МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет математики и компьютерных наук

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Т.А. Хагуров
подпись
«31» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ФТД.01 ЭКСПЕРИМЕНТАЛЬНАЯ ТЕОРИЯ ЧИСЕЛ

Направление подготовки 01.04.01 Математика

Направленность (профиль) Алгебраические методы защиты информации

Форма обучения очная

Квалификация магистр

Краснодар 2024

Рабочая программа дисциплины Экспериментальная теория чисел
составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки
01.04.01 Математика Алгебраические методы защиты информации
код и наименование направления подготовки

Программу составил(и):
А.В. Рожков, профессор, д.ф.-м.н., профессор
И.О. Фамилия, должность, ученая степень, ученое звание

Рабочая программа дисциплины Экспериментальная теория чисел
утверждена на заседании кафедры функционального анализа и алгебры
протокол № 12 «07» мая 2024 г.
Заведующий кафедрой функционального анализа и алгебры
Барсукова В.Ю.

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук протокол № 3 «14» мая 2024 г.

Председатель УМК факультета Шмалько С.П.

Рецензенты:
Ганижева Л.Л. к.т.н., зав. кафедрой наземного транспорта и механики КубГТУ
Лежнев А.В. к.ф.-м.н., зав. кафедрой математических и компьютерных методов КубГУ

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Цель освоения дисциплины – рассматривает задачи информатизации и научного программирования. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

1.2 Задачи дисциплины.

Задачи освоения дисциплины Экспериментальная теория чисел: получение базовых теоретических и практических сведений и навыков о структуре и алгоритмах символьных математических вычислений. Прежде всего алгебраических, связанных с вычислительными и числовыми вопросами алгебры и криптографии. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли вычислительных приемов и методов, при решении вопросов защиты информации. А также при анализе структур информационных систем и математических методов построения защищенных информационных систем.

Изучение теоретических основ предмета: Информационные объекты. Экспериментальная теория чисел и численный анализ. Элементы теории сложности алгоритмов. Числовые функции, основные теоремы о евклидовых кольцах, алгоритмы решения линейных и квадратных уравнений в конечных полях, кольцах вычетов, алгоритмы нахождения наибольших общих делителей, алгоритмов проверки простоты чисел.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина Экспериментальная теория чисел относится к факультативной части учебного плана ФТД.01.

Данная дисциплина, как алгоритмическая основа криптографии, криптоанализа, теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления магистров. А также развитию навыков применения современных компьютерных средств для решения естественно-научных проблем.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ПК-4 Способен ориентироваться в современных алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах	
ПК-4.1 Умеет применять и реализовывать математически сложные алгоритмы в современных программных комплексах ПК-4.2 Применяет в профессиональной деятельности методику исследования и создания новых моделей, методов и технологий в математике и естественных науках ПК-4.3 Демонстрирует умение отбора среди	Знать: об основных задачах и понятиях криптографии; об этапах развития криптографии; о видах информации, подлежащей шифрованию; о классификации шифров; о методах криптографического синтеза и анализа; о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи; о методах криптозащиты компьютерных систем и сетей; Уметь использовать: типовые шифры замены и перестановки; частотные характеристики языков и их использование в криптоанализе; требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем: типовые поточные и блочные шифры, системы шифрования с открытыми ключами, криптографические протоколы;

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
существующих методов наиболее подходящие для решения конкретной прикладной задачи	постановки задач криптоанализа и подходы к их решению; Владеть: криптографической терминологией; навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шифров: навыками математического моделирования в криптографии; современной научно-технической литературой в области криптографической защиты.

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 2 зач. ед. (72 часа), их распределение по видам работ представлено в таблице.

Вид учебной работы		Всего часов	Семестры (часы)			
			1			
Контактная работа, в том числе:						
Аудиторные занятия (всего):		**32**	**32**			
Занятия лекционного типа		16	16	-	-	-
Лабораторные занятия		-	-	-	-	-
Занятия семинарского типа (семинары, практические занятия)		16	16	-	-	-
		-	-	-	-	-
Иная контактная работа:						
Контроль самостоятельной работы (КСР)						
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:		**39.8**	**39.8**			
Курсовая работа		-	-	-	-	-
Проработка учебного (теоретического) материала		6	6	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		19	19	-	-	-
Реферат		4	4	-	-	-
Подготовка к текущему контролю		10,8	10,8	-	-	-
Контроль:						
Подготовка к зачету		-	-			
Общая трудоемкость	**час.**	**72**	**72**	**-**	**-**	**-**
	в том числе контактная работа	**32,2**	**32,2**			
	зач. ед	**2**	**2**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 1 семестре *(очная форма)*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Понятие о компьютерной алгебре. Пакеты компьютерной алгебры. Пакеты на открытом коде.	14	4	4		6
2	Структуры данных в компьютерной алгебре. Техника символьных вычислений.	18	4	4		10
3	LISP-машины. Целочисленная арифметика. Полиномиальная арифметика.	18	4	4		10
4	Редукция алгебраических выражений. Метод критических пар. Алгоритм Евклида. Простые числа. Тесты простоты. Разложение чисел на простые числа.	21,8	4	4		13,8
	Итого по дисциплине:		**16**	**16**		**39,8**

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа магистра

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Понятие о компьютерной алгебре. Пакеты компьютерной алгебры. Пакеты на открытом коде.	Компьютерная алгебра и численный анализ. Точная, целочисленная и полиномиальная арифметики. Системы компьютерной алгебры (СКА). Функциональное назначение. Тип архитектуры. Средства реализации. Область применения. Интегральные оценки качества. Пакеты компьютерной алгебры Maple 2017, PARI/GT 2.9 GAP4r8p8, Sage 8.1. Обзор их возможностей и сравнение функционала	Р
2	Структуры данных в компьютерной алгебре. Техника символьных вычислений.	Базовые структуры данных в Sage Списки (list), динамические массивы. Перечисления (tuples). Словарь или ассоциативный массив (dictionary). Функции и Функции языка Python. Условные операторы, циклы, символьные выражения, алгебраические структуры, матрицы, векторные пространства.	Э
3	LISP-машины. Целочисленная арифметика.	Целочисленная арифметика. Объекты вычислений в целочисленной арифметике – короткие и длинные неотрицательные целые числа. Система счисления	Т

	Полиномиальная арифметика.	(СС) – позиционная, с постоянным основанием. Знак числа и позиция точки (разделителя целой и дробной частей) хранятся и обрабатываются отдельно. Структура данных для представления объектов вычислений в целочисленной.	
4	Редукция алгебраических выражений. Метод критических пар. Алгоритм Евклида. Простые числа. Тесты простоты. Разложение чисел на простые числа.	Редукция алгебраических выражений. Метод локализации. Алгоритм пополнения. Теорема Кнута – Бендикса. Метод критических пар. Метод пополнения. Задача полиномиального упрощения. Редукция полиномов. Базисы Грёбнера. Решение системы полиномиальных уравнений. Алгоритм Бухбергера. Отношение делимости и его свойства.	Р

2.3.2 Занятия практического типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Понятие о компьютерной алгебре. Пакеты компьютерной алгебры. Пакеты на открытом коде.	Расширение состава встроенных и программируемых типов математических объектов. Интеграция СКА с другими компьютерными системами. Унификация и объектная ориентация интерфейса пользователя. Программирование символьных вычислений произвольной сложности. Ускорение работы СКА.	Р
2	Структуры данных в компьютерной алгебре. Техника символьных вычислений.	Структуры данных в GAP. Константы и операторы, Переменные и присваивания, Функции, Списки, Тождественность и равенство списков, Множества, Векторы и матрицы, Записи, Арифметические прогрессии, Использование циклов.	Э
3	LISP-машины. Целочисленная арифметика. Полиномиальная арифметика.	Структура данных для представления объектов вычислений в целочисленной. Язык реализации – C++.Полиномиальная арифметика. Объекты вычислений в полиномиальной арифметике – полиномы степени n (где n – короткое целое число) от одной и нескольких переменных с целочисленными коэффициентами (коэффициенты – длинные целые числа).	Т
4	Редукция алгебраических выражений. Метод критических пар. Алгоритм Евклида.	Алгоритмы вычисления НОД в кольце целых чисел. Алгоритмы вычисления НОД в кольцах полиномов. Бинарный алгоритм вычисления НОД. Расширенный алгоритм Евклида. Расширенный алгоритм Евклида для полиномов над полем.	Р

	Простые числа. Тесты простоты. Разложение чисел на простые числа.	Алгоритм проверки на простоту. Алгоритм тестирования. Тест Эдуарда Люка (1878) – Дерика Генри Лемера (1930). Тест Адлемана- Померанца-Рюмли. Тесты псевдопростоты. Числа Кармайкла.Разложение чисел на простые числа. Метод Адриена Мари Лежандра. Метод Ферма. Метод цепных дробей.	

2.3.3 Занятия семинарского типа.

Не предусмотрены

№	Наименование раздела	Тематика практических занятий (семинаров)	Форма текущего контроля
1	2	3	4
1.			

2.3.4 Лабораторные занятия.

Не предусмотрены

№	Наименование лабораторных работ	Форма текущего контроля
1	3	4
1		
2		

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т).

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Подготовка рефератов и научных сообщений	Рожков А.В. «Темы исследовательских работ и методические указания по их написанию», утвержденные кафедрой функционального анализа и алгебры, протокол № 12 от 7 мая 2024 г.
2	Самостоятельное освоение теории	Рожков А.В. «Перечень электронных источников информации для самостоятельных работ по всему курсу магистерской программы АМЗИ и рекомендации по его использованию». Методические указания, утвержденные кафедрой функционального анализа и алгебры, протокол № 12 от 7 мая 2024.

1. Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

2. Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

3. Методические указания по использованию интерактивных методов обучения. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

4. Методические указания по подготовке эссе, рефератов, курсовых работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол 2№ 9 от 18 мая 2024 г.

5. Методические указания по выполнению лабораторных работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

6. Методические указания по выполнению расчетно-графических заданий. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме с увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

3. Образовательные технологии.

Активные и интерактивные формы, лекции, лабораторные занятия, контрольные работы, реферативные доклады (по некоторым темам в виде презентации) и зачет. В течение семестра магистры решают задачи, указанные преподавателем, к каждому лабораторному занятию. Каждый магистр готовит реферативный доклад по одной из ниже научных тем. Зачет выставляется после выполнения определенного количества (практических и теоретических) заданий контрольных работ и отчета по реферативному докладу. В случае невыполнения какого-то из приведенных требований, магистру для сдачи зачета предлагаются по усмотрению преподавателя некоторые практические и теоретические задания, подобные предложенным ниже.

К образовательным технологиям также относятся интерактивные методы обучения. Интерактивность подачи материала по дисциплине «Базы данных» предполагает не только взаимодействия вида «преподаватель - магистр» и «магистр - преподаватель», но и «магистр - магистр». Все эти виды взаимодействия хорошо достигаются при изложении материала на занятиях в ходе дискуссий, а также на лабораторных занятиях в ходе изложения магистрами реферативных докладов (возможно в виде презентации).

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

4.1 Фонд оценочных средств для проведения текущего контроля.

Список теоретических вопросов (для подготовки к зачету)

1. Константы и операторы в GAP и Sage.
2. Переменные и присваивания.

3. Функции.
4. Списки - тождественность и равенство списков.
5. Множества, Векторы и матрицы.
6. Записи.
7. Использование циклов.
8. Алгоритм пополнения.
9. Теорема Кнута – Бендикса.
10. Метод критических пар.
11. Задача полиномиального упрощения.
12. Базисы Грёбнера. Решение системы полиномиальных уравнений.
13. Алгоритм Бухбергера.
14. Алгоритмы вычисления НОД в кольце целых чисел.
15. Алгоритмы вычисления НОД в кольцах полиномов.
16. Бинарный алгоритм вычисления НОД.
17. Расширенный алгоритм Евклида для полиномов над полем.
18. Алгоритм проверки на простоту.
19. Алгоритм тестирования.
20. Тест Эдуарда Люка – Лемера.
21. Тест Адлемана- Померанца-Рюмли.
22. Тесты псевдопростоты. Числа Кармайкла.
23. Разложение чисел на простые числа.
24. Метод Адриена Мари Лежандра.
25. Метод Ферма.
26. Метод цепных дробей.

4.2 Фонд оценочных средств для проведения промежуточной аттестации. Список типовых алгоритмов (для самостоятельных занятий и зачета)

1. Нахождение примитивного элемента конечного поля.
2. Построение таблицы логарифма Якоби конечного поля.
3. Решение систем линейных уравнений над конечным полем.
4. Алгоритм быстрого возведения в степень.
5. Нахождение обратных элементов в конечном поле.
6. Расширения конечных полей.
7. Алгоритм шифрования AES: структура поля $GF(2^8)$, нахождение обратных элементов.
8. Алгоритм шифрования AES: фактор кольцо $GF(2^8)[\mathrm{x}]/\text{ид}((\mathrm{x}+1)^4)$, преобразование столбцов.
9. Алгоритм шифрования AES: Линейное преобразование, собственные значения матрицы $A=\begin{pmatrix}1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\\1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\end{pmatrix}$.
10. Алгоритм RSA – выбор секретных параметров p,q,d, вычисление открытого ключа n,e.

11. Рюкзачная система шифрования. Быстрорастущий вектор. Сокрытие быстрорастущего вектора после преобразования умножения по модулю.
12. Решение систем линейных уравнений по разным модулям.
13. Решение систем линейных уравнений в кольце целых чисел.
14. Линейный регистр сдвига с обратной связью $S_{n+k} = a_{k-1}S_{n+k-1} + a_{k-2}S_{n+k-2} + ... + a_1S_{n+1} + a_0S_n + a, n = 0,1,2,...$
15. Характеристический многочлен регистра сдвига $x^k = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a_1x + a_0$
16. Нахождение явного вида значений регистра сдвига $S_n = \beta_1\alpha_1{}^n + \beta_2\alpha_2{}^n + ... + \beta_k\alpha_k{}^n, n = 0,1,2,...$, где $\alpha_1, \alpha_2, ..., \alpha_k$ - корни характеристического многочлена, коэффициенты $\beta_1, \beta_2, ..., \beta_k \in P$ являются решениями системы $\begin{cases} \beta_1\alpha_1{}^0 + \beta_2\alpha_2{}^0 + ... + \beta_k\alpha_k{}^0 = S_0 \\ \beta_1\alpha_1{}^1 + \beta_2\alpha_2{}^1 + ... + \beta_k\alpha_k{}^1 = S_1 \\ ... \\ \beta_1\alpha_1{}^{k-1} + \beta_2\alpha_2{}^{k-1} + ... + \beta_k\alpha_k{}^{k-1} = S_{k-1} \end{cases}$.
17. Матрица линейного регистра сдвига
$$A = \begin{pmatrix} 0 & 0 & ... & 0 & 0 & a_0 \\ 1 & 0 & ... & 0 & 0 & a_1 \\ 0 & 1 & ... & 0 & 0 & a_2 \\ 0 & 0 & ... & 0 & 0 & a_3 \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & ... & 0 & 0 & a_{k-3} \\ 0 & 0 & ... & 1 & 0 & a_{k-2} \\ 0 & 0 & ... & 0 & 1 & a_{k-1} \end{pmatrix}$$ ее собственные значения и жорданова форма.
18. Квадратичный закон взаимности. Вычисление квадратичных вычетов и невычетов.
19. Извлечение квадратных корней по простому модулю $p \equiv 3(\mathrm{mod}\,4) \Rightarrow p = 4k + 3$.
20. Извлечение квадратных корней по простому модулю $\mathrm{p} \equiv 1(\mathrm{mod}4) \Rightarrow \mathrm{p}=4\mathrm{k}+1$.

Примерные темы реферативных докладов

1. Расширение состава встроенных и программируемых типов математических объектов.
2. Интеграция СКА с другими компьютерными системами.
3. Унификация и объектная ориентация интерфейса пользователя.
4. Программирование символьных вычислений произвольной сложности.
5. Ускорение работы СКА.
6. LISP-машина.
7. Техника символьных вычислений.
8. Функциональные LISP-выражения.
9. Китайская теорема об остатках и е применение.
10. Примитивные элементы конечных полей.
11. Компьютерная алгебра в криптографии.
12. Алгоритмы быстрого умножения матриц.
13. Рюкзачные алгоритмы.
14. Извлечение квадратных корней в конечных полях.
15. Алгоритм Штрассена.
16. Алгоритм Винограда-Штрассена.

17. Обзор вероятностных алгоритмов разложения на простые множители.

Критерии оценивания результатов обучения

Оценка	Критерии оценивания по экзамену
Высокий уровень «5» (отлично)	оценку «отлично» заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку «хорошо» заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку «удовлетворительно» заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, знает формы допускает незначительные ошибки; студент умеет правильно объяснять материал, иллюстрируя его примерами

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести примеры, довольно ограниченный объем знаний программного материала.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

5.1 Основная литература:

1. Виноградов И.М. Основы теории чисел. 15-е изд. [Электронный ресурс]. - СПб.: Лань, 2023. - URL: https://e.lanbook.com/reader/book/298499
2. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра, 5-е изд. [Электронный ресурс]. - СПб.: Лань, 2024. - URL: https://reader.lanbook.com/book/379334

5.2 Дополнительная литература:

1. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии, 3-е изд. [Электронный ресурс]. - СПб.: Лань, 2024. - https://reader.lanbook.com/book/367010
2. Очков В.Ф., Тихонов А.И. Math CAD и Python: обучение по технологии STEM: Учебное пособие для вузов [Электронный ресурс]. – СПб.: Лань, 2023. – URL: https://e.lanbook.com/reader/book/ 356012

5.3 Периодические издания:

Не предусмотрены

6. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/
2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка (http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование" http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
10. Справочно-информационный портал "Русский язык" http://gramota.ru/;
11. Служба тематических толковых словарей http://www.glossary.ru/;
12. Словари и энциклопедии http://dic.academic.ru/;
13. Образовательный портал "Учеба" http://www.ucheba.com/;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

7. Методические указания для обучающихся по освоению дисциплины (модуля).

Согласно учебному плану дисциплины «Экспериментальная теория чисел» итоговой формой контроля является зачет. Для сдачи зачета магистр должен научиться на лабораторных занятиях решать практические задания по темам разделов 1-3, выполнять домашние задания. Типы практических заданий на зачет соответствуют заданиям. Также на зачете магистрам предлагаются и теоретические задания, состоящие в письменном ответе на один из вопросов. Количество практических и теоретических заданий зависит от активности и результативности работы магистра в течение семестра.

Важнейшим этапом курса является самостоятельная работа по дисциплине (модулю).

Для подготовки к ответам на теоретические вопросы в ходе контрольных работ и на зачете магистрам достаточно использовать материал лекций. Весь этот теоретический материал содержится в учебных пособиях из списка основной литературы. Для изучения теоретического материала, необходимого для подготовки реферативного доклада, кроме основных источников литературы возможно использование дополнительных источников и Интернет-ресурса. В случае затруднений, возникающих у магистров в процессе

самостоятельного изучения теории, преподаватель разъясняет сложные моменты на консультациях.

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

8.1 Перечень информационных технологий.

Базы данных на открытом коде SQL

8.2 Перечень необходимого программного обеспечения.

а) перечень лицензионного программного обеспечения:

№ п/п	Перечень лицензионного программного обеспечения
1.	Microsoft Windows 8, 10
2.	Microsoft Office Professional Plus
3.	Maple 18
4.	MATLAB
5.	Wolfram Mathematica

в) Перечень свободно распространяемого программного обеспечения

№	Перечень свободно распространяемого программного обеспечения
1.	Пакет компьютерной алгебры Sage 8.3. Официальный сайт http://sagemath.org/
2.	Пакет компьютерной алгебры Gap4r9p3. Официальный сайт http://www.gap-system.org/
3.	Пакет компьютерной алгебры PARI/GT 2.11. Официальный сайт http://pari.math.u-bordeaux.fr/
4.	Библиотека для работы с большими целыми числами GMP 6.1.2. Официальный сайт https://gmplib.org/
5.	Язык программирования Python. Официальный сайт https://www.python.org/
6.	Язык программирования Julia. Официальный сайт http://julialang.org/
7.	Язык программирования Cython. Официальный сайт http://cython.org/
8.	Компилятор PyPy, оптимизирующий код Python и Cython. Официальный сайт http://pypy.org/
9.	Python в облаке, интегрированная среда разработки Anaconda. Официальный сайт https://store.continuum.io/cshop/anaconda/
10.	Математические пакеты Python, проект SciPy. Официальный сайт http://www.scipy.org/
11.	Клиентская ОС Debian 9.5. Официальный сайт https://www.debian.org/index.ru.html
12.	Издательская система LaTeX/MiKTeX 2.9. Официальный сайт http://www.miktex.org/
13.	Утилиты Руссиновича https://technet.microsoft.com/ru-ru/library/bb545021.aspx
14.	Анализ защищенности сети Kali Linux 2018.3. https://www.kali.org/
15.	Анализ защищенности сети Snort 3.0. Официальный сайт https://www.snort.org/
16.	Серверная ОС CentOS – 7. Официальный сайт https://www.centos.org/

17.	Офисная система Apache OpenOffice 4.1.5. Официальный сайт https://www.openoffice.org/ru/

8.3 Перечень информационных справочных систем:

1. Справочно-правовая система «Консультант Плюс» (http://www.consultant.ru)
2. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)/
3. Электронная библиотека http://gen.lib.rus.ec/

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю).

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) Программы, демонстрации видео материалов (проигрыватель «Windows Media Player»). Программы для демонстрации и создания презентаций («Microsoft Power Point»).
2.	Семинарские занятия	Не предусмотрены
3.	Лабораторные занятия	Лаборатория, укомплектованная специализированной мебелью и техническими средствами обучения – компьютерами
4.	Курсовое проектирование	Не предусмотрено
5.	Групповые (индивидуальные) консультации	Аудитория для групповых занятий
6.	Текущий контроль, промежуточная аттестация	Аудитория для групповых занятий
7.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.

РЕЦЕНЗИЯ

на фонд оценочных средств дисциплины
ЭКСПЕРИМЕНТАЛЬНАЯ ТЕОРИЯ ЧИСЕЛ

Направление подготовки 01.04.01 Математика
Направленность Алгебраические методы защиты информации

Фонд оценочных средств дисциплины Экспериментальная теория чисел для магистров направленность «Алгебраические методы защиты информации» составлена доктором физико-математических наук, профессором кафедры функционального анализа и алгебры факультета математики и компьютерных наук Кубанского государственного университета Рожковым А.В.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования (ФГОС ВО) по направлению подготовки 01.04.01 Математика. Программа одобрена на заседании кафедры функционального анализа и алгебры и на заседании учебно-методического совета факультета математики и компьютерных наук.

Освоившие программу дисциплины Экспериментальная теория чисел смогут: Определять структуры данных в компьютерной алгебре. Использовать технику символьных вычислений. Применять основные математические методы, используемые в анализе типовых криптографических алгоритмов, ориентироваться в типовых архитектурах вычислительных процессов; использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений.

Фонд оценочных средств дисциплины Экспериментальная теория чисел для магистров направленность «Алгебраические методы защиты информации» сочетает теоретическую и практические части. Получение базовых практических сведений и навыков о структуре и алгоритмах символьных математических вычислений.

Считаю, что фонд оценочных средств дисциплины Экспериментальная теория чисел для магистров направленность «Алгебраические методы защиты информации» может быть рекомендована для подготовки магистров направления подготовки 01.04.01 Математика.

Кандидат физ.-мат. наук,
заведующий кафедрой математических
и компьютерных методов ФГБОУ ВО «КубГУ» М.И. Дроботенко