

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

подпись

Хагуров Т.А.

«27» мая 2022 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДВ.01.01 АЛГОРИТМИЧЕСКИЕ ПРОБЛЕМЫ АЛГЕБРЫ**

Направление подготовки 01.04.01 Математика

Направленность (профиль) Алгебраические методы защиты информации

Форма обучения Очная

Квалификация Магистр

Краснодар 2022

Рабочая программа дисциплины Алгоритмические проблемы алгебры составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 01.04.01 Математика

Программу составил(и):
А.В. Рожков, профессор, д.ф.-м.н., профессор



Рабочая программа дисциплины Алгоритмические проблемы алгебры утверждена на заседании кафедры функционального анализа и алгебры протокол № 9 «13» апреля 2022 г.

Заведующий кафедрой функционального анализа и алгебры

Барсукова В.Ю.
фамилия, инициалы


_____ подпись

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук протокол № 5 «05» мая 2022 г.

Председатель УМК факультета Шмалько С.П.



Рецензенты:

Ганижева Л.Л. к.т.н., доцент кафедры наземного транспорта и механики КубГТУ

Лазарев В.А. д.п.н., профессор кафедры теории функций 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 «Алгоритмические проблемы алгебры»: 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. Компьютерная алгебра 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 «алгоритмические проблемы алгебры» относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана и является дисциплиной по выбору Б1.В.ДВ.01.01.

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-1 Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики	
ПК-1.1 Знает основные понятия, идеи и методы фундаментальных математических дисциплин для решения базовых задач ПК-1.2 Умеет передавать результаты проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области ПК-1.3 Самостоятельно и корректно решает стандартные задачи фундаментальной и прикладной математики ПК-1.4 Имеет навыки решения математических задач, соответствующих квалификации, возникающих при проведении научных и прикладных исследований	Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа Уметь: Применять основные математические методы, используемые в анализе типовых алгоритмов Владеть навыками: использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений.

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	
<p>ПК-4.1 Умеет применять и реализовывать математически сложные алгоритмы в современных программных комплексах</p> <p>ПК-4.2 Применяет в профессиональной деятельности методику исследования и создания новых моделей, методов и технологий в математике и естественных науках</p> <p>ПК-4.3 Демонстрирует умение отбора среди существующих методов наиболее подходящие для решения конкретной прикладной задачи</p>	<p>Знать:</p> <p>О компьютерной реализации информационных объектов.</p> <p>Связи компьютерной алгебры и численного анализа.</p> <p>Элементы теории сложности алгоритмов.</p> <p>Уметь:</p> <p>Определять структуры данных в компьютерной алгебре.</p> <p>Использовать технику символьных вычислений.</p> <p>Применять основные математические методы, используемые в анализе типовых криптографических алгоритмов.</p> <p>Владеть навыками:</p> <p>классификации систем компьютерной алгебры;</p> <p>ориентироваться в типовых архитектурах вычислительных процессов;</p> <p>использования библиотеки алгоритмов и пакетов расширения;</p>

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)			
		2			
Контактная работа, в том числе:					
Аудиторные занятия (всего):	26	26			
Занятия лекционного типа	12	12	-	-	-
Лабораторные занятия	14	14	-	-	-
Занятия семинарского типа (семинары, практические занятия)			-	-	-
Иная контактная работа:					
Контроль самостоятельной работы (КСР)					
Промежуточная аттестация (ИКР)	0,2	0,2			
Самостоятельная работа, в том числе:	45.8	45.8			
Курсовая работа	-	-	-	-	-
Проработка учебного (теоретического) материала	12	12	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)	9	9	-	-	-
Реферат	8	8	-	-	-
Подготовка к текущему контролю	16,8	16,8	-	-	-

Контроль:						
Подготовка к зачету		-	-			
Общая трудоемкость	час.	72	72	-	-	-
	в том числе контактная работа	26,2	26,2			
	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	
1	2	3	4	5	6	7
1	Понятие о компьютерной алгебре. Пакеты компьютерной алгебры. Пакеты на открытом коде.		4		4	10
2	Редукция алгебраических выражений. Метод критических пар. Алгоритм Евклида. Простые числа. Тесты простоты. Разложение чисел на простые числа.		2		4	10
3	Целочисленная арифметика. Полиномиальная арифметика. Китайская теорема об остатках. Мультипликативные группы конечных полей.		2		2	10
4	Дискретное преобразование Фурье. Быстрое преобразование Фурье. Сложность умножения двух многочленов. Умножение матриц. Метод Штрассена.		4		4	15,8
Итого по дисциплине:			12		14	45,8

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 алгебры. Пакеты компьютерной алгебры. Пакеты на открытом коде.	Компьютерная алгебра и численный анализ. Точная, целочисленная и полиномиальная арифметики. Системы компьютерной алгебры. Функциональное назначение. Тип архитектуры. Средства реализации. Область применения.	Р

2	Редукция алгебраических выражений. Метод критических пар. Алгоритм Евклида. Простые числа. Тесты простоты. Разложение чисел на простые числа.	Структуры данных в GAP. Константы и операторы, Переменные и присваивания, Функции, Списки, Тожественность и равенство списков, Множества, Векторы и матрицы.	Э
3	Целочисленная арифметика. Полиномиальная арифметика. Китайская теорема об остатках. Мультипликативные группы конечных полей.	LISP-машина. Техника символьных вычислений. Функциональные LISP-выражения, LISP-функции для выражений, LISP-константы истинности, LISP-функции для списков, LISP-предикаты, LISP-конструкторы функций, LISP-функции вывода результатов.	Т
4	Дискретное преобразование Фурье. Быстрое преобразование Фурье. Сложность умножения двух многочленов. Умножение матриц. Метод Штрассена.	Редукция алгебраических выражений. Метод локализации. Алгоритм пополнения. Теорема Кнута – Бендикса. Метод критических пар. Метод пополнения. Задача полиномиального упрощения. Редукция полиномов. Базисы Грёбнера.	Р

2.3.1 Занятия лабораторного 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. 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	Редукция алгебраических выражений. Метод критических пар. Алгоритм Евклида. Простые числа. Тесты простоты. Разложение чисел на простые числа.	Структуры данных в GAP. Константы и операторы, Переменные и присваивания, Функции, Списки, Тожественность и равенство списков, Множества, Векторы и матрицы, Записи, Арифметические прогрессии, Использование циклов.	Э
3	Целочисленная арифметика. Поли-	LISP-машина. Техника символьных вычислений. Функциональные LISP-выражения, LISP-функции для выражений, LISP-константы истинности, LISP-	Т

	номиальная арифметика. Китайская теорема об остатках. Мультипликативные группы конечных полей.	функции для списков, LISP-предикаты, LISP-конструкторы функций, LISP-функции вывода результатов. Общая схема вычисления выражения. Внутреннее представление математического выражения в системе символьных вычислений – синтаксическое дерево (список списков).	
4	Дискретное преобразование Фурье. Быстрое преобразование Фурье. Сложность умножения двух многочленов. Умножение матриц. Метод Штрассена.	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. 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

2.3.2 Занятия семинарского типа.

Не предусмотрены

2.3.3 Практические занятия.

Не предусмотрены

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 № 9 от 13 апреля 2022 г.
2	Самостоятельное освоение теории	Рожков А.В. «Алгебра и теория чисел. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 13 апреля 2022 г..

1. Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

2. Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

3. Методические указания по использованию интерактивных методов обучения. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5т от 05 мая 2022 г.

4. Методические указания по подготовке эссе, рефератов, курсовых работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5т от 05 мая 2022 г.

5. Методические указания по выполнению лабораторных работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

6. Методические указания по выполнению расчетно-графических заданий. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 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 «Алгоритмические проблемы алгебры» 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 $GF(2^8)[x]/\text{id}((x+1)^4)$, 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

$$S_{n+k} = a_{k-1}S_{n+k-1} + a_{k-2}S_{n+k-2} + \dots + a_1S_{n+1} + a_0S_n + a, n = 0, 1, 2, \dots$$
15. Характеристический многочлен регистра сдвига $x^k = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_1x + a_0$
16. Нахождение явного вида значений регистра сдвига

$$S_n = \beta_1\alpha_1^n + \beta_2\alpha_2^n + \dots + \beta_k\alpha_k^n, n = 0, 1, 2, \dots$$
, где $\alpha_1, \alpha_2, \dots, \alpha_k$ - корни характеристического многочлена, коэффициенты $\beta_1, \beta_2, \dots, \beta_k \in P$ являются решениями системы

$$\begin{cases} \beta_1\alpha_1^0 + \beta_2\alpha_2^0 + \dots + \beta_k\alpha_k^0 = S_0 \\ \beta_1\alpha_1^1 + \beta_2\alpha_2^1 + \dots + \beta_k\alpha_k^1 = S_1 \\ \dots \\ \beta_1\alpha_1^{k-1} + \beta_2\alpha_2^{k-1} + \dots + \beta_k\alpha_k^{k-1} = S_{k-1} \end{cases}$$
17. Матрица линейного регистра сдвига
ее собственные значения и жорданова форма.
18. Квадратичный закон взаимности. Вычисление квадратичных вычетов и невычетов.
19. Извлечение квадратных корней по простому модулю $p \equiv 3 \pmod{4} \Rightarrow p = 4k + 3$.
20. Извлечение квадратных корней по простому модулю $p \equiv 1 \pmod{4} \Rightarrow p = 4k + 1$.

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 ее 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

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. Шевелев Ю.П. Дискретная математика [Электронный ресурс]. – СПб.: Лань, 2021. – URL: <https://e.lanbook.com/reader/book/161638/>
2. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра, 4-е изд. [Электронный ресурс]. - СПб.: Лань, 2022. - URL: <https://reader.lanbook.com/book/187793>

5.2 Дополнительная литература:

1. Ерусалимский Я.М. Дискретная математика. Теория и практикум [Электронный ресурс]. – СПб.: Лань, 2021. – URL: <https://e.lanbook.com/reader/book/169172>
2. Тропин М.П. Основы прикладной алгебры, 2-е изд. [Электронный ресурс]. - СПб.: Лань, 2020. - URL: <https://e.lanbook.com/reader/book/139282/>

5.3 Периодические издания:

Не предусмотрены

5.3. 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.uceba.com/>;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы
http://xn--273--84d1f.xn--plai/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 «Алгоритмические проблемы алгебры» 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.

Вычисления в пакетах компьютерной алгебры на открытом коде GAP4.9.1 и Sage 8.2

8.2 Перечень необходимого программного обеспечения.

а) перечень лицензионного программного обеспечения:

№	Перечень лицензионного программного обеспечения
1.	Maple Soft Maple 18
2.	Mathcad 3
3.	Mathcad 14
4.	Microsoft office
5.	MS Windows 10 (x64)
6.	MS Office 2013, MS

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, специально оборудованная мультимедийными демонстрационными комплексами, учебной мебелью
2	Семинарские занятия	Специальное помещение, оснащенное учебной мебелью, презентационной техникой (проектор, экран, ноутбук) и соответствующим программным обеспечением (ПО).
3	Лабораторные занятия	Помещение для проведения лабораторных занятий оснащенное учебной мебелью, доской, маркером или мелом
4	Групповые (индивидуальные) консультации	Помещение для проведения групповых (индивидуальных) консультаций, учебной мебелью, доской, маркером или мелом
5	Текущий контроль, промежуточная аттестация	Помещение для проведения текущей и промежуточной аттестации, оснащенное учебной мебелью.
6	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 рабочую программу дисциплины

АЛГОРИТМИЧЕСКИЕ ПРОБЛЕМЫ АЛГЕБРЫ

Направление подготовки 01.04.01 Математика

Направленность Алгебраические методы защиты информации

Рабочая программа дисциплины Алгоритмические проблемы алгебры 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.

Суть рабочей программы – это Изучение теоретических основ предмета: Информационные объекты. Компьютерная алгебра 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

Рабочая программа дисциплины Алгоритмические проблемы алгебры для магистров направленность «Алгебраические методы защиты информации» сочетает теоретическую и практические части, что способствует более глубокому усвоению материала. Предложенные задания научно-исследовательского плана направлены на развитие практических навыков решения задач по направлению защита информации.

Считаю, что рабочая программа дисциплины Алгоритмические проблемы алгебры для магистров направленность «Алгебраические методы защиты информации» может быть рекомендована для подготовки магистров направления подготовки 01.04.01 Математика.

Кандидат технических наук,
доцент кафедры наземного транспорта и механики
ФГБОУ ВО «КубГТУ»



Л.Л. Ганижева

