Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Северо-Осетинский государственный университет имени Коста Левановича Хетагурова»

УТВЕРЖДАЮ
Проректор по УР
_____ Л.М. Дигурова
«28» ____01____ 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Теория чисел и криптография»

Направление подготовки 09.03.01 Информатика и вычислительная техника
Профиль: Информатика и вычислительная техника

Квалификация (степень) выпускника - «бакалавр»

Форма обучения – очная

Владикавказ, 2019

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.01 Информатика и вычислительная техника, утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 г. № 929, учебным планом подготовки бакалавриата по направлению подготовки 09.03.01 Информатика и вычислительная техника, утвержденным Ученым советом ФГБОУ ВО «СОГУ» от 28.05.2019 г. № 10.

Составитель: доц.Джусоева

Рабочая программа обсуждена и утверждена на заседании кафедры алгебра и геометрии.
(протокол №7 от14.03.2019)

Одобрена советом факультета математики и информационных технологий
(протокол №5 от 29.03.19)

1. Структура и общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 2 зачётные единицы. (72 час.).

	Очная Форма обучения
Курс	2
Семестр	3
Лекции	32
Практические занятия	34
Лабораторные занятия	-
Консультации	-
Итого аудиторных занятий	66
Самостоятельная работа	51
Курсовая работа	-
Зачет	-
Экзамен	27
Общее количество часов	72 час.

2. Цели освоения дисциплины

- Целью дисциплины является формирование у студентов понятий, знаний и компетенций, позволяющих использовать теоретико-числовые методы для анализа задач, возникающих в теории защиты информации, кодировании, криптографии.

3. Место дисциплины в структуре ОПОП:

Дисциплина «Теория чисел и криптография» относится к дисциплинам Блок 1. Дисциплины (модули). Часть, формируемая участниками образовательных отношений. Б1.В.11.

Для изучения дисциплины необходимы знания, полученные обучающимися в рамках школьного курса « Алгебра и начала анализа», а также в результате освоения дисциплины «Алгебра», «Математический анализ», изучаемых на первом курсе.

Приступая к изучению дисциплины «Теория чисел и криптография», студент должен иметь представление об основах теории делимости, многочленах и их свойствах, о показательной и логарифмической функциях

4. Требования к результатам освоения дисциплины

Компетенции обучающегося, формируемые в результате освоения дисциплины.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями (результатами освоения образовательной программы):

УК-1 -Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

ПК-6 -Способен создавать и исследовать новые математические модели в промышленности и бизнесе, в том числе с использованием современных информационных технологий и программирования.

Взаимосвязь планируемых результатов обучения по дисциплине с формируемыми компетенциями ОПОП:

Компетенции	Планируемые результаты обучения, соответствующие

Код	Формулировка	формируемым компетенциям ОПОП		
		Знать:	Уметь	Владеть:
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Формулировки основных теорем алгебры и аналитической геометрии из предшествующих дисциплин; 2 Основные математические понятия(целые числа, натуральные числа, основы теории делимости)	УК-1.1 находить корни многочленов высоких степеней, находить каноническое разложение числа;; решать текстовые задачи на делимость;.	УК-1.1 Навыками самостоятельного разбора теорем, навыками применения свойств различных функций и их свойств в решении задач и уравнений . Навыками нахождения корней многочленов высоких степеней, канонического разложение числа;;
		УК-1.2 Элементы теории множеств ,виды отображений . каноническое разложение числа ; основные теоретико – числовые функции мультипликативные функции; понятие множества классов вычетов ,	УК-1.2 Находить теоретико-числовые функции от натуральных чисел, составлять таблицу простых чисел ,не превосходящих заданного n, .	УК-1.2 Навыками применения теоретико – числовых функций в решении задач повышенной сложности. навыками построения и исследования различных систем вычетов, определения типа системы вычетов
		УК-1.3 Основы теории конечных структур- групп, колец и полей.	УК-1.3 Проблема генерации больших простых чисел и её важность в современных прикладных	УК1.3 Навыками и умениями решать различные прикладные и теоретические задачи теоретико - числовыми методами,

			задачах. Основные методы криптографии	навыками определять круг задач, которые могут быть решены с помощью сравнений и их свойств.
ПК-6	Способен создавать и исследовать новые математические модели в промышленности и бизнесе, в том числе с использованием современных информационных технологий и программирования	ПК-6.1 Простые числа специального вида. Числа Мерсена ,Люка,числа –близнецы.	ПК-6.1 разлагать многочлены на множители над различными полями,доказывать неразложимость на множители в кольце целых чисел.	ПК-6.1 навыками применения теоретико-числовых методов для решения различных прикладных задач;
		ПК-6.2 сравнения и их свойства; Теоремы Эйлера и Ферма, теорема Вильсона, квадратич-ные вычеты ,	ПК6-2 уметь решать сравнения с одним неизвестным различными методами	ПК-6.2: Навыками разложения рациональных и иррациональных чисел в цепные дроби
		ПК 6-3 Китайскую теорему об остатках, диофантовы уравнения символы Лежандра и Якоби, квадратичный закон взаимности индексы.	ПК 6-3 Решать системы сравнений по разным модулям, неопределённые уравнения первой степени.	ПК-3 Навыками сведения различных практических задач к диофантовым уравнениям, к системам сравнений, применять свойства символа Лежандра для решения сравнений.

При проведении учебных занятий обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание

дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

5. Содержание и учебно-методическая карта дисциплины

Номер недели	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия			Самостоятельная работа студентов		Формы контроля	Баллы		Литература
		л	пр	лаб	Содержание	Часы		min	max	
1-2	Основы теории делимости Нахождение НОК и НОД. Алгоритм Евклида. Простые числа. Решето Эратосфена.	4	4	-	.Решение задач на делимость методом матиндукции	5	Устный опрос, доклад; решение задач			**[1-4]**
3-4	Мультипликативные функции. Основные теоретико- числовые функции.	4	4	-	Простые числа специального вида. Числа Мерсена, числаЛюка. Числа близнецы	5	Устный опрос, доклад; решение задач	**…**	**…**	**…[1-4]**
5-6	Системы вычетов, полная и приведенная. Сравнения ,свойства	4	4		.Решение уравнений высших степеней. Решение уравнений в конечных полях	10	Устный опрос, доклад; решение задач			**[1-4]**
7-8	Теоремы Эйлера и Ферма. Решение сравнений с одним неизвестным. Цепные дроби .	4	4		Приближение действительных чисел рациональными	5	Устный опрос, доклад; решение задач	**0**	**25**	**[1-4]**
9-10	Методы решений сравнений n-ой степени. Теорема Вильсона .	4	4		Методы решений сравнений	5	Контрольная работа	**0**	**25**	**[1-4]**
11-12	Диофантовы уравнения Китайская теорема об остатках	4	4		Уравнения Пелля	5	Устный опрос, доклад; решение задач			**[1-4]**

13-14	Символы Лежандра и Якоби. Квадратичный закон взаимности	4	4		р-адические числа	6	Устный опрос, доклад; решение задач			**[5-6]**
15-16	Основные приложения теории чисел	4	4		Система RSA.Основные крип-тографиче-ские протоколы-	10	Устный опрос, доклад; решение задач	**0**	**25**	**[5-6]**
17			2				Контрольная работа	0	**25**	
	ИТОГО	32	34	0		51		**0**	**100**	

Таблица 5.1

Примечания:

– Все виды учебной работы могут проводиться дистанционно на основании локальных нормативных актов.

– В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по индивидуальной траектории в рамках индивидуального рабочего плана, изучение данной дисциплины может осуществляться через индивидуальные консультации преподавателя очно, в часы консультаций, по электронной почте и с использованием платформ дистанционного обучения.

6. Образовательные технологии

В соответствии с государственными образовательными стандартами высшего образования реализация учебного процесса должна предусматривать проведение занятий в интерактивных и активных формах. Внедрение этих форм обучения – одно из важнейших направлений совершенствования подготовки студентов в современном вузе. Цель – повышение эффективности образовательного процесса, достижение всеми обучающимися высоких результатов обучения.

Интерактивные формы проведения занятий предполагают обучение в сотрудничестве. Все участники образовательного процесса (преподаватель и студенты) взаимодействуют друг с другом, обмениваются информацией, совместно решают проблемы, моделируют ситуации. Суть использования активных и интерактивных форм проведения состоит в погружении студентов в реальную атмосферу делового сотрудничества по разрешению проблем, оптимальную для выработки навыков и качеств будущего специалиста.

Для решения воспитательных и учебных задач преподавателем могут быть использованы следующие формы обучения.

Традиционные лекции и практические (семинарские) занятия с использованием современных интерактивных технологий.

Лекция-диалог – содержание подается через серию вопросов, на которые студент должен отвечать непосредственно в ходе лекции.

Онлайн-семинар – разновидность веб-конференции, проведение онлайн-встреч или презентаций через Интернет в режиме реального времени. Каждый из участников находится у своего компьютера (средства связи), а связь между ними поддерживается через Интернет посредством загружаемого приложения, установленного на компьютере каждого участника.

Видеоконференция – сеанс видеоконференцсвязи (ВКС) – это технология интерактивного взаимодействия двух и более участников образовательного процесса для обмена информацией в реальном режиме времени.

Видео-лекция – снятая на камеру сокращенная лекция, дополненная фотографиями и схемами, иллюстрирующая подаваемый в лекции материал.

Технология электронного обучения (реализуется при помощи электронной образовательной среды СОГУ при использовании ресурсов ЭБС, при проведении автоматизированного тестирования и т. д.).

Творческое задание составляет содержание (основу) любой интерактивной формы проведения занятия. Выполнение творческих заданий требует от студента воспроизведения полученной ранее информации в форме, определяемой преподавателем и требующей творческого подхода: 1) подборка примеров из практики; 2) подборка материала по определенной проблеме;

Публичная презентация проекта - самый эффективный способ донесения важной информации при публичных выступлениях. Слайд-презентации позволяют эффектно и наглядно представить содержание, выделить и проиллюстрировать сообщение.

Интерактивная лекция представляет собой выступление преподавателя перед аудиторий студентов с применением следующих интерактивных форм обучения: 1. управляемая дискуссия или беседа; 2. демонстрация слайдов или учебных фильмов; 3. мозговой штурм; 4. мотивационная речь и др.

Разработка проекта позволяет участникам мысленно выйти за пределы аудитории и составить проект своих действий по обсуждаемому вопросу Участники могут обратиться за консультацией, дополнительной литературой в специализированные учреждения, библиотеки и т.д.

7. Учебно-методическое обеспечение самостоятельной работы

Самостоятельная работа обучающихся является одним из видов учебных занятий. Самостоятельная работа проводится с целью:

− систематизации и закрепления полученных теоретических знаний и практических умений обучающихся студентов;

− углубления и расширения теоретических знаний;

− формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;

- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

− развития исследовательских умений.

К видам самостоятельной работы при изучении данной дисциплины относится: написание докладов, эссе, подготовка презентаций, самостоятельное изучение литературы по теме и составление по ней конспектов, работа со справочными материалами (терминологическими и иными словарями, энциклопедиями) и т.д.

Темы и формы внеаудиторной самостоятельной работы, ее трудоёмкость содержатся в разделе 5, табл. 5.1.

Методические рекомендации по дисциплине прилагаются.

8. Оценочные средства для текущего контроля успеваемости, рубежной аттестации и промежуточной аттестации по итогам освоения дисциплины

Основными формами текущего контроля по дисциплине являются устный опрос на практическом занятии, доклад по теме, вынесенной на самостоятельное изучение, решение задач на практических занятиях.

Форма рубежного контроля: контрольная работа.

Формы промежуточной аттестации: зачётв конце 3 семестра

Студенты, набравшие в ходе текущего и рубежного контроля 56–100 баллов, автоматически получают «Зачет» или соответствующую шкале экзаменационную оценку. Результирующая оценка рассчитывается по согласно действующей бально-рейтинговой системе

Контрольные задания (демоверсии) для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерный вариант контрольной работы (3 семестр, 1 рубеж)

1)Найти НОД(241,315).
Найти НОД(143,225).

2)Найти НОД(275,209).
Найти НОК [273,143].

3)Найти σ(957).
Найти σ(988).

4)Найти τ(257).
Найти τ(988).

5)Найти φ(957).
Найти φ(988).

6) Доказать, что если (a,b)=5, то (5a+3b, 13a+8b) =5

7)разложить в цепную дробь числа$\sqrt{5}$, $\frac{19}{3}$

Примерный вариант контрольной работы (3 семестр, 2 рубеж)

1)Являются ли данные числа (-7,15,16,17, 11, -9,-8)полной системой вычетов по модулю 7?
Являются ли данные числа (-14,-13,9,10, 4,5,20)полной системой вычетов по модулю 7?

2) Является ли число 281 простым.
Является ли число 631 простым.

3)Чему равен символ Лежандра $(\frac{3}{5})$.
Чему равен символ Лежандра $(\frac{81}{5})$.

4) вычислить последние две цифры 2^{101}

5) Решить сравнения: а))12+27x ≡ 18(mod 5) , 11-12x ≡ 9(mod7)

6) решить диофантово уравнение 5x+3y=14

Вопросы для подготовки к зачёту:

…1Делимость в кольце целых чисел. Свойства делимости целых чисел.
3. Наибольший общий делитель. Свойства НОД.
4. Алгоритм Евклида.
5. Наибольший общий делитель его линейное представление.
6. Наименьшее общее кратное. Связь между НОД и НОК. Свойства НОК.
7. Взаимно простые числа и их свойства.
8. Простые числа и их свойства.
9. Основная теорема арифметики.
10. Распределение простых чисел. Теорема Евклида.
11. Решето Эратосфена.
12. Мультипликативные функции
13. Число и сумма делителей.
14. Функция Эйлера.
15. Конечные цепные дроби. Представление рациональных чисел цепными дробями.
17. Бесконечные цепные дроби. Представление действительных чисел бесконечными цепными дробями.
18. Линейные уравнения с двумя неизвестными.
19. Отношение сравнимости. Свойства отношения сравнимости.
20. Классы вычетов. Полная система вычетов по данному модулю. Свойства

21. Классы вычетов. Приведенная система вычетов по данному модулю. Свойства.
22. Теоремы Эйлера и Ферма .
23. Сравнения с одним неизвестным. Равносильные сравнения.
24. Линейные сравнения с одним неизвестным, способы их решения.
25.Неопределённые уравнения первой степени.
25Символ Лежандра. Квадратичный закон взаимности.

8.1. Формы контроля и критерии оценивания

Этап	**Форма контроля**	**Критерии оценивания (процент от максимального кол-ва баллов)**			
		86-100 %	**71–85%**	**56–70%**	**Менее 56%**
		отлично / зачет	**хорошо / зачет**	**удовлетворительно / зачет**	**неудовлетворительно / незачет**
1. Текущий контроль (max 25 баллов за 1 модуль)					
		18–20 баллов	15–17 баллов	11–14 баллов	0–10 баллов
	Оценка текущей работы студента в течение модуля (max 20б.)	Студент активно работает на занятиях, превосходно выполняет все задания преподавателя.	Студент активно работает на занятиях, хорошо выполняет задания преподавателя.	Студент недостаточно активно работает на занятиях, удовлетворительно выполняет задания преподавателя.	Студент недостаточно активно работает на занятиях, неудовлетворительно выполняет задания преподавателя.
		5 баллов	4 балла	3 балла	0 баллов
	Доклад по теме, вынесенной на самостоятельную работу (max 5б.)	Тема полностью раскрыта. Превосходное владение материалом. Высокий уровень самостоятельности, логичности, аргументированности. Превосходный стиль изложения.	Тема в основном раскрыта. Хорошее владение материалом. Средний уровень самостоятельности, логичности, аргументированности. Хороший стиль изложения.	Тема частично раскрыта. Удовлетворительное владение материалом. Низкий уровень самостоятельности, логичности, аргументированности. Удовлетворительный стиль изложения.	Тема не раскрыта. Неудовлетворительное владение материалом. Недостаточный уровень самостоятельности, логичности, аргументированности. Неудовлетворительный стиль изложения.
2. Рубежный контроль (25баллов. за 1 модуль)					
		22–25 баллов	18–21 балл	14–17 баллов	0–13 баллов
	Контрольная работа	Правильно выполнены все задания. Продемонстрирован высокий уровень	Правильно выполнено более 70% заданий. Присутствуют незначительные	Задания выполнены более чем наполовину. Присутствуют серьезные ошибки.	Задания выполнены менее чем наполовину. Продемонстрирован неудовлетворительный

		владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	ошибки. Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий.	Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий.	уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению конкретных заданий.
3. Итоговый контроль по дисциплине (max 50 баллов)					
		43–50 баллов	36–42 балла	28–35 баллов	0–27 баллов
	Устный экзамен/зачет	Дан полный, развернутый ответ на поставленные вопросы. Ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента.	Дан полный ответ на поставленные вопросы, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Но допущены незначительные ошибки, исправленные студентом с помощью «наводящих» вопросов преподавателя.	Дан недостаточно полный ответ. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Речевое оформление требует поправок, коррекции.	Не получены ответы по базовым вопросам дисциплины или дан неполный ответ и допущены грубые ошибки. Речь неграмотная. Уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

.

Показатели и критерии оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Уровень сформированности компетенций			
«Минимальный уровень не достигнут» (менее 56 баллов)	**«Минимальный уровень» (56-70 баллов)**	**«Средний уровень» (71-85 баллов)**	**«Высокий уровень» (86-100 баллов)**
Компетенции не сформированы. Знания отсутствуют, умения и навыки не сформированы.	*Компетенции сформированы.* Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка.	*Компетенции сформированы.* Знания обширные, системные. Умения носят репродуктивный характер, применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	*Компетенции сформированы.* Знания твердые, аргументированные, всесторонние. Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка
Оценка «неудовлетворительно» /не зачтено	**Оценка «удовлетворительно» / «зачтено»**	**Оценка «хорошо» / «зачтено»**	**Оценка «отлично» / «зачтено»**

9. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература

1.Бухштаб, А.А. Теория чисел / А.А. Бухштаб. – Москва : Просвещение, 1966. – 383 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=454831 :– Текст : электронный.

2.Виноградов, И.М. Основы теории чисел : учебник / И.М. Виноградов ; ред. А.Э. Рывкин. – 6-е изд., испр. – Москва ; Ленинград : Государственное издательство технико-теоретической литературы, 1952. – 181 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=449924 – Текст : электронный.

3.Данилова, Т.В. Теория чисел: Задачи с примерами решений / Т.В. Данилова ; Северный (Арктический) федеральный университет им. М. В. Ломоносова. – Архангельск : Северный (Арктический) федеральный университет (САФУ), 2015. – 104 с.– URL: https://biblioclub.ru/index.php?page=book&id=436368 – Библиогр. в кн. – ISBN 978-5-261-01004-3. – Текст : электронный.**:**

4. Сизый, С.В. Лекции по теории чисел : учебное пособие / С.В. Сизый. – 2-е изд., испр. – Москва : Физматлит, 2008. – 191 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=68386). – ISBN 978-5-9221-0741-9. – Текст : электронный.

б) дополнительная литература:

5. Кнауб, Л.В. Теоретико-численные методы в криптографии : учебное пособие / Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов ; Сибирский федеральный университет. – Красноярск : Сибирский федеральный университет (СФУ), 2011. – 160 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=229582 – ISBN 978-5-7638-2113-7. – Текст : электронный.

6. Аграновский, А.В. Практическая криптография: алгоритмы и их программирование : [16+] / А.В. Аграновский, Р.А. Хади. – Москва : СОЛОН-ПРЕСС, 2009. – 256 с. – (Аспекты защиты). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=117663– ISBN 5-98003-002-6. – Текст : электронный.

в) электронные библиотечные системы, с которыми у СОГУ имеется действующий договор, современные профессиональные базы, информационные справочные системы:

– eLIBRARY.RU [Электронный ресурс]: научная электронная библиотека. – URL: http://www.elibrary.ru.

– База данных «ЭБС elibrary»: http://elibrary.ru

– Издательство «Юрайт» [Электронный ресурс]: электронно-библиотечная система. – URL: http://biblio-online.ru.

- Университетская библиотека online [Электронный ресурс]: электронно-библиотечная система. – URL: http://www.biblioclub.ru.

10. Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, обеспеченных компьютерами, имеющими доступ к сети Интернет, интерактивными досками и мультимедийным оборудованием.

Лицензионное программное обеспечение:

1. Windows 10 Pro for Workstations, (№ 4100072800 Microsoft Products (MPSA) от 04.2016г);
2. Office Standard 2016 (№ 4100072800 Microsoft Products (MPSA) от 04.2016г);
3. Система поиска текстовых заимствований «Антиплагиат ВУЗ»;

Перечень ПО в свободном доступе:

1. Kaspersky Free;
2. WinRar;
3. Google Chrome;
4. Yandex Browser;
5. OperaBrowser;

11. Лист обновления/актуализации

11. Лист обновления/актуализации

1. Рабочая программа

пересмотрена и актуализирована на заседании кафедры алгебры и геометрии; протокол №7 от24.03.2020)

одобрена на заседании совета факультета математики и информационных технологий, протокол № 5 от 27.03.2020 г.