – требования к шифрам и основные характеристики шифров; – принципы построения криптографических алгоритмов; – криптографические стандарты;	ОПК-4
Уметь: – применять методы криптографии при решении задач защиты информации; – осуществлять программную реализацию криптографических алгоритмов; – проводить анализ стойкости криптосистем; – пользоваться научно-технической литературой в области криптографии;	ОПК-4
Владеть: – навыками применения методов криптографии при решении задач защиты информации; – навыками программной реализации криптографических алгоритмов; – навыками проведения анализа стойкости криптосистем;	ОПК-4
Знать: – методы и способы криптографической защиты информации; – показатели эффективности криптографической защиты и методы их оценки; – структуру государственной системы защиты информации; – основные руководящие, методические и нормативные документы по криптографии.	ПК-1
Уметь: – выполнять работы по установке, настройке и обслуживанию криптографических средств защиты информации; – применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;	ПК-1
Владеть: – навыками осуществления приемки, освоения и эксплуатации вводимых технологий и средств криптографии в соответствии с действующими нормативами; – методами осуществления наладки программного обеспечения, настройки, испытания и сдачи в эксплуатацию средств криптографии.	ПК-1

5. Объем учебной дисциплины/модуля

	Астр. часы	
Объем занятий: Итого	135 ч.	5з.е.
В т.ч. аудиторных	76,5 ч.	
Из них:		
Лекций	25,5 ч.	
Лабораторных работ	51,0 ч.	
Практических занятий	– ч.	
Самостоятельной работы	31,5 ч.	
Зачет	в 5 семестре	
Экзамен	в 6 семестре	

7. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов занятий

7.1 Тематический план дисциплины

№	Раздел (тема) дисциплины	Реализуемые компетенции	Контактная работа обучающихся с преподавателем, часов				Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	
5 семестр							
	Раздел 1. Введение в криптографию.						
1.	Тема 1. Основные понятия криптографии.	ОПК-2, ОПК-4, ПК-1	1,5		9		1,5
2.	Тема 2. Классические шифры замены.		1,5		6		1,5
3.	Тема 3. Классические шифры перестановки.		1,5				1,5
	Раздел 2. Современные шифры с симметричным ключом.						
4.	Тема 4. Современныеблочные шифры с симметричным ключом.	ОПК-2, ОПК-4, ПК-1	1,5		6		1,5
5.	Тема 5. Современныепоточные шифры с симметричным ключом.		1,5				1,5
6.	Тема 6. Современный стандарт шифрования (DES).		1,5		6		1,5
7.	Тема 7. Усовершенствованный стандарт шифрования (AES).		1,5				1,5
8.	Тема 8. Российский стандарт ГОСТ 28147-89.		1,5				1,5
	Раздел 3. Современные шифры с асимметричным ключом.						
9.	Тема 9. Алгоритмы шифрования с открытыми ключами.		1,5				1,5

	Итого 5 семестр		**13,5**		**27**		**13,5**
6 семестр							
10.	Тема 10. Алгоритмы генерации простых чисел. Проверка чисел на простоту.	ОПК-2, ОПК-4, ПК-1	1,5		6		3,0
11.	Тема 11. Сложность криптографических алгоритмов.		1,5				1,5
12.	Тема 12. Криптосистемы с открытым ключом.		1,5		6		3,0
13.	Тема 13.Криптосистемы на основе метода эллиптических кривых.		1,5				1,5
	Раздел 4. Методы установления подлинности и целостности данных.						
14.	Тема 14. Аутентификация данных. Электронная цифровая подпись.	ОПК-2, ОПК-4, ПК-1	1,5		6		3,0
15.	Тема 15. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля.		1,5				3,0
	Раздел 5. Криптографические протоколы.						
16.	Тема 16. Понятие о структуре и способах построения криптографических протоколов.	ОПК-2, ОПК-4, ПК-1	1,5		6		1,5
17.	Тема 17. Атаки на криптографические протоколы.		1,5				1,5
	Итого за 6 семестр:		**12,0**		**24,0**		**18,0**
	Итого:		**25,5**		**51,0**		**31,5**

7.2 Наименование и содержание лекций

№ темы	Наименование тем дисциплины, их краткое содержание	Обьем часов	Интерактивая форма проведения
	5 семестр		
	Раздел 1. Введение в криптографию.		
1	Тема 1. Основные понятия криптографии. Методы защиты информации. Криптография и криптоанализ. Понятие шифра и ключа. Симметричные и ассиметричные алгоритмы шифрования.Классификация классических шифров: шифры замены и перестановки, поточные и блочные шифры, моноалфавитные и многоалфавитные шифры.Виды атак криптоанализа. Способы противодействия им.	1,5	
2	Тема 2. Классические шифры замены. Классические шифры с симметричным ключом. Шифры замены: аддитивные, мультипликативные, аффинные, автоключевой, Виженера, Плейфера, Хилла, роторный, одноразового блокнота. Криптоанализ шифров замены.	1,5	
3	Тема 3. Классические шифры перестановки. Бесключевой шифр, ключевые шифры и шифры с двойной перестановкой. Криптоанализ шифров перестановки.	1,5	
	Раздел 2. Современные шифры с симметричным ключом.		
4	Тема 4. Современныеблочные шифры с симметричным ключом. Различия между современным и традиционным шифрами с	1,5	

	симметричным ключом. Современные блочные шифры: шифры замены и шифры перестановки.Основные компоненты современного блочного шифра. ШифрыФейстеля и не-Фейстеля.Атаки на блочные шифры.		
5	Тема 5. Современныепоточные шифры с симметричным ключом. Синхронные и несинхронные шифры потока. Преимущества и проблемы современных шифров потока. Криптоанализ шифров потока.	1,5	
6	Тема 6. Современный стандарт шифрования (DES) Структура шифра DES. Раунды шифрования. Функция DES. Генерация ключей раундов. Двукратный и трехкратный DES. Криптоанализ шифра DES.	1,5	
7	Тема 7. Усовершенствованный стандарт шифрования (AES). Алгоритм расширения ключей. Анализ расширения ключа. Алгоритмы шифрования и дешифрования в AES. Анализ AES.	1,5	
8	Тема 8. Российский стандарт ГОСТ 28147-89, особенности, принципы построения, методы шифрования. Различные комбинированные методы шифрования.	1,5	
	Раздел 3. Современные шифры с асимметричным ключом.		
9	Тема 9. Алгоритмы шифрования с открытыми ключами. Концепция криптографии с открытым ключом. Криптосистема RSA. Стойкость RSA.Виды атак на RSA.	1,5	
	Итого 5 семестр	**13,5**	
	6 семестр		
10	Тема 10. Алгоритмы генерации простых чисел. Проверка чисел на простоту. Способы проверки на простое число. Решето Эратосфена. Phi-функция Эйлера. Простые числа Мерсенны. Простые числа Ферма.Детерминированные и вероятностные алгоритмы проверки чисел на простоту.	1,5	
11	Тема 11. Сложность криптографических алгоритмов. Понятие сложности алгоритма. Линейная, полиномиальная и неполиномиальная сложность. Класс NP – полных задач.Способы определения сложности алгоритмов. Сложность известных алгоритмов, используемых в криптографии и криптоанализе.	1,5	
12	Тема 12. Криптосистемы с открытым ключом. Криптосистема Рабина. Криптографическая система Эль-Гамаля. Алгоритмы шифрования, дешифрования и генерации ключей в криптосистемах Рабина и Эль-Гамаля. Безопасность данных криптосистем.	1,5	
13	Тема 13.Криптосистемы на основе метода эллиптических кривых. Эллиптические кривые в вещественных числах. Эллиптические кривые в GF(p). Эллиптические кривые в $GF(2^n)$. Криптография эллиптической кривой, моделирующая криптосистему Эль-Гамаля. Генерация общедоступных и частных ключей. Шифрование и дешифрование.Безопасность криптосистемы с эллиптической кривой.	1,5	

	Раздел 4. Методы установления подлинности и целостности данных.		
14	Тема 14.Аутентификация данных. Электронная цифровая подпись. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП. Алгоритмы ЭЦП: RSA, Эль-Гамаля, ФиатаШамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ванАнтверпена. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94. 9	1,5	
15	Тема 15. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля. Алгоритм формирования схемы Эль-Гамаля. Алгоритм формирования цифровой подписи. Проверка подписи.	1,5	
	Раздел 5. Криптографические протоколы.		
16	Тема 16. Понятие о структуре и способах построения криптографических протоколов. Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Парольные схемы и протоколы "рукопожатия". Взаимосвязь между протоколами аутентификации и цифровой подписи. Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации.	1,5	
17	Тема 17. Атаки на криптографические протоколы. Виды атак, способ подмены пользователя сети, способ замены долговременного ключа.Способы отражения атак.	1,5	
	Итого 6 семестр	**12**	
	Итого	**25,5**	

7.3 Наименование лабораторных работ

№ темы	Наименование тем дисциплины, их краткое содержание	Обьем часов	Интерактивая форма проведения
	5семестр		
1	Лабораторная работа 1. Программная реализация алгоритма Евклида для вычисления наибольшего общего делителя двух чисел.	**3**	
1	Лабораторная работа 2. Программная реализация расширенного алгоритма Евклида.	**3**	
1	Лабораторная работа 3. Применение расширенного алгоритма Евклида для решения уравнений сравнения, линейных диофантовых уравнений и нахождения мультипликативной инверсии.	**3**	
2-3	Лабораторная работа 4. Программная реализация классических шифров с симметричным ключом.	**6**	
4	Лабораторная работа 5.Программная реализация основных компонентов современных шифров с симметричным	**6**	Компьютерные симуляции

	ключом.		
6	Лабораторная работа 6.Программная реализация шифра DES.	**6**	Компьютерные симуляции
	Итого 5 семестр	**27**	**12**
	6 семестр		
10	Лабораторная работа 7. Программная реализация генератора простых чисел.	**6**	
12	Лабораторная работа 8.Программная реализация шифра RSA.	**6**	Компьютерные симуляции
14-15	Лабораторная работа 9.Программная реализация ЭЦП.	**6**	Компьютерные симуляции
16	Лабораторная работа 10.Программная реализация криптографических протоколов.	**6**	
	Итого за 6 семестр	**24**	**12**
	Итого	**51**	**24**

7.4 Наименованиепрактических занятий

Данный вид работы не предусмотрен учебным планом

7.5 Технологическая карта самостоятельной работы обучающегося

Код реализуемой компетенции	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Обьем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
ОПК-2, ОПК-4, ПК-1	Самостоятельное изучение литературы	конспект	Собеседование	4,86	0,54	5,4
	Подготовка к лабораторным работам	отчет	Отчет письменный	7,29	0,81	8,1
Итого 5 семестр				**12,15**	**1,35**	**13,5**
ОПК-2, ОПК-4, ПК-1	Самостоятельное изучение литературы	конспект	Собеседование	9,72	1,08	10,8
	Подготовка к лабораторным работам	отчет	Отчет письменный, собеседование	6,48	0,72	7,2
	Подготовка к экзамену	экзамен	экзамен	24,3	2,7	27,0
Итого 6 семестр				**40,5**	**4,5**	**45**
Итого				**52,65**	**5,85**	**58,5**

8. Фонд оценочных средств для проведения промежуточной аттестации обучающегося по дисциплине

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОП ВО. Паспорт фонда оценочных средств

Фонд оценочных средств, позволяющий оценить уровень

сформированностикомпетенций, размещен в УМК дисциплины «Криптографические методы защиты информации»на кафедре информационной безопасности, систем и технологий и представлен следующими компонентами:

Код оцениваемой компетенции	Этап формирования компетенции (№ темы)	Средства и технологии оценки	Тип контроля (текущий/ промежуточ-ный)	Вид контроля (устный / письменный)	Наименование оценочного средства
5 семестр					
ОПК-2, ОПК-4, ПК-1	Темы 1 - 9	Собеседова-ние	текущий	устный	Вопросы для собеседования
ОПК-2, ОПК-4, ПК-1	Темы 1 –4,6	Отчет	текущий	письменный	Темы индивидуаль-ныхзаданий для лабора-торных работ
6 семестр					
ОПК-2, ОПК-4, ПК-1	Темы 10 - 17	Собеседова-ние	текущий	устный	Вопросы для собеседования
ОПК-2, ОПК-4, ПК-1	Темы 10, 12, 14 - 16	Отчет	текущий	письменный	Темы индивидуаль-ныхзаданий для лабора-торных работ
ОПК-2, ОПК-4, ПК-1	Темы 1 - 17	Экзамен	промежу-точный	устный	Вопросы к экзамену
				устный	Вопросы для проверки уровня знаний
				устный	Вопросы (задания) для проверки умений и навыков

8.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Уровни сформиро-ванности компетенций	Индикаторы	Дескрипторы			
		2 балла	3 балла	4 балла	5 баллов*
Базовый	**Знать:** **ОПК-2** – основные задачи и понятия крипто-графии; – модели шифров;	Не знает основныепо нятия криптогра-фии.	Знает основные задачи и понятия криптографи и, но не все модели	Знает основные задачи и понятия криптографии, а также модели	

			шифров;	шифров;	
	ОПК-4 – требования к шифрам и их основные характеристики; – принципы построения криптографических алгоритмов;	Не знает требования к шифрам, их основные характеристики и принципыпостроения криптографических алгоритмов;	Знает требования к шифрам, их основные характеристики, но испытывает затруднения при изложениипринциповпостроения криптографических алгоритмов;	Знает требования к шифрам, их основные характеристики и принципыпостроения криптографических алгоритмов;	
	ПК-1 – структуру государственной системы защиты информации; – основные руководящие, методические и нормативные документы по криптографии.	Не знает структуру государственной системы защиты информации и основные нормативныедокументы по криптографии.	Недостаточно хорошо знает структуру государственной системы защиты информации и основные нормативные документы по криптографии	Знает структуру государственной системы защиты информации; основные нормативныедокументы по криптографии.	
	Уметь: **ОПК-2** применять математический аппарат для решения профессиональных задач;	Не умеет применять математический аппарат для решения профессиональных задач.	Недостаточно хорошо умеет применять математический аппарат для решения профессиональных задач	Умеет применять математический аппарат для решения профессиональных задач.	
	ОПК-4 – применять методы криптографии при решении задач защиты информации; – осуществлять программную реализацию криптографических алгоритмов;	Не умеет применять методы криптографии при решении задач защитыинформации ипрограммно реализовыватькриптографические алгоритмы	Умеет применять методы криптографии при решении задач защиты информации, но испытываетзатруднения припрограммной реализациикриптографическихалгоритмов	Умеет применять методы криптографии при решении задач защиты информации ипрограммно реализовыватькриптографические алгоритмы	

	ПК-1 выполнять работы по установке, настройке и обслуживанию криптографических средств защиты информации;	Не умеет выполнять работы по установке, настройке и обслуживанию криптографических средств защиты информации;	Недостаточно хорошо умеет выполнять работы по установке, настройке и обслуживанию криптографических средств защиты информации	Умеет выполнять работы по установке, настройке и обслуживанию криптографических средств защиты информации	
	Владеть: **ОПК-2** – криптографии-ческойтерминологией; – навыками применения математического аппарата при реализации типовых криптографических алгоритмов;	Не владеет криптографической терминологией и навыками применения математического аппарата при реализациитиповыхкриптографиических алгоритмов;	Владеет криптографической терминоло-гией, но имеет недостаточные навыки применения математического аппарата при реализации типовых криптографических алгоритмов;	Владеет криптографической терминологией и навыками применения математического аппарата при реализации типовых криптографических алгоритмов;	
	ОПК-4 – навыками применения методов криптографии при решении задач защиты информации; – навыками программной реализации криптографических алгоритмов;	Не владеет навыками применения методов криптографиии программной реализации криптографических алгоритмов.	Владеет недостаточно уверенно навыками применения методов криптографиии программной реализации криптографических алгоритмов.	Владеет навыками применения методов криптографии и програм-мной реализации криптографических алгоритмов.	
	ПК-1 – навыками приемки, освоения и эксплуатации вводимых технологий и средств криптографии в соответствии с действующими нормативами;	Не владеет навыками приемки, освоения и эксплуатации вводимых технологий и средств криптографии в соответствии с действующими нормативами	Владеет недостаточно уверенно навыками приемки, освоения и эксплуатации вводимых технологий и средств криптографии в соответствии с дей-	Владеет навыками приемки, освоения и эксплуатации вводимых технологий и средств криптографии в соответствии с действующими нормативами;	

			ствующими нормативами;		
Повышенный	**Знать:** **ОПК-2** математические методы исследования моделей шифров;				Знает математические методы исследования моделей шифров.
	ОПК-4 криптографические стандарты;				Знает криптографические стандарты.
	ПК-1 показатели эффективности криптографической защиты и методы их оценки;				Знает показателиэффективностикриптогра-фической защиты и методы их оценки
	Уметь: **ОПК-2** применять математический аппарат для решения профессиональных задач повышенной сложности;				Умеет применять математический аппарат для решения профессиональных задач повышенной сложности;
	ОПК-4 – проводить анализ стойкости криптосистем; – пользоваться научно-технической литературой в области криптографии;				Умеет проводить анализ стойкости криптосистем и пользоваться научно-технической литературой в области криптографии;
	ПК-1 применять отечественные и зарубежные стандарты криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности				Умеет применять отечественные и зарубежные стандарты криптографических методов компьютернойбезопасности.

	компьютерных систем;				
	Владеть: **ОПК-2** навыками оценки криптостойкости типовых криптографичес-ких алгоритмов;				Владеет навыками оценки криптостой-кости типовых криптографи-ческих алгоритмов;
	ОПК-4 навыками проведения анализа стойкости криптосистем;				Владеет навыками проведения анализа стойкости криптосистем
	ПК-1 методами наладки программного обеспечения, настройки, испытания и сдачи в эксплуатацию средств криптографии.				Владеет методами наладки программно-гообеспече-ния, настрой-ки, испыта-ния и сдачи в эксплуата-цию средств криптогра-фии.

Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по дисциплине оценивается в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

Рейтинговая оценка знаний студента

№ п/п	Вид деятельности студентов	Сроки выполнения	Количество баллов
5 семестр			
1.	Сдача отчетов по лабораторным работам 1-3. Собеседование по темам 1-2.	8 неделя	25
2.	Сдача отчетов по лабораторным работам 4-6. Собеседование по темам 3-6.	16 неделя	30
	Итого 5 семестр		**55**
6 семестр			
3.	Сдача отчетов по лабораторным работам 7-8. Собеседование по темам 9-10.	8 неделя	25
4.	Сдача отчетов по лабораторным работам 9-10. Собеседование по темам 14-16.	14 неделя	30
	Итого 6 семестр		**55**
	Итого		**110**

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый

балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

Промежуточная аттестация

Промежуточная аттестацияв 5 семестре проводится в форме **зачета**.

Процедура зачета как отдельное контрольное мероприятие не проводится, оценивание знаний обучающегося происходит по результатам текущего контроля.

Зачет выставляется по результатам работы в семестре, при сдаче всех контрольных точек, предусмотренных текущим контролем успеваемости. Если по итогам семестра обучающийся имеет от 33 до 60 баллов, ему ставится отметка «зачтено». Обучающемуся, имеющему по итогам семестра менее 33 баллов, ставится отметка «не зачтено».

Количество баллов за зачет ($S_{зач}$) при различных рейтинговых баллах по дисциплине по результатам работы в семестре

Рейтинговый балл по дисциплине по результатам работы в семестре ($R_{сем}$)	**Количество баллов за зачет ($S_{зач}$)**
$50 \le R_{сем} \le 60$	**40**
$39 \le R_{сем} < 50$	**35**
$33 \le R_{сем} < 39$	**27**
$R_{сем} < 33$	**0**

Промежуточная аттестацияв 6 семестре проводится в форме **экзамена,**предусматривает проведение обязательной экзаменационной процедуры и оценивается 40 баллами из 100. Минимальное количество баллов, необходимое для допуска к экзамену, составляет 33 балла. Положительный ответ студента на экзамене оценивается рейтинговыми баллами в диапазоне от **20** до **40** (**$20 \le S_{экз} \le 40$**), оценка **меньше 20** баллов считается неудовлетворительной.

Шкала соответствия рейтингового балла экзамена 5-балльной системе

Рейтинговый балл по дисциплине	**Оценка по 5-балльной системе**
35 – 40	Отлично
28 – 34	Хорошо
20 – 27	Удовлетворительно

Итоговая оценка по дисциплине, изучаемой в одном семестре, определяется по сумме баллов, набранных за работу в течение семестра, и баллов, полученных при сдаче экзамена:

Шкала пересчета рейтингового балла по дисциплине в оценку по 5-балльной системе

Рейтинговый балл по дисциплине	Оценка по 5-балльной системе
88 – 100	Отлично
72 – 87	Хорошо
53 – 71	Удовлетворительно
<53	Неудовлетворительно

8.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Вопросы к экзамену (6 семестр)

Вопросы (задача, задание) для проверки уровня обученности.

Знать

1. Основные понятия в области криптографии.
2. Классификация классических шифров: шифры замены и перестановки, поточные и блочные шифры, моноалфавитные и многоалфавитные шифры.
3. Виды атак криптоанализа. Способы противодействия им.
4. Классические шифры с симметричным ключом. Шифры замены: аддитивные, мультипликативные, аффинные, автоключевой, Виженера, Плейфера, Хилла, роторный, одноразового блокнота. Криптоанализ шифров замены.
5. Классические шифры перестановки: бесключевой шифр, ключевые шифры и шифры с двойной перестановкой. Криптоанализ шифров перестановки.
6. Современныеблочные шифры с симметричным ключом. Основные компоненты современного блочного шифра. ШифрыФейстеля и не-Фейстеля.Атаки на блочные шифры.
7. Современныепоточные шифры с симметричным ключом. Синхронные и несинхронные шифры потока. Преимущества и проблемы современных шифров потока. Криптоанализ шифров потока.
8. Современный стандарт шифрования (DES). Структура шифра DES. Раунды шифрования. Функция DES. Генерация ключей раундов.
9. Двукратный и трехкратный DES. Криптоанализ шифра DES.
10. Усовершенствованный стандарт шифрования (AES). Алгоритм расширения ключей. Анализ расширения ключа. Алгоритмы шифрования и дешифрования в AES. Анализ AES.
11. Российский стандарт ГОСТ 28147-89, особенности, принципы построения, методы шифрования.
12. Алгоритмы шифрования с открытыми ключами.Концепция криптографии с открытым ключом. Криптосистема RSA. Стойкость RSA. Виды атак на RSA.
13. Алгоритмы генерации простых чисел. Проверка чисел на простоту. Способы проверки на простое число. Решето Эратосфена. Phi-функция Эйлера. Простые числа Мерсенны. Простые числа Ферма. Детерминированные и вероятностные алгоритмы проверки чисел на простоту.
14. Сложность криптографических алгоритмов. Понятие сложности алгоритма. Линейная, полиномиальная и неполиномиальная сложность. Класс NP – полных задач.Способы определения сложности алгоритмов. Сложность известных алгоритмов, используемых в криптографии и криптоанализе.
15. Криптосистемы с открытым ключом. Криптосистема Рабина. Криптосистема Эль-Гамаля. Алгоритмы шифрования, дешифрования и генерации ключей в криптосистемах Рабина и Эль-Гамаля. Безопасность данных криптосистем.
16. Криптосистемы на основе метода эллиптических кривых. Эллиптические кривые в вещественных числах. Эллиптические кривые в GF(p). Эллиптические кривые в $GF(2^n)$. Криптография эллиптической кривой, моделирующая

криптосистему Эль-Гамаля. Генерация общедоступных и частных ключей. Шифрование и дешифрование.Безопасность криптосистемы с эллиптической кривой.

17. Аутентификация данных. Электронная цифровая подпись. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП.

18. Алгоритмы ЭЦП: RSA, Эль-Гамаля, ФиатаШамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ванАнтверпена.

19. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.9.

20. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля.Алгоритм формирования схемы Эль-Гамаля. Алгоритм формирования цифровой подписи. Проверка подписи.

21. Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Парольные схемы и протоколы "рукопожатия".

22. Взаимосвязь между протоколами аутентификации и цифровой подписи. Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации.

23. Атаки на криптографические протоколы. Виды атак, способ подмены пользователя сети, способ замены долговременного ключа.Способы отражения атак.

Уметь

1. Шифровать тексты с помощью классических шифров.
2. Шифровать двоичные последовательности с помощью современных шифров.
3. Проверять требования к криптосистемам.
4. Использовать перестановки, подстановки и их комбинации.
5. Отражать атаки на криптографические протоколы.
6. Выбирать правильно параметры для шифрования наиболее известными шифрами.
7. Реализовывать криптографические методы.
8. Оценивать криптостойкость алгоритма шифрования.

Владеть

1. Методами управления ключами.
2. Методами генерации, накопления и распределения ключей.
3. Основами знаний по порядку разработки схемы ЭЦП Рабина.
4. Основами знаний по порядку разработки схемы ЭЦП Диффи - Хэллмана.
5. Основами знаний по порядку разработки схемы ЭЦП Эль-Гамаля.
6. Способами построения криптографических протоколов.
7. Способами отражения атак на криптографические протоколы.

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

Процедура проведения **экзамена** осуществляется в соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования в СКФУ.

В экзаменационный билет включаются два теоретических вопроса.

Для подготовки по билету отводится от 40 до 60 минут.

При подготовке к ответу студенту предоставляется право пользования собственными лекциями и лабораторными, а также любой справочной литературой (в течение 3-5 минут) и калькулятором.

Текущая аттестация студентов проводится преподавателем, ведущим лабораторные занятия по дисциплине в форме письменного отчета и собеседования. Допуск к лабораторным работам происходит при наличии у студентов печатного варианта отчета. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя.

Максимальное количество баллов студент получает, если оформление отчета соответсвует установленным требованиям, а отчет полностью раскрывает суть работы. Основанием для снижением оценки являются:

– слабое знание темы и основной терминологии;

– отсутствие умения применить теоретические знания для решения практических задач;

– несвоевременность предоставления выполненных лабораторных работ или несвоевременная их защита.

Отчет может быть отправлен на доработку в следующих случаях:

– неверное оформление;

– неполное раскрытие темы;

– выполнение задания по чужому варианту.

Критерии оценивания конспектов и отчетов приведены в Фонде оценочных средств по дисциплине «Криптографические методы защиты информации».

9. Методические указания для обучающихся по освоению дисциплины

На первом этапе необходимо ознакомиться с рабочей программой дисциплины, в которой рассмотрено содержание тем дисциплины лекционного курса, взаимосвязь тем лекций с лабораторными занятиями, темы и виды самостоятельной работы. По каждому виду самостоятельной работы предусмотрены определённые формы отчетности.

Для успешного освоения дисциплины, необходимо выполнить следующие виды самостоятельной работы, используя рекомендуемые источники информации:

№ п/п	Виды самостоятельной работы	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая	Интернет-ресурсы
1	Самостоятельное изучение литературы	1	1-2	1-2	1-6
2	Подготовка к лабораторным работам	1	1-2	1-2	1-6
3	Подготовка к экзамену	1	1-2	1-2	1-6

10. Учебно-методическое и информационное обеспечение дисциплины

10.1. Рекомендуемая литература

10.1.1. Основная литература:

1. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванов, И.В. Чугунков; под ред. М.А. Иванова; Министерство образования и науки Российской Федерации, Национальный исследовательский ядерный университет «МИФИ». - М.: МИФИ, 2012. - 400 с.: табл., схем. - ISBN 978-5-7262-1676-8; То же [Электронный ресурс]. - URL: //biblioclub.ru /index.php?page=book&id=231673

10.1.2 Дополнительная литература:

1.Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с.: ил. - (Основы

информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429092.

2. Жуков А.Е. Системы блочного шифрования [Электронный ресурс]: учебное пособие по курсу «Криптографические методы защиты информации»/ Жуков А.Е.— Электрон.текстовые данные.— М.: Московский государственный технический университет имени Н.Э. Баумана, 2013.— 80 с.— Режим доступа: http://www.iprbookshop.ru/31633.— ЭБС «IPRbooks».

10.1.3Методическая литература:

1. Методические указания по выполнению лабораторных работ по дисциплине «Криптографические методы защиты информации» для студентов направления подготовки 10.03.01 «Информационная безопасность» очной формы обучения. Пятигорск, 2017.

2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Криптографические методы защиты информации» для студентов направления подготовки 10.03.01«Информационная безопасность» очной формы обучения. Пятигорск, 2017.

10.1.4 Интернет-ресурсы:

1. Университетская библиотека online. http://www.biblioclub.ru.
2. ЭБС «IPRbooks». http://www.iprbookshop.ru.
3. Электронная библиотека СКФУ.. http://catalog.ncstu.ru.
4. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.

11. Программное обеспечение

Базовый пакет программ Microsoft Office Standard 2013. Бессрочная лицензия. Дата окончания срока поддержки (обновления) 11.04.2023г., Microsoft Windows Профессиональная. Бессрочная лицензия

12. Материально-техническое обеспечение дисциплины

1. Учебная аудитория для проведения занятий лекционного типа: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: проектор, экран настенный, персональный компьютер.

Учебно-наглядные пособия в виде тематических презентаций, соответствующих рабочим программам дисциплин

2. Учебная аудитория для проведения занятий семинарского типа (лабораторных работ): Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, компьютер преподавателя, проектор , доска магнитно-маркерная

Подключение к сети «Интернет», выход в корпоративную сеть университета

3. Учебная аудитория для групповых и индивидуальных консультаций: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: проектор, доска магнитно-маркерная, персональные компьютеры, переносной ноутбук

4. Учебная аудитория для текущего контроля и промежуточной аттестации: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: проектор, доска магнитно-маркерная, персональные компьютеры, переносной ноутбук