


Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

**УТВЕРЖДЕНО**  
 решением Ученого совета факультета математики,  
 информационных и авиационных технологий  
 от « 16 » 06 2020 г. протокол № 5/20  
 Председатель / М.А. Волков /  
 (подпись, расшифровка подписи)  
06 2020 г.

### РАБОЧАЯ ПРОГРАММА

Дисциплина	Вычислительные методы в алгебре и теории чисел
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления
Курс	2

Специальность: 10.05.01 «Компьютерная безопасность»  
*код направления (специальности), полное наименование*

Специализация: «Математические методы защиты информации»  
*полное наименование*

Форма обучения: очная  
*очная, заочная, очно-заочная (указать только те, которые реализуются)*

Дата введения в учебный процесс УлГУ: « 01 » 09 2020 г.


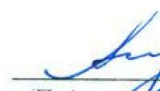
Программа актуализирована на заседании кафедры: протокол №      от      20     г.


Программа актуализирована на заседании кафедры: протокол №      от      20     г.

Программа актуализирована на заседании кафедры: протокол №      от      20     г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Рацеев Сергей Михайлович	ИБиТУ	профессор, д.ф-м.н, доцент

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой, реализующей дисциплину	Заведующий выпускающей кафедрой
 / <u>А.С. Андреев</u> / (Подпись) (Ф.И.О.) « <u>16</u> » <u>06</u> 20 <u>20</u> г.	 / <u>А.С. Андреев</u> / (Подпись) (Ф.И.О.) « <u>16</u> » <u>06</u> 20 <u>20</u> г.

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

## 1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Многие криптографические алгоритмы базируются на результатах классической теории чисел. Поэтому особое внимание в дисциплине уделено изучению этих результатов, находящихся в центре внимания приложений, особенно криптографии.

### Цели освоения дисциплины:

- обеспечение подготовки в одной из важных областей, находящихся на границе теории чисел, информатики и криптографии;
- освоение основных методов разработки алгоритмов для решения задач, возникающих как в самой теории чисел и таких приложениях, как криптография.

### Задачи освоения дисциплины:

- овладение основными вычислительными методами классической и современной теории чисел;
- овладение методами теоретико-числового характера;
- выявление различных приложений теории чисел.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к вариативной части цикла Б1.В образовательной программы и читается в 4-м семестре студентам специальности «Компьютерная безопасность» очной формы обучения.


Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Математический анализ», «Алгебра», «Дискретная математика», «Информатика». Предполагается также знакомство с одним из языков программирования высокого уровня. Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: элементы высшей алгебры, элементы абстрактной алгебры.

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих специальных дисциплин: «Криптографические методы защиты информации», «Криптографические протоколы», «Методы алгебраической геометрии в криптографии», «Теория кодирования, сжатия и восстановления информации», а также для прохождения учебной, производственной и преддипломной практик, государственной итоговой аттестации.

## 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины «Вычислительные методы в алгебре и теории чисел» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОК-8 – способностью к самоорганизации и самообразованию	Знать: основные методы решения алгоритмических проблем, возникающих в теории чисел и в их приложениях к решению практических задач; Уметь: применять изученные математические методы при решении профессиональных задач и задач с практическим содержанием

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		


	<p>нием; Владеть: математическим аппаратом, изученным в данном курсе</p>
ОПК-2 – способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	<p>Знать: основные методы решения алгоритмических проблем, возникающих в теории чисел и в их приложениях к решению практических задач; формировать алгоритмическое мировоззрение, творческое мышление и навыки в проведении самостоятельных научных исследований; Уметь: применять изученные математические методы при решении профессиональных задач и задач с практическим содержанием; Владеть: математическим аппаратом, изученным в данном курсе</p>
ОПК-4 – способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	<p>Знать: основные методы решения алгоритмических проблем, возникающих в теории чисел и в их приложениях к решению практических задач; Уметь: применять изученные математические методы при решении профессиональных задач и задач с практическим содержанием; Владеть: математическим аппаратом, изученным в данном курсе</p>
ПК-4 – способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	<p>Знать: основные методы решения алгоритмических проблем, возникающих в теории чисел и в их приложениях к решению практических задач; Уметь: применять изученные математические методы при решении профессиональных задач и задач с практическим содержанием; Владеть: математическим аппаратом, изученным в данном курсе</p>

#### 4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 3.

4.2. Объем дисциплины по видам учебной работы:

Вид учебной работы	Количество часов (форма обучения - дневная)	
	Всего по плану	В т.ч. по семестрам
		4


Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

Контактная работа обучающихся с преподавателем	48	48	
Аудиторные занятия:			
• Лекции	16	16	
• Практические и семинарские занятия	16	16	
• Лабораторные работы (лабораторный практикум)	16	16	
Самостоятельная работа	60	60	
Всего часов по дисциплине	108	108	
Форма текущего контроля знаний и контроля самостоятельной работы		Лабораторные работы, проверка решения задач	
Курсовая работа			
Виды промежуточной аттестации (экзамен, зачет)		зачет	
Общая трудоемкость в зач. ед.	3	3	

#### 4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы:

Форма обучения \_\_\_\_\_ очная \_\_\_\_\_

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	
<b>Раздел 1. Теория делимости</b>							
1. Разложение по модулю.	16	2	2	4	4	8	Лабораторная работа. Домашние задания
2. Диофантовы уравнения первой степени.	16	2	2	4		8	Лабораторная работа. Домашние задания
3. Простые числа. Факторизация.	12	2	2			8	Домашние задания
4. Цепные дроби.	16	2	2	4	4	8	Лабораторная

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

би.							работа. Домашние задания
5. Бесконечные цепные дроби	8	2	2			4	Домашние задания
6. Мультипликативные функции.	12	2	2			8	Домашние задания
<b>Раздел 2. Сравнения</b>							
7. Сравнения.	16	2	2	4	4	8	Лабораторная работа. Домашние задания
8. Сравнения первой степени.	12	2	2			8	Домашние задания
<b>ВСЕГО</b>	<b>108</b>	<b>16</b>	<b>16</b>	<b>16</b>	<b>12</b>	<b>60</b>	

## 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### Раздел 1. Теория делимости

#### Тема 1. Разложение по модулю.

Теорема о разложении одного целого числа по модулю другого (основная теорема делимости целых чисел).  $q$ -ичные системы счисления (представление и единственность). Отношение делимости в кольце целых чисел и его свойства. Наибольший общий делитель и его свойства. Алгоритм Евклида. Обобщенный алгоритм Евклида. Взаимно простые числа и их свойства.

#### Тема 2. Диофантовы уравнения первой степени.

Линейные диофантовы уравнения первой степени. Критерий существования решения. Формула общего решения. Наименьшее общее кратное и его свойства. Формула для наименьшего общего кратного пары целых чисел.

#### Тема 3. Простые числа. Факторизация.

Простые числа и их свойства. Теорема Евклида. Простейшие проверки целого числа на простоту. Решето Эратосфена. Основная теорема арифметики (о разложении целых чисел в произведение простых). Каноническое разложение целого числа. Формулы для наибольшего общего делителя и для наименьшего общего кратного набора целых чисел на основе их канонических разложений. Факторизация числа  $n!$ .

#### Тема 4. Цепные дроби.

Конечные цепные дроби. Представление рационального числа конечной цепной дробью. Подходящие дроби, их вычисление и основные свойства.


#### Тема 5. Бесконечные цепные дроби.

Бесконечные цепные дроби. Представление действительных чисел бесконечными цепными дробями.

#### Тема 6. Мультипликативные функции.

Мультипликативные функции и их свойства. Примеры мультипликативных функций. Леммы о мультипликативных функциях. Формулы для количества и суммы делителей целого числа. Функция Мебиуса и ее свойства. Функция Эйлера и формула для ее вычисления.

### Раздел 2. Сравнения

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

### Тема 7. Сравнения.

Отношение сравнимости в кольце целых чисел и его свойства. Полная и приведенная системы вычетов и их свойства. Теорема Эйлера. Теорема Ферма (малая).

### Тема 8. Сравнения первой степени.

Сравнения первой степени  $ax \equiv b \pmod{m}$ , случай  $(a, m)=1$ . Сравнения первой степени  $ax \equiv b \pmod{m}$ , случай  $(a, m)>1$ . Системы сравнений первой степени. Системы сравнений первой степени и методы их решения. Китайская теорема об остатках. Схема разделения секрета на основе китайской теоремы об остатках.

## 6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

### Раздел 1. Теория делимости

#### Тема 1. Разложение по модулю (семинар).

$q$ -ичные системы счисления (представление и единственность). Отношение делимости в кольце целых чисел и его свойства. Наибольший общий делитель и его свойства. Алгоритм Евклида. Обобщенный алгоритм Евклида. Взаимно простые числа и их свойства.

#### Тема 2. Диофантовы уравнения первой степени (семинар).

Линейные диофантовы уравнения первой степени. Формула общего решения. Наименьшее общее кратное и его свойства. Формула для наименьшего общего кратного пары целых чисел.

#### Тема 3. Простые числа. Факторизация (семинар).

Простые числа и их свойства. Простейшие проверки целого числа на простоту. Решето Эратосфена. Каноническое разложение целого числа. Формулы для наибольшего общего делителя и для наименьшего общего кратного набора целых чисел на основе их канонических разложений. Факторизация числа  $n!$ .

#### Тема 4. Цепные дроби (семинар).

Конечные цепные дроби. Представление рационального числа конечной цепной дробью. Подходящие дроби, их вычисление.

#### Тема 5. Бесконечные цепные дроби (семинар).

Бесконечные цепные дроби. Представление действительных чисел бесконечными цепными дробями.

#### Тема 6. Мультипликативные функции (семинар).

Мультипликативные функции и их свойства. Примеры мультипликативных функций. Леммы о мультипликативных функциях. Формулы для количества и суммы делителей целого числа. Функция Мебиуса и ее свойства. Функция Эйлера и формула для ее вычисления.

### Раздел 2. Сравнения

#### Тема 7. Сравнения (семинар).


Отношение сравнимости в кольце целых чисел и его свойства. Полная и приведенная системы вычетов и их свойства. Теорема Эйлера. Теорема Ферма (малая).

#### Тема 8. Сравнения первой степени (семинар).

Сравнения первой степени  $ax \equiv b \pmod{m}$ , случай  $(a, m)=1$ . Сравнения первой степени  $ax \equiv b \pmod{m}$ , случай  $(a, m)>1$ . Системы сравнений первой степени. Системы сравнений первой степени и методы их решения. Китайская теорема об остатках. Схема разделения секрета на основе китайской теоремы об остатках.

## 7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Лабораторные работы проводятся в интерактивной форме, а именно, используются: диалоговое обучение, в ходе которого осуществляется взаимодействие между студентом и преподавателем,

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

между самими студентами, группами студентов; элементы деловых игр, «мозговой штурм» или дискуссии по рассматриваемым вопросам.

Полные задания для лабораторных работ приводятся в учебно-методическом пособии:

Аминаров А. В. Лабораторный практикум по математическим методам защиты информации : учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2016. 55 с.

## **Раздел 1. Теория делимости**

### **Тема 1. Разложение по модулю.**

Целью работы является освоение обобщенного алгоритма Евклида.

Задание. Требуется составить программу, которая для любых целых чисел  $a$  и  $b$ , одновременно не равных нулю, находит частное решение уравнения  $ax+by=(a,b)$ .

Методические указания: основное внимание должно быть уделено освоению обобщенного алгоритма Евклида.

### **Тема 2. Диофантовы уравнения первой степени.**

Целью работы является освоение методов решений линейных диофантовых уравнений первой степени вида  $ax+by=c$ .

Задание. Требуется составить программу, которая для любых целых чисел  $a$  и  $b$ , одновременно не равных нулю, находит все решения линейного диофантова уравнения первой степени вида  $ax+by=c$ .

Методические указания: основное внимание должно быть уделено освоению методов решений линейных диофантовых уравнений.

### **Тема 4. Цепные дроби.**

Целью работы является освоение представлений рациональных чисел конечными цепными дробями и представление конечных цепных дробей рациональными числами.

Задание. Требуется составить программу, которая для любых целых чисел  $a$  и  $b$ , причем  $b$  не равно нулю, представляет рациональное число  $a/b$  в виде конечной цепной дроби. И наоборот, представить конечную цепную дробь в виде рационального числа вида  $a/b$ .

Методические указания: основное внимание должно быть уделено освоению методов представлений рациональных чисел конечными цепными дробями.

## **Раздел 2. Сравнения**

### **Тема 7. Сравнения.**

Целью работы является освоение методов решений сравнений первой степени.

Задание. Требуется составить программу, которая для любых целых чисел  $a$ ,  $b$  и  $m$ ,  $m>0$ , находит все решения сравнения  $ax \equiv b \pmod{m}$ .

Методические указания: основное внимание должно быть уделено освоению методов решений сравнений первой степени.

### **Тема 7. Сравнения.**

Целью работы является освоение методов решений систем сравнений первой степени.

Задание. Требуется составить программу, которая находит решение системы сравнений первой степени с помощью китайской теоремы об остатках.


Методические указания: основное внимание должно быть уделено освоению методов решений систем сравнений первой степени.

## **8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ**

Курсовые и контрольные работы не предусмотрены учебным планом дисциплины.

## **9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ**

1. Теорема о делении с остатком.
2.  $q$ -ичные системы счисления (представление и единственность).
3. Отношение делимости в кольце целых чисел и его свойства.


Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

4. Наибольший общий делитель и его свойства.
5. Алгоритм Евклида. Бинарный алгоритм Евклида.
6. Обобщенный алгоритм Евклида.
7. Взаимно простые числа и их свойства.
8. Наименьшее общее кратное и его свойства.
9. Диофантовы уравнения первой степени. Теорема о существовании решения для уравнений вида  $a_1x_1 + \dots + a_nx_n = (a_1, \dots, a_n)$ .
10. Критерий существования решения диофантова уравнения первой степени.
11. Описание всех решений уравнения вида  $ax + by = c$ .
12. Системы диофантовых уравнений первой степени.
13. Простые числа и их свойства.
14. Простейшие проверки целого числа на простоту. Решето Эратосфена.
15. Основная теорема арифметики. Каноническое разложение целого числа.
16. Вычисление н.о.д. и н.о.к. на основе канонического разложения чисел. Нахождение всех делителей целого числа при известном каноническом разложении.
17. Целая часть числа. Каноническое разложение числа  $n!$ .
18. Конечные цепные дроби. Представление рационального числа конечной цепной дробью.
19. Подходящие дроби и их вычисление с помощью рекуррентных последовательностей  $\{P_k\}$  и  $\{Q_k\}$ .
20. Свойства подходящих дробей: разность соседних подходящих дробей, несократимость подходящих дробей.
21. Свойство монотонности последовательностей  $\{P_k\}$  и  $\{Q_k\}$ . Поведение четных и нечетных подходящих дробей.
22. Бесконечные цепные дроби. Сходимость бесконечных цепных дробей.
23. Разложение действительных чисел в цепные дроби.
24. Мультипликативные функции и их свойства. Примеры мультипликативных функций.
25. Леммы о мультипликативных функциях.
26. Формула суммы и числа делителей целого числа.
27. Функция Мебиуса и ее свойства.
28. Функция Эйлера и ее вычисление.
29. Отношение сравнимости в кольце целых чисел и его свойства.
30. Полная система вычетов и ее свойства.
31. Приведенная система вычетов и ее свойства.
32. Теорема Эйлера. Теорема Ферма.
33. Сравнения первой степени  $ax \equiv b \pmod{m}$ . Случай  $(a, m)=1$ .
34. Сравнения первой степени  $ax \equiv b \pmod{m}$ . Случай  $(a, m)>1$ .
35. Системы сравнений 1-й степени и методы их решения. Китайская теорема об остатках.


## 10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1. Разложение по модулю.	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение задач	8	Зачет, проверка лабораторных работ, проверка решения задач
2. Диофантовы уравнения первой степени.	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение задач	8	Зачет, проверка лабораторных работ, проверка решения задач
3. Простые числа.	Проработка учебного материала	8	Зачет, проверка ре-



Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

Факторизация.	ла, подготовка к сдаче зачета, решение задач		шения задач
4. Цепные дроби.	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение задач	8	Зачет, проверка лабораторных работ, проверка решения задач
5. Бесконечные цепные дроби	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение задач	4	Зачет, проверка лабораторных работ, проверка решения задач
6. Мультипликативные функции.	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение задач	8	Зачет, проверка лабораторных работ, проверка решения задач
7. Сравнения.	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение задач	8	Зачет, проверка лабораторных работ, проверка решения задач
8. Сравнения первой степени.	Проработка учебного материала, подготовка к сдаче зачета, решение задач	8	Зачет, проверка решения задач

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

## 11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### а) Список рекомендуемой литературы

1. Курош А.Г. Курс высшей алгебры : учебник для вузов по спец. "Математика". 17-е изд., стер. СПб. : Лань, 2008. 432 с.
2. Семушин И.В. Вычислительные методы алгебры и оценивания : учеб. пособие. Ульяновск : УлГТУ, 2011. 366 с.
3. Рацеев С.М. Математические методы защиты информации : электронный учебный курс / С. М. Рацеев; УлГУ, ФМИАТ. - Ульяновск : УлГУ, 2018. — URL: <http://edu.ulsu.ru/courses/921/interface>

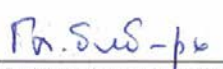
### дополнительная

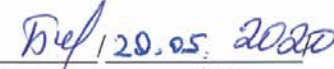
1. Сборник задач по алгебре : учебник для вузов / под ред. А. И. Кострикина. - 3-е изд., испр. и доп. М. : Физматлит, 2001. 464 с.
2. Поднебесова Г.Б. Абстрактная и компьютерная алгебра [Электронный ресурс]: практикум/ Поднебесова Г.Б.— Электрон. текстовые данные.— Челябинск: Южно-Уральский государственный гуманитарно-педагогический университет, 2016.— 125 с.— Режим доступа: <http://www.iprbookshop.ru/83852.html>

### учебно-методическая


1. Аминаров А. В. Лабораторный практикум по математическим методам защиты информации : учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2016. 55 с. - URL: <http://lib.ulsu.ru/MegaPro/Download/MObject/270>
2. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисциплине «Вычислительные методы в алгебре и теории чисел» для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» / С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 180 КБ). - Текст : электронный. Режим доступа: <http://lib.ulsu.ru/MegaPro/Download/MObject/4678>

Согласовано:





должность сотрудника научной библиотеки      ФИО      подпись      дата

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

## б) Программное обеспечение

Для образовательного процесса по данной дисциплине необходим стационарный класс ПК с установленным следующим программным обеспечением:

- операционная среда ОС Windows/Linux;
- системы программирования на языках Си/C++ (Code::Blocks).

## в) Профессиональные базы данных, информационно-справочные системы

### 1. Электронно-библиотечные системы:

1.1. IPRbooks : электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2020]. – URL: <http://www.iprbookshop.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. ЮРАЙТ : электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2020]. - URL: <https://www.biblio-online.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. Консультант студента : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2020]. – URL: [http://www.studentlibrary.ru/catalogue/switch\\_kit/x2019-128.html](http://www.studentlibrary.ru/catalogue/switch_kit/x2019-128.html). – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2020]. – URL: <https://e.lanbook.com>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2020]. - URL: <http://znanium.com>. – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.6. Clinical Collection : коллекция для медицинских университетов, клиник, медицинских библиотек // EBSCOhost : [портал]. – URL: <http://web.a.ebscohost.com/ehost/search/advanced?vid=1&sid=e3ddfb99-a1a7-46dd-a6eb-2185f3e0876a%40sessionmgr4008>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

2. **КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2020].

### 3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2020]. – URL: <https://dlib.eastview.com/browse/udb/12>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2020]. – URL: <http://elibrary.ru>. – Режим доступа : для авториз. пользователей. – Текст : электронный


3.3. «Grebennikon» : электронная библиотека / ИД Гребенников. – Москва, [2020]. – URL: <https://id2.action-media.ru/Personal/Products>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. **Национальная электронная библиотека** : электронная библиотека : федеральная государственная информационная система : сайт / Министерство культуры РФ ; РГБ. – Москва, [2020]. – URL: <https://нэб.рф>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. **SMART Imagebase** // EBSCOhost : [портал]. – URL: <https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741>. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

### 6. Федеральные информационно-образовательные порталы:

6.1. Единое окно доступа к образовательным ресурсам : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://window.edu.ru/>. – Текст : электрон-

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

ный.

6.2. Российское образование : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://www.edu.ru>. – Текст : электронный.

**7. Образовательные ресурсы УлГУ:**


7.1. Электронная библиотека УлГУ : модуль АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: <http://lib.ulsu.ru/MegaPro/Web>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.


7.2. Образовательный портал УлГУ. – URL: <http://edu.ulsu.ru>. – Режим доступа : для зарегистр. пользователей. – Текст : электронный.

Согласовано:

Зам.нач. УИТиТ  
должность сотрудника УИТиТ

/ Клочкова А.В.  
ФИО

 20.05.2020  
подпись дата

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

## 12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещение 3/317. Аудитория для проведения практических и лабораторных занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций с набором демонстрационного оборудования для обеспечения тематических иллюстраций. Помещение укомплектовано ученической доской и комплектом мебели (посадочных мест – 24). Генератор шума для акустического зашумления помещения. Сканирующий радиоприемник AP 3000 А. Широкополосная антенна. Осциллограф АСК 2102. Прибор В6-9 (селективный вольтметр). Генератор НЧ ГЗ-118. Поисковый прибор ST 032 «Пиранья». Имитатор закладных устройств ИМФ-2. Универсальный акустический излучатель к генератору акустического шума OMS-2000. Универсальный электромагнитный излучатель к генератору акустического шума. Генератор электромагнитного зашумления Гром-ЗИ4. Детектор поля D 006. Экран настенный, мультимедийный проектор. Информационные плакаты. Компьютер, Wi-Fi с доступом к сети «Интернет», ЭИОС, ЭБС. 432017, Ульяновская область, г. Ульяновск, ул. Набережная реки Свияги, д. 106 (3 корпус).

Помещение 503. Аудитория для проведения практических и лабораторных занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. Помещение укомплектовано ученической доской и комплектом мебели (посадочных мест – 10). Компьютеры, Wi-Fi с доступом к сети «Интернет», ЭИОС, ЭБС. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106 (1 корпус).

Аудитория -230. Аудитория для самостоятельной работы. Аудитория укомплектована ученической мебелью. 16 персональных компьютеров.

Аудитория -237. Читальный зал научной библиотеки с зоной для самостоятельной работы. Аудитория укомплектована ученической мебелью. Компьютерная техника, телевизор, экран, проектор. Стол для лиц с ОВЗ. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106-1 корпус.

Реализация программы дисциплины требует наличия учебной лаборатории. Оборудование учебной лаборатории: посадочные места по количеству студентов. Технические средства обучения: компьютеры с лицензионным программным обеспечением:

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- системы программирования на языках Си/C++ (Code::Blocks, Visual Studio).

## 13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающимся) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических возможностей:





- для лиц с нарушением зрения: в форме электронного документа, индивидуальные консультации с привлечением тифлосурдопереводчика, индивидуальные задания и консультация;
- для лиц с нарушением слуха: в форме электронного документа, индивидуальные консультации с привлечением сурдопереводчика, индивидуальные задания и консультация;
- для лиц с нарушением опорно-двигательного аппарата: в форме электронного документа, индивидуальные задания и консультация.


Разработчик \_\_\_\_\_

подпись

ФИО

## ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/вы- пускающей кафедрой	Подпись	Дата
1	Внесение изменений в п.п. 4.2 Объем дисциплины по видам учебной работы п. «Общая трудоемкость дисциплины» с оформлением приложения 1	Андреев А.С.		08.04.2020 Протокол заседания кафедры № 12
2	Внесение изменений в п. 13 «Специальные условия для обучающихся с ограниченными возможностями здоровья» с оформлением приложения 2	Андреев А.С.		08.04.2020 Протокол заседания кафедры № 12
3	Внесение изменений в п/п а) Список рекомендуемой литературы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 3	Андреев А.С.		27.05.2020 Протокол заседания кафедры № 14
4	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 4	Андреев А.С.		27.05.2020 Протокол заседания кафедры № 14

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		


## Приложение 1

### 4.2. Объем дисциплины по видам учебной работы:

Вид учебной работы	Количество часов (форма обучения - дневная)		
	Всего по плану	В т.ч. по семестрам	
		4	
Контактная работа обучающихся с преподавателем	48	48/48*	
Аудиторные занятия:			
• Лекции	16	16/16*	
• Практические и семинарские занятия	16	16/16*	
• Лабораторные работы (лабораторный практикум)	16	16/16*	
Самостоятельная работа	60	60	
Всего часов по дисциплине	108	108	
Форма текущего контроля знаний и контроля самостоятельной работы		Лабораторные работы, проверка решения задач	
Курсовая работа			
Виды промежуточной аттестации (экзамен, зачет)		зачет	
Общая трудоемкость в зач. ед.	3	3	

\*Количество часов работы ППС с обучающимися в дистанционном формате с применением электронного обучения

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

## Приложение 2

### 13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:


- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей



Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

## Приложение 3

### 11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

#### а) Список рекомендуемой литературы

1. Курош А.Г. Курс высшей алгебры : учебник для вузов по спец. "Математика". 17-е изд., стер. СПб. : Лань, 2008. 432 с.
2. Семушин И.В. Вычислительные методы алгебры и оценивания : учеб. пособие. Ульяновск : УлГТУ, 2011. 366 с.
3. Рацеев С.М. Математические методы защиты информации : электронный учебный курс / С. М. Рацеев; УлГУ, ФМИАТ. - Ульяновск : УлГУ, 2018. — URL: <http://edu.ulsu.ru/courses/921/interface>




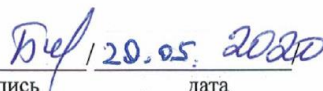
#### дополнительная

1. Сборник задач по алгебре : учебник для вузов / под ред. А. И. Кострикина. - 3-е изд., испр. и доп. М. : Физматлит, 2001. 464 с.
2. Поднебесова Г.Б. Абстрактная и компьютерная алгебра [Электронный ресурс]: практикум/ Поднебесова Г.Б.— Электрон. текстовые данные.— Челябинск: Южно-Уральский государственный гуманитарно-педагогический университет, 2016.— 125 с.— Режим доступа: <http://www.iprbookshop.ru/83852.html>


#### учебно-методическая

1. Аминаров А. В. Лабораторный практикум по математическим методам защиты информации : учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2016. 55 с. - URL: <http://lib.ulsu.ru/MegaPro/Download/MObject/270>
2. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисциплине «Вычислительные методы в алгебре и теории чисел» для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» / С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 180 КБ). - Текст : электронный. Режим доступа: <http://lib.ulsu.ru/MegaPro/Download/MObject/4678>

Согласовано:

должность сотрудника научной библиотеки      ФИО      подпись      дата

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

## Приложение 4

### 11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

#### в) Профессиональные базы данных, информационно-справочные системы

##### 1. Электронно-библиотечные системы:

1.1. IPRbooks : электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2020]. – URL: <http://www.iprbookshop.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. ЮРАЙТ : электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2020]. - URL: <https://www.biblio-online.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. Консультант студента : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2020]. – URL: [http://www.studentlibrary.ru/catalogue/switch\\_kit/x2019-128.html](http://www.studentlibrary.ru/catalogue/switch_kit/x2019-128.html). – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2020]. – URL: <https://e.lanbook.com>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Znanium.com : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2020]. - URL: <http://znanium.com>. – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.6. Clinical Collection : коллекция для медицинских университетов, клиник, медицинских библиотек // EBSCOhost : [портал]. – URL: <http://web.a.ebscohost.com/ehost/search/advanced?vid=1&sid=e3ddfb99-a1a7-46dd-a6eb-2185f3e0876a%40sessionmgr4008>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

2. **КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2020].

##### 3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2020]. – URL: <https://dlib.eastview.com/browse/udb/12>. – Режим доступа : для авториз. пользователей. – Текст : электронный.


3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2020]. – URL: <http://elibrary.ru>. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. «Grebennikon» : электронная библиотека / ИД Гребенников. – Москва, [2020]. – URL: <https://id2.action-media.ru/Personal/Products>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. **Национальная электронная библиотека** : электронная библиотека : федеральная государственная информационная система : сайт / Министерство культуры РФ ; РГБ. – Москва, [2020]. – URL: <https://нэб.рф>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. **SMART Imagebase** // EBSCOhost : [портал]. – URL: <https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741>. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

##### 6. Федеральные информационно-образовательные порталы:

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа дисциплины		

6.1. [Единое окно доступа к образовательным ресурсам](#) : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://window.edu.ru/>. – Текст : электронный.

6.2. [Российское образование](#) : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://www.edu.ru>. – Текст : электронный.

**7. Образовательные ресурсы УлГУ:**


7.1. Электронная библиотека УлГУ : модуль АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: <http://lib.ulsu.ru/MegaPro/Web>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

7.2. Образовательный портал УлГУ. – URL: <http://edu.ulsu.ru>. – Режим доступа : для зарегистр. пользователей. – Текст : электронный.

Согласовано:

Зам.нач. УИТиТ  
должность сотрудника УИТиТ

/ Клочкова А.В.  
ФИО

 20.05.2020  
подпись дата