

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

Хазуров Т.А.

«29» мая 2020 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.05 АЛГЕБРАИЧЕСКАЯ АЛГОРИТМИКА**

Направление подготовки 01.04.01 Математика

Направленность (профиль) Алгебраические методы защиты информации

Форма обучения Очная

Квалификация Магистр

Краснодар 2020

Рабочая программа дисциплины Алгебраическая алгоритмика 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 Алгебраическая алгоритмика утверждена на заседании кафедры функционального анализа и алгебры, протокол № 9 «12» апреля 2019 г.

Заведующий кафедрой Барсукова В.Ю.



Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук
протокол № 2 от «24»_апреля 2019 г.

Председатель УМК факультета Титов Г.Н.



Рецензенты:

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

Дроботенко М.И. к.ф.-м.н., зав. кафедрой математических и компьютерных методов КубГУ

Рабочая программа дисциплины Алгебраическая алгоритмика 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 Алгебраическая алгоритмика утверждена на заседании кафедры функционального анализа и алгебры, протокол № 9 «10» апреля 2020 г.

Заведующий кафедрой Барсукова В.Ю. _____

Рабочая программа обсуждена на заседании кафедры функционального анализа и алгебры, протокол № 9 «10» апреля 2020 г.

Заведующий кафедрой Барсукова В.Ю. _____

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук
протокол № 2 от «30» апреля 2020 г.

Председатель УМК факультет Шмалько С.П. _____

Рецензенты:

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

Дроботенко М.И. 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.

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.

1.2 Задачи дисциплины.

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 «алгебраическая алгоритмика» относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана Б1.В.04.

Алгебраической алгоритмике предшествует алгебра и теория алгоритмов. 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.

Изучение данной учебной дисциплины направлено на формирование у обучающихся общекультурных/общепрофессиональных/профессиональных компетенций (ОК/ОПК/ПК)

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1.	ПК-1	Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики	Основные теоремы алгебры, теории чисел и других разделов теоретической математики	Применять стандартные алгоритмы фундаментальной и прикладной математики	Методами анализа математических Моделей, возникающих в области информационных технологий и защиты информации
2.	ПК-4	Способностью к применению методов	О компьютерной реализации	Применять основные математическ	использования библиотеки алгоритмов и пакетов

№ п.п.	Индекс компет енции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
		математического и алгоритмического о моделирования при решении теоретических и прикладных задач	информацион ных объектов. Связи компьютерно й алгебры и численного анализа.	ие методы, используемые в анализе типовых алгоритмов.	расширения; поиска и использования современной научно- технической литературой в области символьных вычислений.

В результате освоения данной дисциплины обучающийся должен:

Знать:

О компьютерной реализации информационных объектов.

Связи компьютерной алгебры и численного анализа.

Элементы теории сложности алгоритмов.

Уметь:

Определять структуры данных в компьютерной алгебре.

Использовать технику символьных вычислений.

Применять основные математические методы, используемые в анализе типовых криптографических алгоритмов.

Владеть навыками:

классификации систем компьютерной алгебры;

ориентироваться в типовых архитектурах вычислительных процессов;

использования библиотеки алгоритмов и пакетов расширения;

поиска и использования современной научно-технической литературой в области символьных вычислений.

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
(для магистров ОФО).

Вид учебной работы	Всего часов	Семестры (часы)			
		3			
Контактная работа, в том числе:					
Аудиторные занятия (всего):	22	22			
Занятия лекционного типа	10	10	-	-	-
Лабораторные занятия	-	-	-	-	-
Занятия семинарского типа (семинары, практические занятия)	12	12	-	-	-
	-	-	-	-	-
Иная контактная работа:					
Контроль самостоятельной работы (КСР)					
Промежуточная аттестация (ИКР)	0,2	0,2			
Самостоятельная работа, в том числе:					
Курсовая работа	-	-	-	-	-
Проработка учебного (теоретического) материала	14	14	-	-	-

Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		12	12	-	-	-
Реферат		12	12	-	-	-
Подготовка к текущему контролю		11,8	11,8	-	-	-
Контроль:						
Подготовка к зачету		-	-			
Общая трудоемкость	час.	72	72	-	-	-
	в том числе контактная работа	22,2	22,2			
	зач. ед	2	2			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 11 семестре (очная форма)

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	
1	2	3	4	5	6	7
1	Присваивание. Последовательность. Цикл. Альтернатива. Рекурсия. Быстрый алгоритм возведения в степень. Работа с матрицами.	21,8	4	4		13,8
2	Арифметика целых чисел. Работа с большими числами. Наибольший общий делитель. Алгоритмы факторизации.	18	2	4		12
3	Евклидовы кольца. Неприводимые многочлены. Конечные кольца.	16	2	2		12
4	Китайская теорема об остатках. Вычисления в кольцах вычетов. Функция Эйлера. Дискретное преобразование Фурье.	16	2	2		12
	Итого по дисциплине:	22	10	12		49,8

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	Присваивание. Последовательность. Цикл. Альтернатива	Структура данных для представления объектов вычислений в целочисленной. Язык реализации – C++. Полиномиальная арифметика	Р
2	Арифметика целых чисел. Работа с большими числами	Расширение состава встроенных и программируемых типов математических объектов. Интеграция СКА с другими	Э

		компьютерными системами. Унификация и объектная ориентация интерфейса пользователя.	
3	Наибольший общий делитель. Алгоритмы факторизации	Алгоритм проверки на простоту. Алгоритм тестирования. Тест Эдуарда Люка (1878) – Дерики Генри Лемера (1930). Тест Адлемана-Померанца-Рюмли.	Т
4	Китайская теорема об остатках. Вычисления в кольцах вычетов	Тесты псевдопростоты. Числа Кармайкла. Разложение чисел на простые числа. Метод Адриена Мари Лежандра. Метод Ферма. Метод цепных дробей.	Р
5	Дискретное преобразование Фурье.	Алгоритмы вычисления НОД в кольцах полиномов. Бинарный алгоритм вычисления НОД. Расширенный алгоритм Евклида. Расширенный алгоритм Евклида для полиномов над полем.	Т

2.3.2 Занятия семинарского типа.

Не предусмотрены

2.3.3 Лабораторные занятия.

№	Наименование лабораторных работ	Форма текущего контроля
1	3	4
1	Пакеты компьютерной алгебры на открытом коде.	ЛР
2	Алгоритмы факторизации целых чисел.	РГЗ
3	Редукция алгебраических выражений. Метод локализации. Алгоритм пополнения.	Отчет по лабораторной работе
4	Базисы Грёбнера. Решение системы полиномиальных уравнений.	РГЗ

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 10.04.2020 г.
2	Самостоятельное решение задач	Рожков А.В. «Алгебраические методы криптографии. Методические указания», утвержденные кафедрой

		функционального анализа и алгебры, протокол № 9 от 10.04.2020 г.
3	Самостоятельное освоение теории	Рожков А.В. «Алгебра и теория чисел. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 10.04.2020 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,

Перечень

электронных документов, которые могут быть представлены
в печатной форме с увеличенным шрифтом

1. Рожков А.В. «Темы исследовательских работ и методические указания по их написанию», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017 г.
2. Рожков А.В. «Алгебраические методы криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017.
3. Рожков А.В. «Алгебра и теория чисел. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017 г.

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 «Алгебраическая алгоритмика» 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 самостоятельных работ)

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. Задача полиномиального упрощения.
10. Базисы Грёбнера. Решение системы полиномиальных уравнений.
11. Алгоритм Бухбергера.
12. Алгоритмы вычисления НОД в кольце целых чисел.
13. Алгоритмы вычисления НОД в кольцах полиномов.
14. Бинарный алгоритм вычисления НОД.
15. Расширенный алгоритм Евклида для полиномов над полем.
16. Алгоритм проверки на простоту.
17. Алгоритм тестирования.
18. Тест Эдуарда Люка – Лемера.
19. Тест Адлемана- Померанца-Рюмли.
20. Тесты псевдопростоты. Числа Кармайкла.
21. Разложение чисел на простые числа.
22. Метод Ферма.
23. 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 RSA – выбор секретных параметров p, q, d , вычисление открытого ключа n, e .
9. Рюкзачная система шифрования. Быстрорастущий вектор. Скрытие быстрорастущего вектора после преобразования умножения по модулю.
10. Решение систем линейных уравнений по разным модулям.
11. Решение систем линейных уравнений в кольце целых чисел.
12. Линейный регистр сдвига с обратной связью
$$S_{n+k} = a_{k-1}S_{n+k-1} + a_{k-2}S_{n+k-2} + \dots + a_1S_{n+1} + a_0S_n + a, n = 0, 1, 2, \dots$$

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

5.1 Основная литература:

1. Шевелев Ю.П. Дискретная математика, 4-е изд. [Электронный ресурс]. – СПб.: Лань, 2019. – URL: <https://e.lanbook.com/reader/book/118616>

2. Ерусалимский Я.М. Дискретная математика. Теория и практикум [Электронный ресурс]. – СПб.: Лань, 2018. – URL: <https://e.lanbook.com/reader/book/106869>

5.2 Дополнительная литература:

1. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра, 3-е изд. [Электронный ресурс]. - СПб.: Лань, 2020. - URL: <https://e.lanbook.com/reader/book/126718/>
2. Кожухов С.Ф., Совертков П.И. Сборник задач по дискретной математике, 2-е изд. [Электронный ресурс]. – СПб.: Лань, 2018. – URL: <https://e.lanbook.com/reader/book/102606/>
3. Окулов С.М. Основы программирования, 10-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2020. - URL: <https://e.lanbook.com/reader/book/135560>

5.3 Периодические издания:

Не предусмотрены

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

1. Пакет компьютерной алгебры Sage 9.1. Официальный сайт <http://sagemath.org/>
2. Пакет компьютерной алгебры Gap4r11p0. Официальный сайт <http://www.gap-system.org/>
3. Пакет компьютерной алгебры PARI/GT 2.13. Официальный сайт <http://pari.math.u-bordeaux.fr/>

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

Согласно учебному плану дисциплины «Алгебраическая алгоритмика» 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 GAP4.11.0 и Sage 9.1

8.2 Перечень необходимого программного обеспечения.

а) перечень лицензионного программного обеспечения:

№	Перечень лицензионного программного обеспечения
1.	Maple Soft Maple 18
2.	Mathcad 14
3.	Microsoft office
4.	MS Windows 10 (x64)
5.	MS Office 2013, MS
6.	Office 2010, 7Zip

в) Перечень свободно распространяемого программного обеспечения

№	Перечень свободно распространяемого программного обеспечения
1.	Пакет компьютерной алгебры Sage 9.1. Официальный сайт http://sagemath.org/
2.	Пакет компьютерной алгебры Gap4r11p0. Официальный сайт http://www.gap-system.org/
3.	Пакет компьютерной алгебры PARI/GT 2.13. Официальный сайт http://pari.math.u-bordeaux.fr/
4.	Библиотека для работы с большими целыми числами GMP 6.2.0. 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 10.4. 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 2020.2. 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)

РЕЦЕНЗИЯ

на рабочую программу дисциплины

АЛГЕБРАИЧЕСКАЯ АЛГОРИТМИКА

Направление подготовки 01.04.01 Математика

Направленность Алгебраические методы защиты информации

Рабочая программа дисциплины Алгебраическая алгоритмика 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.

Содержание рабочей программы – это изучение теоретических основ Алгебраической алгоритмики. 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 Алгебраическая алгоритмика 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 Алгебраическая алгоритмика 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