


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 «21» \_\_\_\_\_ 2019 г., протокол № 5/19

Председатель \_\_\_\_\_ 2019 г.



### РАБОЧАЯ ПРОГРАММА

Дисциплина	Теоретико-числовые методы в криптографии
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления
Курс	3

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 \_\_\_\_\_ 2019 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
 _____ / А.С. Андреев / (Подпись) (Ф.И.О.) « 19 » 06 20 19 г.	 _____ / А.С. Андреев / (Подпись) (Ф.И.О.) « 19 » 06 20 19 г.

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

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

### 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;
- освоение основных методов разработки алгоритмов для решения задач, возникающих как в самой теории чисел и таких приложениях, как криптография;
- выявление различных приложений теории чисел.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к базовой части цикла Б1 образовательной программы и читается в 6-м семестре студентам специальности «Компьютерная безопасность» очной формы обучения.

Для ее успешного изучения необходимы знания и умения, приобретенные в результате освоения курсов «Вычислительные методы в алгебре и теории чисел», «Информатика», а также некоторых разделов дисциплин «Алгебра и геометрия», «Дискретная математика», «Математическая логика и теория алгоритмов» и «Математический анализ». Кроме того, необходимо наличие практических навыков программирования на одном из языков программирования высокого уровня.


Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: вычислительные методы в алгебре и теории чисел, элементы высшей алгебры.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин, как «Криптографические методы защиты информации», «Криптографические протоколы», «Методы алгебраической геометрии в криптографии», а также для прохождения учебной, производственной и преддипломной практик, государственной итоговой аттестации.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-2 – способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории	Знать: алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; Уметь: проводить вычисления в числовых и конечных кольцах и полях с

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

алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ; Владеть: навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.
---	--

#### 4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

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


##### 4.2. Объем дисциплины по видам учебной работы (в часах):

Вид учебной работы	Количество часов (форма обучения: <u>очная</u> )	
	Всего по плану	В т.ч. по семестрам
		6
1	2	3
Контактная работа обучающихся с преподавателем	54	54
Аудиторные занятия		
• Лекции	36	36
• Практические и семинарские занятия		
• Лабораторные работы (лабораторный практикум)	18	18
Самостоятельная работа	54	54
Форма текущего контроля знаний и контроля самостоятельной работы		Лабораторные работы, проверка решения задач
Курсовая работа		
Виды промежуточной аттестации		Зачет
Всего часов по дисциплине	108	108
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			

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

						та	
1	2	3	4	5	6	7	
<b>Раздел 1. Сравнения</b>							
1. Системы линейных диофантовых уравнений	12	6				6	
2. Степенные вычеты	16	6		2	2	8	Лабораторная работа. Проверка решения задач
3. Сравнения второй степени	20	6		4	4	10	Лабораторная работа. Проверка решения задач
<b>Раздел 2. Тесты на простоту. Факторизация. Дискретное логарифмирование</b>							
4. Тесты на простоту	20	6		4	4	10	Лабораторная работа. Проверка решения задач
5. Задача факторизации	20	6		4	4	10	Лабораторная работа. Проверка решения задач
6. Методы дискретного логарифмирования	20	6		4	4	10	Лабораторная работа. Проверка решения задач
Итого:	108	36	0	18	18	54	

## 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### Раздел 1. Сравнения

#### Тема 1. Системы линейных диофантовых уравнений.

Системы линейных диофантовых уравнений. Допустимые преобразования расширенной матрицы. Алгоритм решения систем диофантовых уравнений. Критерий существования решения. Формула общего решения.

#### Тема 2. Степенные вычеты.

Показатель числа. Свойства показателя. Первообразные корни по простому модулю. Первообразные корни по составному модулю. Критерий, описывающий все случаи существования первообразных корней. Индексы (дискретные логарифмы). Свойства индексов.


#### Тема 3. Сравнения второй степени.

Квадратичные вычеты и невычеты. Критерий Эйлера. Символ Лежандра. Свойства символа Лежандра. Критерий Гаусса. Квадратичный закон взаимности Гаусса. Символ Якоби. Свойства символа Якоби. Алгоритм эффективного вычисления символа Лежандра на основе символа Якоби. Вычисление квадратного корня. Алгоритм Тонелли-Шенкса.

### Раздел 2. Тесты на простоту. Факторизация. Дискретное логарифмирование

#### Тема 4. Тесты на простоту.

Тест на простоту на основе малой теоремы Ферма. Псевдопростые числа по заданному основанию. Числа Кармайкла и их свойства. Критерий Корселя. Критерий Эйлера простоты числа. Эйлеровы псевдопростые числа по заданному основанию. Тест на простоту Соловей-Штрассена. Теорема Миллера. Теорема Рабина. Тест на простоту Миллера-Рабина. Генерация простых чисел. N-1 методы доказательства простоты. Метод Поклингтона проверки на простоту. Теорема Лемера. Алгоритм построения простых чисел  $p$  с известным простым де-

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

лителем  $q$  числа  $p-1$ .

### Тема 5. Задача факторизации.

Задача факторизации.  $p$ -метод Полларда.  $(p-1)$ -метод Полларда.

### Тема 6. Методы дискретного логарифмирования.

Метод Гельфонда-Шенкса.  $p$ -метод Полларда. Метод исчисления порядка. Решение систем сравнений, возникающих в методе исчисления порядка.

## 6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Практические и семинарские занятия не предусмотрены учебным планом.

## 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, 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. Сравнения

#### Тема 2. Степенные вычеты.

Цель работы: освоение методов нахождения первообразных корней.

Задание. Требуется составить программу, которая для любого простого числа  $p > 2$  и любого натурального  $n$  находит все первообразные корни по модулю  $p$ ; первообразный корень по модулю  $p^n$ ; первообразный корень по модулю  $2p^n$ .

Входные данные:  $p$  и  $n$ .

Выходные данные: первообразные корни по соответствующим модулям.

Методические указания. Использовать следующий критерий первообразного корня.

Пусть  $a \in \mathbb{Z}$ ,  $m \in \mathbb{N}$ ,  $(a, m) = 1$ ,  $\varphi(m) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$  – каноническое разложение числа  $\varphi(m)$ .

Число  $a$  является первообразным корнем по модулю  $m$  тогда и только тогда, когда

$$a^{\frac{\varphi(m)}{p_i}} \not\equiv 1 \pmod{p_i}, \quad i = 1, \dots, n.$$

#### Тема 3. Сравнения второй степени.

Цель работы: освоение методов вычисления символа Якоби.

Задание. Требуется составить программу, которая для любого целого числа  $a$  и любого нечетного целого  $m > 2$  вычисляет значение символа Якоби  $\left(\frac{a}{m}\right)$ .

Входные данные:  $a$  и  $m$ .


Выходные данные: значение символа Якоби  $\left(\frac{a}{m}\right)$ .

Методические указания. Использовать эффективный алгоритм вычисления символа Лежандра на основе символа Якоби.

#### Тема 3. Сравнения второй степени.

Цель работы: освоение методов вычисления квадратного корня по простому модулю.

Задание. Требуется составить программу, которая для любого целого числа  $a$ , любого не-

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

четного простого числа  $p$ ,  $\left(\frac{a}{p}\right) = 1$ , находит такое  $x$ , что  $x^2 \equiv a \pmod{p}$ .

Входные данные:  $a$  и  $p$ .

Выходные данные: квадратный корень числа  $a$  по модулю  $p$ .

Методические указания. Использовать алгоритм Тонелли-Шенкса.

## Раздел 2. Тесты на простоту. Факторизация. Дискретное логарифмирование

### Тема 4. Тесты на простоту.

Цель работы: освоение методов проверки числа на простоту.

Задание. Требуется составить программу, которая для любого целого числа  $n$  проверяет, является ли оно простым.

Входные данные:  $n$

Выходные данные: Заключение о том, что число составное, либо заключение о том, что число не является составным с некоторой вероятностью.

Варианты заданий.

1. Метод Соловея-Штрассена.

2. Метод Миллера-Рабина.

Методические указания. Использовать тест Соловея-Штрассена или тест Миллера-Рабина.

### Тема 4. Тесты на простоту.

Цель работы: освоение методов генерации простых чисел.

Задание. Требуется составить программу, которая генерирует простые числа.

Входные данные:  $k$  – разрядность простого числа.

Выходные данные:  $k$ -битное простое число.

Методические указания. Использовать алгоритм на основе теста Миллера-Рабина.

### Тема 5. Задача факторизации.

Цель работы: освоение методов факторизации целых чисел.

Задание. Требуется составить программу, которая раскладывает целые числа на множители.

Входные данные:  $n$  – натуральное число.

Выходные данные: разложение числа  $n$  на множители.

Методические указания. Использовать алгоритм  $\rho$ -метода Полларда.

### Тема 6. Методы дискретного логарифмирования.

Цель работы: освоение методов дискретного логарифмирования.

Задание. Требуется составить программу, которая вычисляет дискретный логарифм  $\log_a b$ .

Входные данные:  $a, b$  – натуральные числа,  $p$  – простое.

Выходные данные: дискретный логарифм  $\log_a b$ .

Варианты заданий:

1. Метод Гельфонда-Шенкса.

2.  $\rho$ -метод Полларда.

3. Метод исчисления порядка.


Методические указания: основное внимание должно быть уделено освоению методов факторизации на примере метода Гельфонда-Шенкса,  $\rho$ -метода Полларда, метода исчисления порядка.

## 8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Курсовые и контрольные работы не предусмотрены учебным планом дисциплины.

## 9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ


1. Сравнения произвольной степени по простому модулю.

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

2. Сравнения по составному модулю.
3. Степенные вычеты. Показатель числа. Свойства показателя.
4. Первообразные корни по простому модулю  $p$ .
5. Первообразные корни по модулю  $p^n$ .
6. Первообразные корни по модулю  $2p^n$ .
7. Индексы (дискретные логарифмы), их свойства.
8. Сравнения второй степени. Квадратичный вычет. Критерий Эйлера квадратичного вычета по простому модулю.
9. Квадратичный невычет. Критерий квадратичного невычета по простому модулю.
10. Символ Лежандра и его свойства.
11. Критерий Гаусса и его следствие.
12. Квадратичный закон взаимности Гаусса.
13. Алгоритм вычисления символа Лежандра, использующий факторизацию.
14. Символ Якоби и его свойства.
15. Эффективный алгоритм вычисления символа Лежандра на основе символа Якоби.
16. Алгоритм Тонелли-Шенкса вычисления квадратного корня по простому модулю.
17. Тест на простоту на основе малой теоремы Ферма.
18. Псевдопростые числа по заданному основанию.
19. Числа Кармайкла и их свойства. Критерий Корсельта.
20. Метод Поклингтона проверки на простоту.
21. Критерий Эйлера простоты числа.
22. Эйлеровы псевдопростые числа по заданному основанию.
23. Тест на простоту Соловея-Штрассена.
24. Теорема Миллера. Теорема Рабина. Тест на простоту Миллера-Рабина.
25. Генерация простых чисел.
26. Задача факторизации.  $p$ -метод Полларда.
27. Задача факторизации.  $(p-1)$ -метод Полларда.
28. Методы дискретного логарифмирования. Метод Гельфонла-Шенкса.
29. Методы дискретного логарифмирования. Метод исчисления порядка.


### 10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1. Системы линейных диофантовых уравнений	Проработка учебного материала, подготовка к сдаче зачета, решение задач	6	Зачет, проверка решения задач
2. Степенные вычеты	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение задач	8	Зачет, проверка лабораторных работ, проверка решения задач
3. Сравнения второй степени	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение задач	10	Зачет, проверка лабораторных работ, проверка решения задач
4. Тесты на простоту	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета	10	Зачет, проверка лабораторных работ
5. Задача факторизации	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета	10	Зачет, проверка лабораторных работ, проверка решения

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

			задач
6. Методы дискретного логарифмирования	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение задач	10	Зачет, проверка лабораторных работ, 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

#### основная

1. Основы криптографии : учеб. пособие для вузов по спец. в обл. информ. безопасности / А. П. Алферов [и др.]. М. : Гелиос АРВ, 2001. 479 с.
2. 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. 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>
2. ГОСТ-Эксперт – единая база ГОСТов Российской Федерации для образования и промышленности:
  - 2.1. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012. — URL: <https://gostexpert.ru/gost/gost-34.10-2012>
  - 2.2. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2013. — URL: <https://gostexpert.ru/gost/gost-34.11-2012>

#### 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 «Теоретико-числовые методы в криптографии» 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 : 149 КБ). - Текст : электронный. Режим доступа: <http://lib.ulsu.ru/MegaPro/Download/MObject/4682>

Согласовано:

Гл. биб-ро ИБ УлГУ Полкина И.О 20.05.2019  
 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/ Альт Рабочая станция 8;
- системы программирования на языках Си/C++ (Code::Blocks, Visual Studio).

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

### 1. Электронно-библиотечные системы:

1.1. **IPRbooks** [Электронный ресурс]: электронно-библиотечная система / группа компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов , [2019]. - Режим доступа: <http://www.iprbookshop.ru>.

1.2. **ЮРАЙТ** [Электронный ресурс]: электронно-библиотечная система / ООО Электронное издательство ЮРАЙТ. - Электрон. дан. – Москва , [2019]. - Режим доступа: <https://www.biblio-online.ru>.

1.3. **Консультант студента** [Электронный ресурс]: электронно-библиотечная система / ООО Политехресурс. - Электрон. дан. – Москва, [2019]. - Режим доступа: <http://www.studentlibrary.ru/pages/catalogue.html>.

1.4. **Лань** [Электронный ресурс]: электронно-библиотечная система / ООО ЭБС Лань. - Электрон. дан. – С.-Петербург, [2019]. - Режим доступа: <https://e.lanbook.com>.

1.5. **Znanium.com** [Электронный ресурс]: электронно-библиотечная система / ООО Знаниум. - Электрон. дан. – Москва, [2019]. - Режим доступа: <http://znanium.com>.

2. **КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2019].

3. **База данных периодических изданий** [Электронный ресурс] : электронные журналы / ООО ИВИС. - Электрон. дан. - Москва, [2019]. - Режим доступа: <https://dlib.eastview.com/browse/udb/12>.

4. **Национальная электронная библиотека** [Электронный ресурс]: электронная библиотека. - Электрон. дан. – Москва, [2019]. - Режим доступа: <https://нэб.рф>.

5. **Электронная библиотека диссертаций РГБ** [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2019]. - Режим доступа: <https://dvs.rsl.ru>.

### 6. Федеральные информационно-образовательные порталы:

6.1. Информационная система [Единое окно доступа к образовательным ресурсам](http://window.edu.ru). Режим доступа: <http://window.edu.ru>

6.2. Федеральный портал [Российское образование](http://www.edu.ru). Режим доступа: <http://www.edu.ru>

### 7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ. Режим доступа : <http://lib.ulsu.ru/MegaPro/Web>

7.2. Образовательный портал УлГУ. Режим доступа : <http://edu.ulsu.ru>


Согласовано:

Зам.нач. УИТиТ  
должность сотрудника УИТиТ

/ Ключкова А.В.  
ФИО

  
подпись

/ 20.05.2019  
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. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106-1 корпус

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.

## 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

\_\_\_\_\_ / Рахеев С.М. /

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: <u>очная</u> )	
	Всего по плану	В т.ч. по семестрам
		6
1	2	3
Контактная работа обучающихся с преподавателем	54	54/54*
Аудиторные занятия		
• Лекции	36	36/36*
• Практические и семинарские занятия		
• Лабораторные работы (лабораторный практикум)	18	18/18*
Самостоятельная работа	54	54
Форма текущего контроля знаний и контроля самостоятельной работы		Лабораторные работы, проверка решения задач
Курсовая работа		
Виды промежуточной аттестации		Зачет
Всего часов по дисциплине	108	108
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

##### основная

1. Основы криптографии : учеб. пособие для вузов по спец. в обл. информ. безопасности / А. П. Алферов [и др.]. М. : Гелиос АРВ, 2001. 479 с.
2. 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>

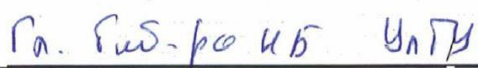
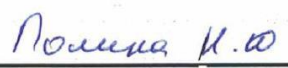

##### дополнительная

1. 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>
2. ГОСТ-Эксперт – единая база ГОСТов Российской Федерации для образования и промышленности:
  - 2.1. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012. — URL: <https://gostexpert.ru/gost/gost-34.10-2012>
  - 2.2. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2013. — URL: <https://gostexpert.ru/gost/gost-34.11-2012>

##### 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 «Теоретико-числовые методы в криптографии» 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 : 149 КБ). - Текст : электронный. Режим доступа: <http://lib.ulsu.ru/MegaPro/Download/MObject/4682>

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. Электронно-библиотечные системы:

1.1. **IPRbooks** [Электронный ресурс]: электронно-библиотечная система / группа компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов , [2019]. - Режим доступа: <http://www.iprbookshop.ru>.

1.2. **ЮРАЙТ** [Электронный ресурс]: электронно-библиотечная система / ООО Электронное издательство ЮРАЙТ. - Электрон. дан. – Москва , [2019]. - Режим доступа: <https://www.biblio-online.ru>.

1.3. **Консультант студента** [Электронный ресурс]: электронно-библиотечная система / ООО Политехресурс. - Электрон. дан. – Москва, [2019]. - Режим доступа: <http://www.studentlibrary.ru/pages/catalogue.html>.

1.4. **Лань** [Электронный ресурс]: электронно-библиотечная система / ООО ЭБС Лань. - Электрон. дан. – С.-Петербург, [2019]. - Режим доступа: <https://e.lanbook.com>.

1.5. **Znanium.com** [Электронный ресурс]: электронно-библиотечная система / ООО Знаниум. - Электрон. дан. – Москва, [2019]. - Режим доступа: <http://znanium.com>.

2. **КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2019].

3. **База данных периодических изданий** [Электронный ресурс] : электронные журналы / ООО ИВИС. - Электрон. дан. - Москва, [2019]. - Режим доступа: <https://dlib.eastview.com/browse/udb/12>.

4. **Национальная электронная библиотека** [Электронный ресурс]: электронная библиотека. - Электрон. дан. – Москва, [2019]. - Режим доступа: <https://нэб.рф>.

5. **Электронная библиотека диссертаций РГБ** [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2019]. - Режим доступа: <https://dvs.rsl.ru>.

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

6.1. Информационная система **Единое окно доступа к образовательным ресурсам**. Режим доступа: <http://window.edu.ru>

6.2. Федеральный портал **Российское образование**. Режим доступа: <http://www.edu.ru>

##### 7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ. Режим доступа : <http://lib.ulsu.ru/MegaPro/Web>

7.2. Образовательный портал УлГУ. Режим доступа : <http://edu.ulsu.ru>

Согласовано:

Зам.нач. УИТиТ  
должность сотрудника УИТиТ

/ Ключкова А.В.  
ФИО

  
подпись

/ 20.05.2019  
дата