МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зам. директора по учебной работе
ИСТиД (филиал) СКФУ в г. Пятигорске
_____ М.В. Мартыненко
«_____» _____ 202_ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Математические основы криптологии»

Направление подготовки	**10.03.01 Информационная безопасность**
Направленность (профиль)	**Комплексная защита объектов информатизации**
Квалификация выпускника	бакалавр
Форма обучения	Очная
Год начала обучения	2020 г.
Реализуется в 5 семестре	

СОГЛАСОВАНО:
Зав. кафедрой систем управления и информационных технологий
_____ И.М. Першин
"__" _____ 202___ г.

Рассмотрено УМК
Протокол №___
от «___»_____202_г.

Председатель УМК института
_____ Нарыжная А.Б.

РАЗРАБОТАНО:
Зав. кафедрой систем управления и информационных технологий
_____ И.М. Першин
"__" _____ 202___ г.

доцент кафедры систем управления и информационных технологий
_____ Битюцкая Н.И.
«__» _____ 202_ г.

Пятигорск, 2020

1. Цель и задачи освоения дисциплины

Цель изучения дисциплины «Математические основы криптологии» - теоретическая и практическая подготовка студентов в изучении математических основ криптологии и их применении для решения задач повышения криптостойкости систем шифрования, уяснения особенностей применения генераторов псевдослучайных величин при создании ключей шифрования.

Основные задачи изучения дисциплины:

- ознакомить студентов с общими задачами, решаемыми криптологией;
- дать сведения о месте, занимаемом предметом «Математические основы криптологии», в решении задач защиты информации;
- дать сведения об использовании рекуррентных генераторов псевдослучайных чисел в алгоритмах создания криптостойких ключей;
- научить использовать функции усложнения и рандомизации для решения задач повышения криптостойкости и имитостойкости шифрованной информации.

2. Место дисциплины в структуре ОП

Дисциплина является дисциплиной по выбору блока Б1, её освоение происходит в 5 семестре.

3. Связь с предшествующими дисциплинами

Пререквизитом является дисциплина «Дискретная математика».

4. Связь с последующими дисциплинами

Знания, умения и навыки, приобретенные студентами при изучении дисциплины, необходимы для успешного освоения дисциплин «Криптографические методы защиты информации».

5. Компетенции обучающегося, формируемые в результате изучения дисциплины

5.1 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.
ПСК-3	Способность изучать и обобщать опыт различных учреждений, организаций и предприятий в области повышения эффективности защиты информации.
ПСК-5	Способность разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение.
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

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

Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций	Формируемые компетенции
Знать:	ОПК-2

– основные задачи и понятия криптографии; – 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; – основные методы создания генераторов псевдослучайных чисел, области их применения в системах шифрования;	ОПК-4
Уметь: – применять методы криптографии при решении задач защиты информации; – пользоваться научно-технической литературой в области криптографии;	ОПК-4
Владеть: – навыками применения математических методов при решении задач криптографической защиты информации;	ОПК-4
Знать: – методы и способы криптографической защиты информации; – показатели эффективности криптографической защиты и методы их оценки;	ПСК-3
Уметь: – изучать и обобщать опыт различных учреждений, организаций и предприятий в области повышения эффективности защиты информации.	ПСК-3
Владеть: – навыками обобщения опыта различных учреждений, организаций и предприятий в области повышения эффективности защиты информации.	ПСК-3
Знать: – структуру государственной системы защиты информации; – основные руководящие, методические и нормативные документы по криптографии.	ПСК-5
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;	ПСК-5
Владеть: – навыками осуществления приемки, освоения и эксплуатации вводимых технологий и средств криптографии в соответствии с действующими нормативами; – методами осуществления наладки программного обеспечения,	ПСК-5

настройки, испытания и сдачи в эксплуатацию средств криптографии.	
Знать: – работу по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1
Уметь: – выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1
Владеть: – способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1

6. Объем учебной дисциплины/модуля

	Астр. часов	
Объем занятий: Итого	108 ч.	3 з.е.
В том числе аудиторных	54 ч.	
Из них:		
Лекций	24,0 ч.	
Лабораторных работ	12,0 ч.	
Практических занятий	12,0 ч.	
Самостоятельной работы	33,0 ч.	
Экзамен	в 5 семестре.	

7. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества астрономических 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. Арифметические и **алгебраические основы криптологии.**						
1.	Тема 1. Основные понятия и термины криптографии.	ОПК-2, ОПК-4, ПСК-3,	1,5				1,5
2.	Тема 2. Основы теории делимости.		1,5	1,5	3		1,5
3.	Тема 3. Модульная арифметика.		1,5	1,5	3		1,5

4.	Тема 4. Матрицы вычетов.	ПСК-5, ПК-1	1,5	1,5			1,5
5.	Тема 5. Проверка чисел на простоту.		1,5	1,5	1,5		1,5
6.	Тема 6. Алгоритмы генерации простых чисел.		1,5		1,5		1,5
7.	Тема 7. Разложение чисел на простые множители		1,5	1,5	1,5		1,5
8.	Тема 8. Китайская теорема об остатках.		1,5	1,5	1,5		1,5
9.	Тема 9. Алгебраические основы криптологии.		1,5	1,5			1,5
10.	Тема 10. Эллиптические кривые.		1,5				1,5
	Раздел 2. Криптографические алгоритмы и их сложность.						
11.	Тема 11. Классификация криптосистем.	ОПК-2, ОПК-4, ПСК-3, ПСК-5, ПК-1	1,5	1,5			1,5
12.	Тема 12. Классические шифры замены.		1,5				1,5
13.	Тема 13. Классические шифры перестановки.		1,5				1,5
14.	Тема 14. Современные блочные шифры с симметричным ключом.		1,5				1,5
15.	Тема 15. Современные шифры с асимметричным ключом.		1,5				6
16.	Тема 16. Сложность криптографических алгоритмов.		1,5				6
	Итого за 4 семестр:		**24,0**	**12,0**	**12,0**		**33,0**
	Итого:		**24,5**	**12,0**	**12,0**		**33,0**

7.2 Наименование и содержание лекций

№	Наименование тем дисциплины, их краткое содержание	Обьем часов	Интерактивная форма проведения
	5 семестр		
	Раздел 1. Арифметические и алгебраические основы криптологии.		
1	Тема 1. Основные понятия и термины криптографии. Методы защиты информации. Криптография и криптоанализ. Исторические сведения о развитии криптографии. Понятие шифра и ключа. Симметричные и ассиметричные алгоритмы шифрования.	1,5	
2	Тема 2. Основы теории делимости. Основные понятия теории делимости целых чисел. Алгоритм Евклида нахождения наибольшего общего делителя. Расширенный алгоритм Евклида. Решение линейных диофантовых уравнений.	1,5	
3	Тема 3. Модульная арифметика. Операции по модулю. Система вычетов. Сравнение по модулю. Свойства оператора mod. Аддитивная и мультипликативная инверсии чисел. Применение расширенного алгоритма Евклида для нахождения мультипликативной инверсии. Решение уравнений с одним неизвестным, содержащих сравнение.	1,5	

4	Тема 4. Матрицы вычетов. Определение матрицы вычетов. Операции над матрицами вычетов. Решение систем уравнений, содержащих сравнения.	1,5	
5	Тема 5. Проверка чисел на простоту. Способы проверки на простое число. Решето Эратосфена. Phi-функция Эйлера. Простые числа Мерсенны. Простые числа Ферма. Теорема Ферма. Теорема Эйлера.	1,5	
6	Тема 6. Алгоритмы генерации простых чисел. Генераторы псевдослучайных чисел. Детерминированные и вероятностные алгоритмы проверки чисел на простоту.	1,5	
7	Тема 7. Разложение чисел на простые множители. Основная теорема арифметики. Приложения разложения на множители. Алгоритмы разложения на множители: метод проверки делением, метод Ферма, метод PO (Rho) Полларда.	1,5	
8	Тема 8. Китайская теорема об остатках. Китайская теорема об остатках. Решение систем линейных уравнений с модулями. Примеры практических задач.	1,5	
9	Тема 9. Алгебраические основы криптологии. Группы, кольца, поля, их определения и виды, полиномы над структурой.	1,5	
10	Тема 10. Эллиптические кривые. Эллиптические кривые в вещественных числах. Эллиптические кривые в GF(p). Эллиптические кривые в $GF(2^n)$.	1,5	
	Раздел 2. Криптографические алгоритмы и их сложность.		
11	Тема 11. Классификация криптосистем. Классификация классических шифров: шифры замены и перестановки, поточные и блочные шифры, моноалфавитные и многоалфавитные шифры. Современные шифры с закрытым и открытым ключом.	1,5	
12	Тема 12. 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	
13	Тема 13. Классические шифры перестановки. Бесключевой шифр, ключевые шифры и шифры с двойной перестановкой. Криптоанализ шифров перестановки.	1,5	
14	Тема 14. Современные блочные шифры с симметричным ключом. Различия между современными и традиционными шифрами с симметричным ключом. Современные блочные шифры: шифры замены и шифры	1,5	

	перестановки. Основные компоненты современного блочного шифра.		
15	Тема 15. Современные шифры с асимметричным ключом. Концепция криптографии с открытым ключом. Алгоритмы шифрования с открытыми ключами.	1,5	
16	Тема 16. 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	
	Итого за 5 семестр	**24**	
	Итого	**24**	

7.3 Наименование лабораторных работ

№ темы	Наименование тем дисциплины, их краткое содержание	Обьем часов	Интерактивая форма проведения
	5 семестр		
2	Лабораторная работа 1. Программная реализация алгоритма Евклида для вычисления наибольшего общего делителя двух чисел.	1,5	Компьютерные симуляции
2	Лабораторная работа 2. Программная реализация расширенного алгоритма Евклида.	1,5	Компьютерные симуляции
3	Лабораторная работа 3. Применение расширенного алгоритма Евклида для решения уравнений сравнения, линейных диофантовых уравнений и нахождения мультипликативной инверсии.	3	
5-6	Лабораторная работа 4. Программная реализация генераторов простых чисел.	3	Компьютерные симуляции
7-8	Лабораторная работа 5. Программная реализация классических задач теории чисел, применяемых в криптографии	3	Компьютерные симуляции
	Итого за 5 семестр	**12,0**	**9**
	Итого	**12,0**	**9**

7.4 Наименование практических занятий

№ темы	Наименование работы	Обьем часов	Форма проведения
	5 семестр		
2	Алгоритм Евклида. Расширенный алгоритм Евклида.	1,5	
3	Модульная арифметика. Применение расширенного алгоритма Евклида	1,5	решение разноуровневых и проблемных задач
4	Матрицы вычетов	1,5	
5-6	Проверка чисел на простоту	1,5	решение разноуровневых и

			проблемных задач
7	Разложение чисел на множители	1,5	групповое решение задач
8	Китайская теорема об остатках	1,5	групповое решение задач
9	Алгебраические основы криптологии	1,5	групповое решение задач
11, 12	Классические шифры замены	1,5	групповое решение задач
	Итого за 5 семестр	**12,0**	**9**
	Итого	**12,0**	**9**

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 ПСК-3 ПСК-5 ПК-1	Подготовка к лекциям	конспект	Собеседование	2,16	0,24	2,4
	Самостоятельное изучение литературы	конспект	Собеседование	68,58	7,62	76,2
	Подготовка к лабораторным и практическим занятиям	отчет	Отчет письменный	2,16	0,24	2,4
Итого 5 семестр				**72,9**	**8,1**	**81**
Итого				**72,9**	**8,1**	**81**

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 сформированности компетенций, размещен в УМК дисциплины «Математические основы криптологии» 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/ промежуточный)	Вид контроля (устный / письменный)	Наименование оценочного средства
5 семестр					
ОПК-2, ОПК-4, ПСК-3,	Темы 1 - 16	Собеседование	текущий	устный	Вопросы для собеседования

ПСК-5, ПК-1					
ОПК-2, ОПК-4, ПСК-3, ПСК-5, ПК-1	Темы 2, 3, 5-8	Отчет	текущий	письменный	Темы индивидуальных заданий для лабораторных работ
ОПК-2, ОПК-4, ПСК-3, ПСК-5, ПК-1	Темы 2-9, 11-12	Отчет	текущий	письменный	Темы индивидуальных заданий для практических занятий

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

Уровни сформированности компетенций	Индикаторы	Дескрипторы			
		2 балла	3 балла	4 балла	5 баллов
	ОПК-2				
Базовый	**Знать:** основные задачи и понятия криптографии;	Отсутствуют знания основных задач и понятий криптографии	Частичные знания основных задач и понятий криптографии;	Знает основные задачи и понятия криптографии;	
	Уметь: применять математический аппарат для решения профессиональных задач;	Не умеет применять математический аппарат для решения профессиональных задач;	Частично умеет применять математический аппарат для решения профессиональных задач;	Умеет применять математический аппарат для решения профессиональных задач;	
	Владеть: криптографической терминологией;	Не владеет криптографической терминологией	Частично владеет криптографической терминологией	Владеет криптографической терминологией	
	ОПК-4				
Базовый	**Знать:** требования к шифрам и основные характеристики шифров;	Не знает требования к шифрам и основные характеристики шифров;	Частично знает требования к шифрам и основные характеристики шифров;	Знает требования к шифрам и основные характеристики шифров;	
	Уметь: применять методы криптографии при решении задач защиты информации;	Не умеет применять методы криптографии при решении задач защиты информации;	Частично умеет применять методы криптографии при решении задач защиты информации;	Умеет применять методы криптографии при решении задач защиты информации;	
	Владеть: навыками применения	Не владеет навыками применения	Частично владеет навыками	Владеет навыками применения	

	математических методов при решении задач криптографической защиты информации;	математических методов при решении задач криптографической защиты информации;	применения математических методов при решении задач криптографической защиты информации;	математических методов при решении задач криптографической защиты информации;	
	ПСК-3				
Базовый	**Знать:** методы и способы криптографической защиты информации;	Не знает методы и способы криптографической защиты информации;	Частично знает методы и способы криптографической защиты информации;	Знает методы и способы криптографической защиты информации;	
	Уметь: изучать опыт различных учреждений, организаций и предприятий в области повышения эффективности защиты информации.	Не умеет изучать опыт различных учреждений, организаций и предприятий в области повышения эффективности защиты информации	Частично умеет изучать опыт различных учреждений, организаций и предприятий в области повышения эффективности защиты информации	Умеет изучать опыт различных учреждений, организаций и предприятий в области повышения эффективности защиты информации.	
	Владеть: навыками изучения опыта различных учреждений, организаций и предприятий в области повышения эффективности защиты информации.	Не владеет навыками изучения опыта различных учреждений, организаций и предприятий в области повышения эффективности защиты информации.	Частично владеет навыками изучения опыта различных учреждений, организаций и предприятий в области повышения эффективности защиты информации.	Владеет навыками изучения опыта различных учреждений, организаций и предприятий в области повышения эффективности защиты информации.	
	ПСК-5				
Базовый	**Знать:** структуру государственной системы защиты информации;	Не знает структуру государственной системы защиты информации;	Частично знает структуру государственной системы защиты информации;	Знает структуру государственной системы защиты информации;	
	Уметь: выполнять работы по установке, настройке и обслуживанию криптографических средств защиты информации;	Не умеет выполнять работы по установке, настройке и обслуживанию криптографических средств защиты информации;	Частично 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:	Не владеет	Частично	Владеет	

	навыками осуществления приемки, освоения и эксплуатации вводимых технологий и средств криптографии в соответствии с действующими нормативами;	навыками осуществления приемки, освоения и эксплуатации вводимых технологий и средств криптографии в соответствии с действующими нормативами	владеет навыками осуществления приемки, освоения и эксплуатации вводимых технологий и средств криптографии в соответствии с действующими нормативами	навыками осуществления приемки, освоения и эксплуатации вводимых технологий и средств криптографии в соответствии с действующими нормативами;	
Базовый	ПК-1				
	Знать: работу по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	Не знает работу по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	Частично знает работу по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	Знает работу по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	
	Уметь: выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Не умеет выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Частично умеет выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	Умеет выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	
	Владеть: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	Не владеет способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств	Частично владеет способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических	Владеет способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и	

		защиты информации	средств защиты информации	технических средств защиты информации;	
	ОПК-2				
Повышенный	**Знать:** модели шифров и математические методы их исследования;				Знает модели шифров и математические методы их исследования;
	Уметь: исследовать модели шифров				Умеет исследовать модели шифров
	Владеть: навыками применения математического аппарата при реализации типовых криптографических алгоритмов и оценке их криптостойкости;				Владеет навыками применения математического аппарата при реализации типовых криптографических алгоритмов и оценке их криптостойкости
	ОПК-4				
Повышенный	**Знать:** основные методы создания генераторов псевдослучайных чисел;				Знает основные методы создания генераторов псевдослучайных чисел;
	Уметь: пользоваться научно-технической литературой в области криптографии;				Умеет пользоваться научно-технической литературой в области криптографии;
	Владеть: методами генерации псевдослучайных чисел				Владеет методами генерации псевдослучайных чисел
	ПСК-3				
Повышенный	**Знать:** показатели эффективности криптографической защиты и методы их оценки;				Знает показатели эффективности криптографической защиты и методы их оценки;
	Уметь: обобщать опыт различных учреждений, организаций и предприятий в области повышения эффективности защиты				Умеет обобщать опыт различных учреждений, организаций и предприятий в области повышения эффективности защиты информации

	информации.				
	Владеть: навыками обобщения опыта различных учреждений, организаций и предприятий в области повышения эффективности защиты информации.				Владеет навыками обобщения опыта различных учреждений, организаций и предприятий в области повышения эффективности защиты информации
	ПСК-5				
Повышенный	**Знать:** основные руководящие, методические и нормативные документы по криптографии.				Знает основные руководящие, методические и нормативные документы по криптографии.
	Уметь: применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;				Умеет применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
	Владеть: методами осуществления наладки программного обеспечения, настройки, испытания и сдачи в эксплуатацию средств криптографии.				Владеет методами осуществления наладки программного обеспечения, настройки, испытания и сдачи в эксплуатацию средств криптографии
Повышенный	ПК-1				
	Знать: работу по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических				Знает работу по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических

	средств защиты информации				средств защиты информации.
	Уметь: выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации				Умеет выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
	Владеть: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.				Владеет способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

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. Сдача отчетов по практическим занятиям 1-4 Собеседование по темам 1-8.	8 неделя	25
2.	Сдача отчетов по лабораторным работам 4-5. Сдача отчетов по практическим занятиям 5-8. Собеседование по темам 9-16.	14 неделя	30
	Итого 5 семестр		**55**
	Итого		**55**

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 аттестация в 5 семестре проводится в форме **зачета с оценкой.**

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**

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

Экзамен не предусмотрен учебным планом.

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

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

Текущая аттестация студентов проводится преподавателем, ведущим лабораторные и практические занятия по дисциплине в форме собеседований и письменных отчетов по результатам выполнения лабораторных и практических работ. Допуск к лабораторным работам происходит при наличии у студентов печатного варианта отчета. Защита отчета проходит в форме устных ответов студентов на вопросы преподавателя. При оценивании ответов учитывается полнота и степень раскрытия темы, владение материалом, ответы на дополнительные вопросы.

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 отчета.

Отчет может быть отправлен на доработку в следующих случаях:

- неверное выполнение задания;

– неверное оформление;
– выполнение задания по чужому варианту.

Критерии оценивания собеседований и письменных отчетов приведены в ФОС по дисциплине «Математические основы криптологии».

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 и практическими 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	1-2	1	1-2	1-6
2.	Подготовка к лабораторным работам	1-2	1	1-2	1-6
3.	Подготовка к практическим занятиям	1-2	1	1-2	1-6

10. Учебно-методическое и информационное обеспечение дисциплины

10.1. Рекомендуемая литература

10.1.1. Основная литература:

1. Фороузан Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. - 2-е изд., испр. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 511 с. : ил., схем. - [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id =428998.

2. Басалова Г.В. Основы криптографии [Электронный ресурс]/ Басалова Г.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 282 с.— Режим доступа: http://www.iprbookshop.ru/52158.— ЭБС «IPRbooks».

10.1.2 Дополнительная литература:

1. Гашков, С. Б. Криптографические методы защиты информации : учеб. пособие / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. - М.: ИЦ "Академия", 2010. - 304 с.

10.1.3 Методическая литература:

1. Методические указания по выполнению лабораторных работ по дисциплине «Математические основы криптологии» 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 «Математические основы криптологии» для студентов направления подготовки 10.03.01 «Информационная безопасность» очной формы обучения. Пятигорск, 2017.

10.1.4 Интернет-ресурсы:

1. http://www.intuit.ru – сайт дистанционного образования в области информационных технологий

2. http://www.iqlib.ru - интернет библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия;

3. http://www.biblioclub.ru - электронная библиотечная система «Университетская библиотека – online»: специализируется на учебных материалах для ВУЗов по научно-гуманитарной тематике, а так же содержит материалы по точным и естественным наукам.

4. http://window.edu.ru – образовательные ресурсы ведущих вузов.

5. http://cryptography.ru – сайт «Математическая криптография».

6. http://algolist.manual.ru - сайт, посвященный алгоритмам и методам.

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

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

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

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

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

3. 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

4. Учебная аудитория для проведения занятий лекционного типа: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: переносной ноутбук, переносной проектор, доска. Учебно-наглядные пособия в виде тематических презентаций, соответствующих рабочим программам дисциплин

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой СУиИТ

_____ И.М.Першин

«____» _____ 202_ г.

Вопросы для собеседования

по дисциплине «Математические основы криптологии»

5 семестр

Базовый уровень

Тема 1. Основные понятия и термины криптографии.
1. Методы защиты информации.
2. Криптография и криптоанализ.
3. Понятие шифра и ключа.
4. Симметричные и ассиметричные алгоритмы шифрования.

Тема 2. Основы теории делимости.
1. Основные понятия теории делимости целых чисел.
2. Алгоритм Евклида нахождения наибольшего общего делителя.
3. Расширенный алгоритм Евклида.

Тема 3. Модульная арифметика.
1. Операции по модулю. Система вычетов.
2. Сравнение по модулю. Свойства оператора mod.
3. Аддитивная и мультипликативная инверсии чисел.

Тема 4. Матрицы вычетов.
1. Определение матрицы вычетов.
2. Операции над матрицами вычетов.

Тема 5. Проверка чисел на простоту.
1. Способы проверки на простое число.
2. Решето Эратосфена.
3. Phi-функция Эйлера.
4. Простые числа Мерсенны.
5. Простые числа Ферма.

Тема 6. Алгоритмы генерации простых чисел.
1. Генераторы псевдослучайных чисел.
2. Детерминированные алгоритмы проверки чисел на простоту.

Тема 7. Разложение чисел на простые множители.
1. Основная теорема арифметики.
2. Приложения разложения на множители.
3. Алгоритмы разложения на множители: метод проверки делением, метод Ферма.

Тема 8. Китайская теорема об остатках.
1. Китайская теорема об остатках.
2. Решение систем линейных уравнений с модулями. Примеры практических задач.

Тема 9. Алгебраические основы криптологии.
1. Группы, кольца, поля, их определения и виды.
Тема 10. Эллиптические кривые.
1. Эллиптические кривые в вещественных числах.
2. Эллиптические кривые в GF(p).
Тема 11. Классификация криптосистем.
1. Классификация классических шифров: шифры замены и перестановки.
2. Поточные и блочные шифры.
3. Моноалфавитные и многоалфавитные шифры.
Тема 12. Классические шифры замены.
1. Классические шифры с симметричным ключом.
2. Шифры замены: аддитивные, мультипликативные, аффинные.
Тема 13. Классические шифры перестановки.
1. Бесключевой шифр.
2. Ключевые шифры.
3. Шифры с двойной перестановкой.
Тема 14. Современные блочные шифры с симметричным ключом.
1. Различия между современными и традиционными шифрами с симметричным ключом.
2. Современные блочные шифры: шифры замены и шифры перестановки.
Тема 15. Современные шифры с асимметричным ключом.
1. Концепция криптографии с открытым ключом.
Тема 16. Сложность криптографических алгоритмов.
1. Понятие сложности алгоритма.
2. Линейная, полиномиальная и неполиномиальная сложность.
3. Класс NP – полных задач.
4. Способы определения сложности алгоритмов.

Повышенный уровень

Тема 1. Основные понятия и термины криптографии.
1. Симметричные и ассиметричные алгоритмы шифрования.
Тема 2. Основы теории делимости.
1. Решение линейных диофантовых уравнений.
Тема 3. Модульная арифметика.
1. Применение расширенного алгоритма Евклида для нахождения мультипликативной инверсии.
2. Решение уравнений с одним неизвестным, содержащих сравнение.
Тема 4. Матрицы вычетов.
1. Решение систем уравнений, содержащих сравнения.
Тема 5. Проверка чисел на простоту.
1. Теорема Ферма.
2. Теорема Эйлера.
Тема 6. Алгоритмы генерации простых чисел.
1. Вероятностные алгоритмы проверки чисел на простоту.
Тема 7. Разложение чисел на простые множители.
1. Алгоритмы разложения на множители: метод PO (Rho) Полларда.
Тема 8. Китайская теорема об остатках.
1. Примеры практических задач на применение китайской теоремы об остатках.
Тема 9. Алгебраические основы криптологии.
1. Полиномы над структурой.
Тема 10. Эллиптические кривые.
1. Эллиптические кривые в $GF(2^n)$.
Тема 11. Классификация криптосистем.
1. Современные шифры с закрытым и открытым ключом.

Тема 12. Классические шифры замены.
1.Криптоанализ шифров замены.
Тема 13. Классические шифры перестановки.
1. Криптоанализ шифров перестановки.
Тема 14. Современные блочные шифры с симметричным ключом.
1. Основные компоненты современного блочного шифра.
Тема 15. Современные шифры с асимметричным ключом.
1. Алгоритмы шифрования с открытыми ключами.
Тема 16. Сложность криптографических алгоритмов.
1. Сложность известных алгоритмов, используемых в криптографии и криптоанализе.

1. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если он в ходе собеседования правильно ответил на вопрос по теме собеседования, сопровождая наглядными примерами.
Оценка «хорошо» выставляется студенту, если он в ходе собеседования ответил на вопрос по теме собеседования, при этом есть неуверенность с практическими примерами.
Оценка «удовлетворительно» выставляется студенту, если он ходе собеседования ответил неуверенно на вопросы по теме собеседования, не смог привести практические примеры.
Оценка «неудовлетворительно» выставляется студенту, если он не ответил на вопрос по теме собеседования.

2. Описание шкалы оценивания

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**

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

Процедура проведения данного оценочного мероприятия включает в себя устные ответы студентов на вопросы собеседования.

Предлагаемые студенту вопросы позволяют проверить компетенции ОПК-2, ОПК-4, ПСК-3, ПСК-5.

Каждому студенту предлагается ответить на два вопроса базового уровня и один вопрос повышенного уровня.

При подготовке к ответу студенту предоставляется право пользования лекциями, и методическими материалами к самостоятельной работе.

При оценивании ответов студента учитываются:

- точность и последовательность формулировок;
- умение приводить конкретные примеры по теме вопроса.

Составитель _____ Н.И. Битюцкая
(подпись)

«____»_____20 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой СУиИТ
_____ И.М.Першин
«____» _____ 202_ г.

Темы индивидуальные заданий для лабораторных работ по дисциплине «Математические основы криптологии»

5 семестр

Индивидуальные задания:

Базовый уровень

1. Вычисление наибольшего общего делителя для двух чисел при помощи алгоритма Евклида.
2. Расширенный алгоритм Евклида.
3. Нахождение мультипликативной инверсии числа по заданному модулю с использованием расширенного алгоритма Евклида.
4. Решение линейного диофантового уравнения с использованием расширенного алгоритма Евклида.
5. Решение уравнения сравнения с использованием расширенного алгоритма Евклида.
6. Реализация детерменированного алгоритма проверки на простоту.
7. Реализация алгоритма решета Эратосфена проверки числа на простоту.
8. Реализация теста Ферма проверки числа на простоту.
9. Реализация алгоритма испытания квадратным корнем проверки числа на простоту.
10. Программная реализация алгоритма разложения числа на множители методом проверки делением.
11. Программная реализация алгоритма Ферма разложения числа на множители.

Повышенный уровень

1. Программная реализация алгоритма Миллера-Рабина проверки числа на простоту.
2. Программная реализация метода РО Полларда разложения числа на множители.
3. Вычисление Phi-функции Эйлера φ(n) для заданного числа n.
4. Решение системы трех уравнений сравнения с одной неизвестной и различными модулями с использованием китайской теоремы об остатках.

1. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если отчет по работе выполнен в соответствии с требованиями, предъявляемыми методическими рекомендациями по выполнению лабораторных работ, а также раскрыты полностью все вопросы по заданию.

Оценка «хорошо» выставляется студенту, если отчет по работе выполнен в соответствии с требованиями, предъявляемыми методическими рекомендациями по выполнению лабораторных работ, а также частично раскрыты вопросы по заданию.

Оценка «удовлетворительно» выставляется студенту, если отчет по работе выполнен в соответствии с требованиями, предъявляемыми методическими

рекомендациями по выполнению лабораторных работ, а также раскрыт не полностью перечень необходимых вопросов по заданию.

Оценка «неудовлетворительно» выставляется студенту, если отчет по работе выполнен не в соответствии с требованиями, предъявляемыми методическими рекомендациями по выполнению лабораторных работ, а также не раскрыты вопросы по заданию.

2. Описание шкалы оценивания

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**

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

Процедура проведения данного оценочного мероприятия включает в себя: выполнение индивидуального задания и оформление отчета по лабораторным работам. Предлагаемые студенту задания позволяют проверить компетенции ОПК-2, ОПК-4, ПСК-3, ПСК-5.

Для подготовки к данному оценочному мероприятию необходимо к концу текущей лабораторной работы предоставить отчет по выполнению лабораторной работы.

При подготовке к ответу студенту предоставляется право пользования справочными материалами.

При проверке задания, оцениваются:

- последовательность и рациональность выполнения;
- знания технологий, использованных при выполнении задания,
- оформление отчета по лабораторной работе.

Составитель _____ Н.И. Битюцкая

«____»_____2020 г.

Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой СУиИТ
_____ И.М.Першин
«____» _____ 202_ г.

Темы индивидуальные заданий для практических занятий по дисциплине «Математические основы криптологии»

5 семестр

Индивидуальные задания:

Базовый уровень

1. Вычисление наибольшего общего делителя для двух чисел при помощи алгоритма Евклида.
2. Расширенный алгоритм Евклида.
3. Нахождение мультипликативной инверсии числа по заданному модулю с использованием расширенного алгоритма Евклида.
4. Решение линейного диофантового уравнения с использованием расширенного алгоритма Евклида.
5. Решение уравнения сравнения с использованием расширенного алгоритма Евклида.
6. Операции над матрицами вычетов.
7. Проверка числа на простоту методом проверки делением.
8. Проверка числа на простоту с помощью решета Эратосфена.
9. Проверка числа на простоту с помощью теста Ферма.
10. Проверка числа на простоту с помощью испытания квадратным
11. Разложения числа на множители с помощью деления.
12. Разложения числа на множители с использованием алгоритма Ферма.

Повышенный уровень

1. Нахождение матрицы вычетов, инверсной данной.
2. Проверка числа на простоту по алгоритму Миллера-Рабина.
3. Разложения числа на множители с помощью метода РО Полларда.
4. Вычисление Phi-функции Эйлера φ(n) для заданного числа n.
5. Решение системы трех уравнений сравнения с одной неизвестной и различными модулями с использованием китайской теоремы об остатках.

4. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если отчет по работе выполнен в соответствии с предъявляемыми требованиями, а также раскрыты полностью все вопросы по заданию.

Оценка «хорошо» выставляется студенту, если отчет по работе выполнен в соответствии с с предъявляемыми требованиями, а также частично раскрыты вопросы по заданию.

Оценка «удовлетворительно» выставляется студенту, если отчет по работе выполнен в соответствии с с предъявляемыми требованиями, а также раскрыт не полностью перечень необходимых вопросов по заданию.

Оценка «неудовлетворительно» выставляется студенту, если отчет по работе выполнен не в соответствии с предъявляемыми требованиями, а также не раскрыты вопросы по заданию.

5. Описание шкалы оценивания

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**

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

Процедура проведения данного оценочного мероприятия включает в себя: выполнение индивидуального задания и оформление отчета. Предлагаемые студенту задания позволяют проверить компетенции ОПК-2, ОПК-4, ПСК-3, ПСК-5.

Для прохождения данного оценочного мероприятия необходимо самостоятельно выполнить индивидуальное задание, выданное преподавателем и подготовить письменный отчет по его выполнению.

При проверке задания, оцениваются:

- последовательность и рациональность выполнения;
- знание теории, использованной при выполнении задания,
- правильность оформления отчета.

Составитель _____ Н.И. Битюцкая

«____»_____2020г.

Оценочный лист

№ п/п	Ф.И.О. студента	Параметры состояния образованности									Итоговый балл
		Предметно-информационная составляющая образованности				Деятельностно-коммуникативная составляющая образованности			Ценностно-ориентационная составляющая образованности		
		Контрольно-методический срез	Общеучебные умения и навыки			Уровень развития устной речи	Умение работать с информацией	Грамотность	Умение использовать получен-ные знания в повседневной жизни	Уровень адекватности самооценки	
			Умение анализировать	Умение доказывать	Умение делать выводы						
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											
9.											
10.											
11.											
12.											
13.											
14.											
15.											
16.											
17.											