

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



Жагуров Т.А.

подпись

«29» мая 2020 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ  
Б1.В.ДВ.04.01 КОМПЬЮТЕРНАЯ АЛГЕБРА И  
КРИПТОГРАФИЯ**

Направление подготовки 02.03.01 Математика и компьютерные науки

Направленность (профиль) Алгебра, теория чисел и дискретный анализ

Форма обучения очная

Квалификация бакалавр

Краснодар 2020

Рабочая программа дисциплины Компьютерная алгебра и криптография составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 02.03.01 Математика и компьютерные науки

Программу составил(и):

А.В. Рожков, профессор, д.ф.-м.н., профессор \_\_\_\_\_

Рабочая программа дисциплины Компьютерная алгебра и криптография утверждена на заседании кафедры функционального анализа и алгебры протокол № 9 от «10» апреля 2020 г.

Заведующий кафедрой (разработчика) Барсукова В.Ю. \_\_\_\_\_

Рабочая программа обсуждена на заседании кафедры функционального анализа и алгебры

протокол № 9 от «10» апреля 2020 г.

Заведующий кафедрой (выпускающей) Барсукова В.Ю. \_\_\_\_\_

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук

протокол № 2 от «30» апреля 2020 г.

Председатель УМК факультета 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 защиты информации. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

### **1.2 Задачи дисциплины.**

Задачи освоения дисциплины «Компьютерная алгебра и криптография»: получение базовых теоретических и исторических сведений о структуре и алгоритмах функционирования криптоалгоритмов. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли защиты информации в структуре информатизации и математических методов построения защищенных информационных систем.

Изучение теоретических основ предмета и получение сведений:

- о нормативных требованиях по административно-правовому регулированию в области криптографической защиты информации;
- 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.

### **1.3 Место дисциплины (модуля) в структуре образовательной программы.**

Дисциплина «Компьютерная алгебра и криптография» относится к части, формируемой участниками образовательных отношений блока Б1 и является дисциплиной по выбору.

Данная дисциплина, как математическая основа теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления студентов.

### **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 компетенций

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1.	ПК-1	Способен продемонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий	О компьютерной реализации информационных объектов. Связи компьютерной ал-	Определять структуры данных в компьютерной алгебре. использовать технику символьных вычислений.	навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шифров:

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
2.	ПК-5	Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования	гебры и численного анализа. Элементы теории сложности алгоритмов. об основных задачах и понятиях криптографии об этапах развития криптографии	требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем.	навыками математического моделирования в криптографии; современной научно-технической литературой в области криптографической защиты..

В результате освоения данной дисциплины обучающийся должен:

*Знать:*

О компьютерной реализации информационных объектов.

Связи компьютерной алгебры и численного анализа.

Элементы теории сложности алгоритмов.

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:*

Определять структуры данных в компьютерной алгебре.

использовать технику символьных вычислений.

требования к шифрам и основные характеристики шифров;

принципы построения современных шифрсистем:

типовые поточные и блочные шифры, системы шифрования с открытыми ключами, криптографические протоколы;

постановки задач криптоанализа и подходы к их решению;

основные математические методы, используемые в анализе типовых криптографических алгоритмов.

*Владеть:*

классификации систем компьютерной алгебры;

ориентироваться в типовых архитектурах вычислительных процессов;

использования библиотеки алгоритмов и пакетов расширения;

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 3 зач. ед. (108 часа), их распределение по видам работ представлено в таблице.

Вид учебной работы		Всего часов	Семестры (часы)			
			6			
<b>Контактная работа, в том числе:</b>						
<b>Аудиторные занятия (всего):</b>		<b>68</b>	<b>68</b>			
Занятия лекционного типа		34	34	-	-	-
Лабораторные занятия		34	34	-	-	-
Занятия семинарского типа (семинары, практические занятия)				-	-	-
		-	-	-	-	-
<b>Иная контактная работа:</b>						
Контроль самостоятельной работы (КСР)		11	11			
Промежуточная аттестация (ИКР)		0,2	0,2			
Курсовая работа		7	7	-	-	-
<b>Самостоятельная работа, в том числе:</b>						
Проработка учебного (теоретического) материала		5	5	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		5	5	-	-	-
Реферат				-	-	-
Подготовка к текущему контролю		2,8	2,8	-	-	-
<b>Контроль:</b>						
Подготовка к зачету		-	-			
<b>Общая трудоёмкость</b>	<b>час.</b>	<b>108</b>	<b>108</b>	<b>-</b>	<b>-</b>	<b>-</b>
	<b>в том числе контактная работа</b>	<b>79,2</b>	<b>79,2</b>			
	<b>зач. ед</b>	<b>3</b>	<b>3</b>			

## 2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоёмкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 6 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.	24	8		8	8
2	Структуры данных в компьютерной алгебре. Техника символьных вычислений.	22	8		8	6
3	Модели шифров. Блочные и поточные шифры. Понятие криптосистемы.	26	8		10	8
4	Поточные шифры. Синхронизированные и самосинхронизирующиеся. Надежность шифров.	24,8	10		8	6,8
	<b>Итого по дисциплине:</b>		<b>34</b>		<b>34</b>	<b>28,8</b>

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

## 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 арифметика. 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. 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.	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. 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.	Р
3	Модели шифров. Блочные и поточные шифры. Понятие криптосистемы.	Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки. Одноалфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены. Стандартные алгоритмы криптографической защиты данных.	Э

4	Поточные шифры. Синхронизированные и самосинхронизирующиеся. Надежность шифров.	Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы. Криптографическая стойкость шифров. Ненадежность ключей и сообщений. Совершенные шифры. Характеризация совершенных шифров с минимальным числом ключей. Безусловно стойкие и вычислительно стойкие шифры.	Р
---	---------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---

### 2.3.2 Занятия семинарского типа.

Не предусмотрены

### 2.3.3 Лабораторные занятия.

№	Наименование лабораторных работ	Форма текущего контроля
1	3	4
1	Интегральные оценки качества. Пакеты компьютерной алгебры Maple 2017, PARI/GT 2.9, GAP4r8p8, Sage 8.1. Обзор их возможностей и сравнение функционала.	Р
2	Расширение состава встроенных и программируемых типов математических объектов. Интеграция СКА с другими компьютерными системами. Унификация и объектная ориентация интерфейса пользователя	Р
3	Базовые структуры данных в Sage Списки (list), динамические массивы. Перечисления (tuples). Словарь или ассоциативный массив (dictionary). Функции и Функции языка Python.	Э
4	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.	Р
5	Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты.	Р
6	Криптоанализ шифров перестановки. Одно алфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены.	Э
7	Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы.	Р
8	Криптографическая стойкость шифров. Ненадежность ключей и сообщений.	Р

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. Курсовые работы

Темы курсовых работ

1. Освоение процессов зашифрования и расшифрования для простейших шифров.
2. Свойства простейших шифров.
3. Расчет мощности ключевой системы различных шифров.
4. Оценка расстояния единственности для простейших шифров.
5. Криптоанализ шифра Виженера.
6. Расчет характеристик метода перебора ключей.
7. Вычисление характеристик двоичных функций.
8. Анализ схемы DES при небольшом числе итераций.
9. Вычисление характеристик датчиков псевдослучайных чисел.
10. Применение тестов на простоту целых чисел.
11. Изучение свойств алгоритма RSA.
12. Анализ некоторых алгоритмов выработки хэш-функций.
13. Методы и средства хранения ключевой информации
14. Протоколы аутентификации PAP и CHAP.
15. Система аутентификации и авторизации Kerberos.

### 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 апреля 2020 г.
2	Самостоятельное освоение теории	Рожков А.В. «Комментарии к лекциям по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 10 апреля 2020 г.
3	Решение задач	Рожков А.В. «Решebник типовых задач по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 10 апреля 2020 г.
4	Решение задач	Рожков А.В. «Алгебраические методы криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 10 апреля 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 № 9 от 10 апреля 2020 г.
2. Рожков А.В. «Комментарии к лекциям по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 10 апреля 2020 г.
3. Рожков А.В. «Решебник типовых задач по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 10 апреля 2020 г.
4. Рожков А.В. «Алгебраические методы криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 10 апреля 2020 г.

### 3. Образовательные технологии.

Активные и интерактивные формы, лекции, контрольные работы, реферативные доклады (по некоторым темам в виде презентации) и зачет. В течение семестра студенты решают задачи, указанные преподавателем, к каждому лабораторному занятию. Каждый студент 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, студенту 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 «Компьютерная алгебра и криптография» предполагает не только взаимодействия вида «преподаватель - студент» и «студент - преподаватель», но и «студент - студент». Все эти виды взаимодействия хорошо достигаются при изложении материала на занятиях в ходе дискуссий, а также на лабораторных занятиях в ходе изложения студентами реферативных докладов (возможно в виде презентации).

Се- местр	Вид за- нятия	Используемые интерактивные образовательные техноло- гии	Коли- че- ство часов
6	Лабора- торные занятия	Тема Разновидности шифров перестановки: маршрутные, вер- тикальные перестановки, решетки и лабиринты	2
		Тема . Криптоанализ шифров перестановки.	2
		Тема Одно алфавитные и многоалфавитные замены.	2
		Тема Вычисления средствами системы GAP4.	2
	Лабора- торные занятия	Дискуссия на тему: «.Вопросы криптоанализа простейших шифров замены... с докладами-презентациями	2
		Круглый стол на тему: «Разложение АТ-групп в прямое произ- ведение. и.» с докладами-презентациями	2
		Стандартные алгоритмы криптографической защиты данных.	2
		Компьютерная симуляция: Нерешенные проблемы. Варианты обобщения конструкции.	2
<i>Итого:</i>			16

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций со студентом при помощи электронной информационно-образовательной среды ВУЗа.

#### **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. Защита персональных данных.
11. История криптографии; классические шифры, шифры гаммирования.
12. Принципы построения криптографических алгоритмов.
13. Различие между программными и аппаратными реализациями шифров.
14. Функция Эйлера и Мебиуса.
15. Группы обратимых элементов в кольцах.
16. Структура мультипликативной группы кольца вычетов.
17. Обратимые элементы.
18. Примитивные элементы.
19. Особенности использования вычислительной техники в криптографии вопросы организации сетей засекреченной связи.
20. Криптографические хеш-функции.
21. Электронная подпись.
22. Криптографические протоколы.
23. Предмет и задачи программно-аппаратной защиты информации.
24. Идентификация субъекта, понятие протокола идентификации.
25. Пароли и ключи, организация хранения ключей.

##### **4.2 Фонд оценочных средств для проведения промежуточной аттестации.**

Список типовых алгоритмов (для самостоятельных и лабораторных занятий)

1. Применения и разработки шифровальных средств.
2. Применения электронной подписи.
3. Криптографические методы обеспечения информационной безопасности.
4. Алгоритмы проверки на простоту.
5. Эллиптические кривые над конечными полями
6. Алгоритмы вычисления в конечных полях.
7. Электронная подпись по схеме Эль Гамала.
8. Электронная подпись на основе RSA.
9. Случайные и псевдослучайные гаммы.
10. Регистры сдвига с обратной связью.
11. Схема Файстеля.
12. Подсчет количества точек на эллиптической кривой.
13. Операция сложения на эллиптической кривой.
14. Схема алгоритма RSA.
15. Криптограммы, полученные при повторном использовании ключа.

16. Нахождение примитивного элемента конечного поля.
17. Построение таблицы логарифма Якоби конечного поля.
18. Решение систем линейных уравнений над конечным полем.
19. Алгоритм быстрого возведения в степень.
20. Нахождение обратных элементов в конечном поле.
21. Расширения конечных полей.
22. Алгоритм шифрования AES: структура поля  $GF(2^8)$ , нахождение обратных элементов.
23. Алгоритм шифрования AES: фактор кольца  $GF(2^8)[x]/\text{ид}((x+1)^4)$ , преобразование столбцов.
24. Алгоритм шифрования AES: Линейное преобразование, собственные значения матрицы.
25. Алгоритм RSA – выбор секретных параметров  $p, q, d$ , вычисление открытого ключа  $n, e$ .
26. Рюкзачная система шифрования. Быстрорастущий вектор. Соккрытие быстрорастущего вектора после преобразования умножения по модулю.
27. Решение систем линейных уравнений по разным модулям.
28. Решение систем линейных уравнений в кольце целых чисел.
29. Линейный регистр сдвига с обратной связью
 
$$S_{n+k} = a_{k-1}S_{n+k-1} + a_{k-2}S_{n+k-2} + \dots + a_1S_{n+1} + a_0S_n + a, n = 0, 1, 2, \dots$$
30. Характеристический многочлен регистра сдвига  $x^k = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_1x + a_0$
31. Матрица линейного регистра сдвига ее собственные значения и жорданова форма.
32. Квадратичный закон взаимности. Вычисление квадратичных вычетов и невычетов.
33. Извлечение квадратных корней по простому модулю  $p \equiv 3 \pmod{4} \Rightarrow p = 4k + 3$ .
34. Извлечение квадратных корней по простому модулю  $p \equiv 1 \pmod{4} \Rightarrow p = 4k + 1$ .
35. Криптоанализ шифра однобуквенной простой замены.
36. Криптоанализ системы шифрования RSA при неправильном выборе модуля.
37. Вскрытие шифра Вернама при повторном использовании ключа.

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

### 5.1 Основная литература:

1. Мартынов Л.М. Алгебра и теория чисел для криптографии: учебное пособие [Электронный ресурс]. - СПб.: Лань, 2020. - URL: <https://e.lanbook.com/reader/book/140740>
2. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 3-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2015. – URL: <https://e.lanbook.com/reader/book/70724/>

### 5.2. Дополнительная литература:

1. Столов Е.Л. Цифровая обработка сигналов. Водяные знаки в аудиофайлах [Электронный ресурс]. - СПб.: Лань, 2018. - URL: <https://e.lanbook.com/reader/book/106736/>
2. Аверченков В.И., Рытов М.Ю., Шпичак С.А. Криптографические методы защиты информации: учебное пособие, 2-е изд. [Электронный ресурс]. – М.: ФЛИНТА, 2017 - URL: <https://e.lanbook.com/book/92914>.

### 1.3. Периодические издания:

Не предусмотрены

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

Не предусмотрены

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

Согласно учебному плану дисциплины «Компьютерная алгебра и криптография» итоговой формой контроля является зачет. Для сдачи зачета студент 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 студентам предлагаются и теоретические задания, состоящие в письменном ответе на один из вопросов. Количество практических и теоретических заданий зависит от активности и результативности работы студента 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 студентам 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 студентов 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.**

**8.2 Перечень необходимого программного обеспечения.**

**а) перечень лицензионного программного обеспечения:**

№	Перечень лицензионного программного обеспечения
1.	Maple Soft Maple 18
2.	Mathcad Prime3
3.	Mathcad 14
4.	Microsoft office
5.	MS Windows 10 (x64)
6.	MS Office 2013, MS
7.	Office 2010, 7Zip

**в) Перечень свободно распространяемого программного обеспечения**

№	Перечень свободно распространяемого программного обеспечения
1.	Пакет компьютерной алгебры Sage 8.2. Официальный сайт <a href="http://sagemath.org/">http://sagemath.org/</a>
2.	Пакет компьютерной алгебры Gap4r9p1. Официальный сайт <a href="http://www.gap-system.org/">http://www.gap-system.org/</a>
3.	Пакет компьютерной алгебры PARI/GT 2.9. Официальный сайт <a href="http://pari.math.u-bordeaux.fr/">http://pari.math.u-bordeaux.fr/</a>
4.	Библиотека для работы с большими целыми числами GMP 6.1.2. Официальный сайт <a href="https://gmplib.org/">https://gmplib.org/</a>
5.	Язык программирования Python. Официальный сайт <a href="https://www.python.org/">https://www.python.org/</a>
6.	Язык программирования Julia. Официальный сайт <a href="http://julialang.org/">http://julialang.org/</a>

7.	Язык программирования Cython. Официальный сайт <a href="http://cython.org/">http://cython.org/</a>
8.	Компилятор PyPy, оптимизирующий код Python и Cython. Официальный сайт <a href="http://pypy.org/">http://pypy.org/</a>
9.	Python в облаке, интегрированная среда разработки Anaconda. Официальный сайт <a href="https://store.continuum.io/cshop/anaconda/">https://store.continuum.io/cshop/anaconda/</a>
10.	Математические пакеты Python, проект SciPy. Официальный сайт <a href="http://www.scipy.org/">http://www.scipy.org/</a>
11.	Клиентская ОС Debian 9.4. Официальный сайт <a href="https://www.debian.org/index.ru.html">https://www.debian.org/index.ru.html</a>
12.	Издательская система LaTeX/MiKTeX 2.9. Официальный сайт <a href="http://www.miktex.org/">http://www.miktex.org/</a>
13.	Утилиты Руссиновича <a href="https://technet.microsoft.com/ru-ru/library/bb545021.aspx">https://technet.microsoft.com/ru-ru/library/bb545021.aspx</a>
14.	Анализ защищенности сети Kali Linux 2018.2. <a href="https://www.kali.org/">https://www.kali.org/</a>
15.	Офисная система Apache OpenOffice 4.1.5. Официальный сайт <a href="https://www.openoffice.org/ru/">https://www.openoffice.org/ru/</a>

### 8.3 Перечень информационных справочных систем:

1. <http://www.pravo.gov.ru> – официальный портал правовой информации
2. <http://www.government.ru> - интернет-портал Правительства РФ
3. <http://graph.document.kremlin.ru> - раздел «Документы» портала Президента России
4. <http://minsvyaz.ru/ru> - сайт Минкомсвязи РФ
5. <http://www.rsoc.ru> - сайт Федеральной службы Роскомнадзор
6. <http://www.scrf.gov.ru> – сайт Совета безопасности РФ
7. <http://base.consultant.ru> – сайт правовой информации «Консультант+»
8. <http://www.fstec.ru> – официальный сайт ФСТЭК России
9. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru/>)
10. 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 с предустановленными GAP и Sage 320H, 309 H
4.	Курсовое проектирование	
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 рабочую программу дисциплины **КОМПЬЮТЕРНАЯ АЛГЕБРА И КРИПТОГРАФИЯ**

Направление подготовки 02.03.01 Математика и компьютерные науки  
Направленность Алгебра, теория чисел и дискретный анализ

Рабочая программа дисциплины Компьютерная алгебра и криптография для студентов направленность Алгебра, теория чисел и дискретный анализ 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 02.03.01 Математика и компьютерные науки. Программа одобрена на заседании кафедры функционального анализа и алгебры и на заседании учебно-методического совета факультета математики и компьютерных наук.

Содержание рабочей программы. Изучение теоретических основ предмета и получение сведений: о нормативных требованиях по административно-правовому регулированию в области криптографической защиты информации; 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.

Рабочая программа дисциплины Компьютерная алгебра и криптография для студентов направленность Алгебра, теория чисел и дискретный анализ сочетает теоретическую и практические части. Получение базовых практических сведений и навыков о структуре и алгоритмах символьных математических вычислений.

Считаю, что рабочая программа дисциплины Компьютерная алгебра и криптография для студентов направленность Алгебра, теория чисел и дискретный анализ может быть рекомендована для подготовки студентов направления подготовки 02.03.01 Математика и компьютерные науки.

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

  
М.И. Дроботенко

## РЕЦЕНЗИЯ

на рабочую программу дисциплины

### КОМПЬЮТЕРНАЯ АЛГЕБРА И КРИПТОГРАФИЯ

Направление подготовки 02.03.01 Математика и компьютерные науки  
Направленность Алгебра, теория чисел и дискретный анализ

Рабочая программа дисциплины Компьютерная алгебра и криптография для студентов направленность Алгебра, теория чисел и дискретный анализ 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 02.03.01 Математика и компьютерные науки. Программа одобрена на заседании кафедры функционального анализа и алгебры и на заседании учебно-методического совета факультета математики и компьютерных наук.

Студенты, освоившие дисциплину Компьютерная алгебра и криптография должны 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.

Рабочая программа дисциплины Компьютерная алгебра и криптография для студентов направленность Алгебра, теория чисел и дискретный анализ 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 Компьютерная алгебра и криптография для студентов направленность Алгебра, теория чисел и дискретный анализ может быть рекомендована для подготовки студентов направления подготовки 02.03.01 Математика и компьютерные науки.

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



Л.Л. Ганижева