МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
и.о. заведующего кафедрой
ERP-систем и бизнес-процессов
С.Л. Кенин

30.05.2023

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.47 Теоретико-числовые методы в криптографии

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

Анализ безопасности компьютерных систем

Математические методы защиты информации

Безопасность компьютерных систем и сетей

3. Квалификация (степень) выпускника: Специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

ERP-систем и бизнес-процессов

6. Составители программы:

Иванкин Михаил Петрович, к.т.н., доцент кафедры ERP-систем и бизнес-процессов

7. Рекомендована:

Научно-методическим советом факультета ПММ, протокол № 7 от 26.05.2023 г.

8. Учебный год: 2027/2028 **Семестр(ы):** 9

9. Цели и задачи учебной дисциплины

Целью изучения дисциплины «Теоретико-числовые методы в криптографии» является освоение студентом математического аппарата теории чисел для последующего успешного использования основных методов теории чисел в профессиональной деятельности. Задачами дисциплины являются: развитие у студентов соответствующих общекультурных, профессиональных и профессиональноспециализированных компетенций; ознакомление с основами классической и современной теории чисел и численными алгоритмами, имеющими практические приложения в криптографии; формирование умения строгой оценки эффективности применяемых алгоритмов с математической точки зрения; формирование четкого осознания необходимости и важности математической подготовки для специалиста по компьютерной безопасности. Цели образовательного процесса достигаются посредством применения инновационных образовательных технологий в обеспечении компетентностного подхода.

10. Место учебной дисциплины в структуре ОПОП: Дисциплина относится к обязательной части блока Б1 дисциплин учебного плана.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ОПК-8	Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;	ОПК-8.1	знает строение мультипликативной группы колец вычетов	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов.
		ОПК-8.2	знает способы представления действительных чисел цепными дробями	
		ОПК-8.3	знает основные свойства символов Лежандра и Якоби	
		ОПК-8.4	знает критерии простоты и их использование для факторизации натуральных чисел	
		ОПК-8.5	знает алгоритмы проверки чисел на простоту; построения больших простых чисел	
		ОПК-8.6	умеет строить большие простые числа	
		ОПК-8.7	умеет применять алгоритмы проверки чисел на простоту; построения больших простых чисел	

		ОПК-8.8	умеет применять алгоритмы разложения чисел на множители	
		ОПК-8.9	владеет навыками применения теории чисел в криптографии и	
			других дисциплинах	
ОПК-10	Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-10.12	знает основные методы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах	
		ОПК-10.13	знает базовые понятия теории эллиптических кривых	
		ОПК-10.14	умеет эффективно производить операции с большими числами, а также в кольцах вычетов, кольцах многочленов и конечных полях	
		ОПК-10.15	умеет исследовать и решать сравнения в кольцах вычетов	
		ОПК-10.16	умеет использовать достаточные условия простоты для построения больших простых чисел	
		ОПК-10.17	умеет оценивать теоретическую сложность применяемых алгоритмов	
		ОПК-10.18	владеет навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов	
		ОПК-10.19	владеет методами построения быстрых вычислительных алгоритмов алгебры и теории чисел	

12. Объем дисциплины в зачетных единицах/час.— 5/180.

Форма промежуточной аттестации - экзамен.

13. Виды учебной работы

Вид учебной работы	Трудоемкость	
		По семестрам

		Всего	9 семестр		
Аудиторные занятия		108	108		
в том числе:	лекции	54	54		
	практические	0	0		
	лабораторные	54	54		
Самостоятельная работа		36	36		
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – __час.)*		0/36	0/36		
Итого:		180	180		

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Введение в математические проблемы криптографии. Основы теории чисел.	В криптографии важную роль играют простые числа. Рассмотрены основы теории делимости. Приведены простые (с методической точки зрения) алгоритмы выявления простоты числа и алгоритм нахождения всех простых чисел, не превосходящих заданного числа. Рассмотрены алгоритмы нахождения наибольшего общего делителя и представления наибольшего общего делителя двух чисел в виде линейной комбинации (с целыми коэффициентами) этих чисел. Показаны области использования непрерывных дробей в криптографии. Описаны важнейшие функции теории чисел, в том числе широко используемая в криптографии функция Эйлера. На содержательном уровне описаны основные проблемы и понятия криптографии. В традиционной криптографии довольно часто используют преобразование y=ax+b (mod) m. Рассмотрено использование таких преобразований для генерации псевдослучайных последовательностей. Делимость, простые числа, наибольший общий делитель. Алгоритм Евклида, расширенный алгоритм Евклида. Цепные дроби. Асимптотический закон распределения простых чисел. Мультипликативные функции.	Теоретикочисловые методы в криптографии (10.05.01)
1.2	Теория сравнений. Вычеты.	Доказаны важные для криптографии с открытым ключом теоремы Ферма и Эйлера о свойстве операции возведения в степень по заданному модулю. Полная система вычетов, приведенная система вычетов. Zn, Zp, Z*n, Z* p Обратный элемент в Zn Алгебраические структуры на целых числах. Теорема Эйлера, теорема Ферма, тест Ферма на простоту. Криптосистема RSA. Понижение степени сравнения.	

1.3	Сравнения первой степени. Системы сравнений первой степени.	Исследовано нахождение решений сравнений первой степени и систем таких сравнений. В частности, доказана широко используемая в современной криптографии Китайская теорема об остатках. Приведены алгоритмы нахождения символов Лежандра и Якоби, значения которых позволяют решить вопрос о разрешимости сравнений второй степени по простому модулю.	
1.4	Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.	Квадратичные сравнения. Символ Лежандра. Закон взаимности. Существование решений квадратичного сравнения по простому модулю. Решение квадратичных сравнений по простому модулю. Символ Якоби и его свойства. Тест СоловеяШтрассена на простоту. Тест Миллера-Рабина. Существование и количество решений квадратичного сравнения по составному модулю. Решение квадратичных сравнений по составному модулю. Квадраты и псевдоквадраты. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации. Числа Блюма. BBSгенератор. Криптосистемы Блюма-Гольдвассер,	
		Гольдвассер-Микали.	
1.5	Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа.	Циклическая группа Z* p (Up). Порождающий элемент и дискретный логарифм. Задача дискретного логарифмирования. Криптосистемы Диффи-Хэллмана и Эль-Гамаля. Теоремы Сэлфриджа и Поклингтона. (n-1) – тесты на простоту. Доказуемо простые числа общего вида. Числа Ферма, теорема Пепина, тест Пепина. Числа Мерсенна и тест Лукаса-Лемера. Теорема Диемитко и процедура генерации простых чисел ГОСТ Р34.10-94.	
1.6	Алгоритмы криптоанализа шифров с открытым ключом.	Элементы теории сложности. Оценки сложности по времени, по объему требуемой памяти. Полиномиальная сложность, субэкспоненциальная сложность, экспоненциальная сложность алгоритмов. Сложность элементарных операций. Теоретико-числовые проблемы, лежащие в основе двухключевых криптосистем – факторизация, дискретное логарифмирование. Алгоритмы факторизации. Метод пробных делений, метод Ферма, метод квадратичного решета, ро-метод Полларда, p—1 – метод Полларда, методы случайных квадратов. Примеры, оценки сложности указанных алгоритмов. Алгоритмы дискретного логарифмирования. Метод прямого поиска, ро-метод Полларда, метод исчисления индексов, «шаг младенца-шаг великана». Примеры, оценки сложности указанных алгоритмов.	
1.7	Конечные группы и поля многочленов.	Многочлены над Zp, Zn. Сложение, умножение, факторизация многочленов. Не приводимые многочлены. Поля Галуа.	
2. Лабораторные работы			

2.1	Введение в математические проблемы криптографии. Основы теории чисел.	Простые числа. Основы теории делимости. Простые алгоритмы выявления простоты числа и алгоритм нахождения всех простых чисел, не превосходящих заданного числа. Алгоритмы нахождения наибольшего общего делителя и представления наибольшего общего делителя двух чисел в виде линейной комбинации (с целыми коэффициентами) этих чисел. Функция Эйлера. Алгоритм Евклида, расширенный алгоритм Евклида. Цепные дроби. Асимптотический закон распределения простых чисел. Мультипликативные функции.	
2.2	Теория сравнений. Вычеты.	Теоремы Ферма и Эйлера. . Полная система вычетов, приведенная система вычетов. Zn, Zp, Z*n, Z* p Обратный элемент в Zn. Алгебраические структуры на целых числах. Теорема Эйлера, теорема Ферма, тест Ферма на простоту. Криптосистема RSA. Понижение степени сравнения.	
2.3	Сравнения первой степени. Системы сравнений первой степени.	Нахождение решений сравнений первой степени и систем таких сравнений. Китайская теорема об остатках.	
2.4	Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.	Квадратичные сравнения. Символ Лежандра. Решение квадратичных сравнений по простому модулю. Символ Якоби и его свойства. Тест СоловеяШтрассена на простоту. Решение квадратичных сравнений по составному модулю. Квадраты и псевдоквадраты. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации. Числа Блюма. BBS-генератор. Криптосистемы Блюма-Гольдвассер, Гольдвассер-Микали.	
2.5	Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа.	Циклическая группа Z* p (Up). Порождающий элемент и дискретный логарифм. Задача дискретного логарифмирования. Криптосистемы Диффи-Хэллмана и Эль-Гамаля. Теоремы Сэлфриджа и Поклингтона. (n-1) – тесты на простоту. Доказуемо простые числа общего вида. Числа Ферма, теорема Пепина, тест Пепина. Числа Мерсенна и тест Лукаса-Лемера. Теорема Диемитко и процедура генерации простых чисел ГОСТ Р34.1094	
2.6	. Алгоритмы криптоанализа шифров с открытым ключом.	Элементы теории сложности. Алгоритмы факторизации. Метод пробных делений, метод Ферма, метод квадратичного решета, ро-метод Полларда, р—1 – метод Полларда, методы случайных квадратов. Алгоритмы дискретного логарифмирования. Метод прямого поиска, ро-метод Полларда, метод исчисления индексов, «шаг младенца-шаг великана».	
2.7	Конечные группы и поля многочленов.	Многочлены над Zp, Zn. Сложение, умножение, факторизация многочленов. Не приводимые многочлены. Поля Галуа.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практические	Лабораторные	Самостоятельная работа	Контрольная работа	Всего
1	Введение в математические проблемы криптографии. Основы теории чисел.	4	0	6	2	2	14
2	Теория сравнений. Вычеты.	8	0	8	6	4	26
3	Сравнения первой степени. Системы сравнений первой степени.	8	0	8	6	6	28
4	Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.	8	0	8	6	6	28
5	Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа.	8	0	8	6	6	28
6	Алгоритмы криптоанализа шифров с открытым ключом.	8	0	8	6	6	28
7	Конечные группы и поля многочленов.	10	0	8	4	6	28
	Итого:	54	0	54	36	36	180

14. Методические указания для обучающихся по освоению дисциплины

Изучение теоретического материала, представленного в лекциях, основной и дополнительной рекомендуемой литературе, итоговое повторение теоретического материала. Подготовка к лабораторным работам, контрольной работе и экзамену.

При использовании дистанционных образовательных технологий и электронного обучения следует выполнять все указания преподавателя по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Введение в теоретико-числовые методы криптографии : учебное пособие для спо / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург : Лань, 2021. — 396 с. — ISBN 978-5-8114-6926-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/153680 (дата обращения: 10.04.2021). — Режим доступа: для авториз. пользователей.

2	Василенко О. Н. Теоретико-числовые методы в криптографии [электронный ресурс] / О. Н. Василенко. – Электрон. Текстовые дан. – Москва: МЦНМО, 2003. -328 с. — Режим доступа: http://nozdr.ru

б) дополнительная литература:

№ п/п	Источник
3	Корниенко, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Корниенко, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, [б. г.]. — Часть 1 — 2017. — 64 с. — ISBN 978-5-7641-1053-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111765 (дата обращения: 10.02.2020). — Режим доступа: для авториз. пользователей.
4	Корниенко, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Корниенко, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, 2018 — Часть 2 — 2018. — 63 с. — ISBN 978-5-7641-1215-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/138103 (дата обращения: 10.02.2020). — Режим доступа: для авториз. пользователей.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)***:**

№ п/п	Ресурс
	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
6	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
	Теоретико-числовые методы в криптографии (0.05.01)/ Ю.А. Крыжановская. — Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru.

16. Перечень учебно-методического обеспечения для самостоятельной работы В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения теоретико-числовых методов. Также предусмотрено получение консультаций по вопросам изучаемой дисциплине, изучение теоретического материала, представленного в лекциях, основной и дополнительной рекомендуемой литературе, выполнение индивидуальных и групповых заданий лабораторных работ, итоговое повторение теоретического материала. Также к СРС относится подготовка к контрольной работе и экзамену.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебнометодический комплекс, который включает в себя: программу курса, учебные пособия, методические указания по выполнению практических заданий. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение)

При реализации дисциплины используются следующие образовательные технологии: логическое построение дисциплины, обозначение теоретического и практического компонентов в учебном материале. Применяются разные типы лекций (вводная, обзорная, информационная, проблемная).

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс, размещенный на платформе Электронного университета ВГУ (LMS moodle).

18. Материально-техническое обеспечение дисциплины:

Учебная аудитория для лекций: специализированная мебель, компьютер преподавателя, мультимедийный проектор, экран.

Учебная аудитория для лабораторных занятий: специализированная мебель, персональные компьютеры, мультимедийный проектор, экран.

Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ.

Программное обеспечение: ОС Windows v.7, 8, 10, набор утилит (архиваторы, файлменеджеры), LibreOffice v.5-7, Foxit PDF Reader, Visual Studio, v. 2010-2019.

Список аудиторий ФКН:

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 479

Учебная аудитория: специализированная мебель, компьютер преподавателя i5-84002,8ГГц, монитор с ЖК 19’’, мультимедийный проектор, экран

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, ауд. 505п

Учебная аудитория: специализированная мебель, компьютер преподавателя i5-3220-3.3ГГц, монитор с ЖК 17’’, мультимедийный проектор, экран

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 292

Учебная аудитория: специализированная мебель, компьютер преподавателя PentiumG3420-3,2ГГц, монитор с ЖК 17", мультимедийный проектор, экран. Система для видеоконференций Logitech ConferenceCam Group и ноутбук 15.6’’ FHD Lenovo V15515API

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 380

Учебная аудитория: специализированная мебель, компьютер преподавателя i3-32403,4ГГц, монитор с ЖК 17’’, мультимедийный проектор, экран

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, аудитория 291

Учебная аудитория: специализированная мебель, персональные компьютеры на базе i33220-3,3ГГц, мониторы ЖК 19’’ (16 шт.), мультимедийный проектор, экран.

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, аудитория 293

Учебная аудитория: специализированная мебель, персональные компьютеры на базе Core i7-11700K-3.6 ГГц, мониторы ЖК 24’’ (16 шт.), мультимедийный проектор, экран.

Лабораторное оборудование компьютерной графики видеоадаптеры GeForce RTX 3070.

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 297

Учебная аудитория: специализированная мебель, ноутбуки HP EliteBook на базе Intel Core i5-8250U-3.4 ГГц, мониторы ЖК 24’’ (16 шт.), мультимедийный проектор, экран.

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 382

Учебная аудитория: специализированная мебель, персональные компьютеры на базе i59600KF-3,7ГГц, мониторы ЖК 24’’ (16 шт.), ТВ панель-флипчарт.

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 385
Учебная аудитория: специализированная мебель, персональные компьютеры на базе i32120-3,3ГГц, мониторы ЖК 19’’ (16 шт.), мультимедийный проектор, экран.

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 387
Учебная аудитория: специализированная мебель, компьютер преподавателя Core2DuoE7600-3ГГц, монитор с ЖК 22’’, мультимедийный проектор, экран.

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, аудитория 314п
Учебная аудитория: специализированная мебель, персональные компьютеры на базе i37100-3,6ГГц, мониторы ЖК 19’’ (16 шт.), мультимедийный проектор, экран.

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, аудитория 316п
Учебная аудитория: специализированная мебель, персональные компьютеры на базе i39100-3,6ГГц, мониторы ЖК 19’’ (30 шт.), мультимедийный проектор, экран

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Введение в математические проблемы криптографии. Основы теории чисел. Теория сравнений. Вычеты.	ОПК-8	ОПК-8.1; ОПК-8.2; ОПК-8.3; ОПК-8.4; ОПК-8.5; ОПК-8.6; ОПК-8.7; ОПК-8.8; ОПК-8.9	Устный опрос, лабораторные работы. Контрольная работа.
2	Сравнения первой степени. Системы сравнений первой степени.			
3	Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.			
4	Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа.			
5	Алгоритмы криптоанализа шифров с открытым ключом.			
6	Конечные группы и поля многочленов.			
7	Введение в математические проблемы криптографии.	ОПК-10	ОПК-10.12; ОПК-10.13; ОПК-10.14;	Лабораторные работы.

	Основы теории чисел.		ОПК-10.15; ОПК10.16; ОПК-10.17; ОПК-10.18; ОПК-10.19	Контрольная работа.
Промежуточная аттестация, форма контроля - зачет				Перечень вопросов

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

 устный опрос,
лабораторные работы,
контрольная работа.

Перечень вопросов для устного опроса

1. Простые числа. Основы теории делимости. Простые алгоритмы выявления простоты числа, алгоритм нахождения всех простых чисел, не превосходящих заданного числа.
2. Области использования непрерывных дробей в криптографии.
3. Важнейшие функции теории чисел.
4. Основные проблемы и понятия криптографии.
5. Преобразование y=ax+b (mod) m. Его использование для генерации псевдослучайных последовательностей.
6. Алгоритм Евклида, расширенный алгоритм Евклида. Цепные дроби.
7. Асимптотический закон распределения простых чисел. Мультипликативные функции. Функция Эйлера.
8. Теоремы Ферма и Эйлера. тест Ферма на простоту.
9. Полная система вычетов, приведенная система вычетов. Zn, Zp, Z*n, Z* p Обратный элемент в Zn Алгебраические структуры на целых числах.
10. Криптосистема RSA. Понижение степени сравнения.
11. Нахождение решений сравнений первой степени и систем таких сравнений.
12. Китайская теорема об остатках.
13. Алгоритмы нахождения символов Лежандра и Якоби.
14. Квадратичные сравнения. Закон взаимности. Существование решений квадратичного сравнения по простому модулю.
15. Решение квадратичных сравнений по простому модулю. Символ Якоби и его свойства.
16. Тест Соловея-Штрассена на простоту.
17. Тест Миллера-Рабина.
18. Существование и количество решений квадратичного сравнения по составному модулю.
19. Решение квадратичных сравнений по составному модулю. Квадраты и псевдоквадраты.
20. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации. Числа Блюма. BBS-генератор.

21. Криптосистемы Блюма-Гольдвассер, Гольдвассер-Микали.
22. Циклическая группа Z* p (Up).
23. Порождающий элемент и дискретный логарифм. Задача дискретного логарифмирования. Криптосистемы Диффи-Хэллмана и Эль-Гамаля.
24. Теоремы Сэлфриджа и Поклингтона. (n-1) – тесты на простоту. Доказуемо простые числа общего вида.
25. Числа Ферма, теорема Пепина, тест Пепина. Числа Мерсенна и тест Лукаса-Лемера.
26. Теорема Диемитко и процедура генерации простых чисел ГОСТ Р34.10-94.
27. Элементы теории сложности. Оценки сложности по времени, по объему требуемой памяти. Полиномиальная сложность.
28. субэкспоненциальная сложность, экспоненциальная сложность алгоритмов.
29. Сложность элементарных операций.
30. Факторизация, дискретное логарифмирование.
31. Алгоритмы факторизации.
32. Алгоритмы дискретного логарифмирования.
33. Сложение и умножение многочленов.
34. Разложение многочленов на сомножители. Неприводимые многочлены.
35. Различие понятий – кодирование и шифрование.
36. От каких характеристик кода зависит его корректирующая способность.
37. Сравните коды Хэмминга и циклические коды по эффективности контроля целостности информации.
38. Теоретико-числовые проблемы, лежащие в основе двухключевых криптосистем – факторизация, дискретное логарифмирование. Алгоритмы факторизации. Метод пробных делений, метод Ферма, метод квадратичного решета, ро-метод Полларда, р—1 – метод Полларда, методы случайных квадратов. Примеры, оценки сложности указанных алгоритмов. Алгоритмы дискретного логарифмирования.
39. Метод прямого поиска, ро-метод Полларда, метод исчисления индексов, «шаг младенца-шаг великана». Примеры, оценки сложности указанных алгоритмов.
40. Многочлены над Zp, Zn.
41. Сложение, умножение, факторизация многочленов.
42. Не приводимые многочлены.
43. Поля Галуа.

Перечень заданий для контрольных работ

Вариант 1.

1. Простые числа.
2. Теорема Эйлера.
3. Китайская теорема об остатках.
4. Тест Миллера-Рабина.
5. Криптосистемы Диффи-Хэллмана.
6. «шаг младенца-шаг великана».
7. Не приводимые многочлены.

Вариант 2.

1. Основы делимости.
2. Теорема Ферма.
3. Алгоритмы нахождения символов Лежандра и Якоби.

4. Тест Соловея-Штрассена.
5. Теорема Диемитко и процедура генерации простых чисел ГОСТ Р34.10-94 6. метод исчисления индексов
7. Поля Галуа.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного опроса; лабораторных работ; контрольной работы.

Перечень лабораторных работ

Лабораторная работа №1. Введение в математические проблемы криптографии. Основы теории чисел.	*Теоретические сведения* Простые числа. Основы теории делимости. Простые алгоритмы выявления простоты числа и алгоритм нахождения всех простых чисел, не превосходящих заданного числа. Алгоритмы нахождения наибольшего общего делителя и представления наибольшего общего делителя двух чисел в виде линейной комбинации (с целыми коэффициентами) этих чисел. Функция Эйлера. Алгоритм Евклида, расширенный алгоритм Евклида. Цепные дроби. Асимптотический закон распределения простых чисел. Мультипликативные функции. *Практическая часть* Реализовать программно рассмотренные алгоритмы.
Лабораторная работа №2. Теория сравнений. Вычеты.	*Теоретические сведения* Теоремы Ферма и Эйлера. Полная система вычетов, приведенная система вычетов. Zn, Zp, Z*n, Z* p Обратный элемент в Zn. Алгебраические структуры на целых числах. 4. Теорема Эйлера, теорема Ферма, тест Ферма на простоту. Криптосистема RSA. Понижение степени сравнения. *Практическая часть* Программно реализовать операции и тесты.
Лабораторная работа №3 Сравнения первой степени. Системы сравнений первой степени.	*Теоретические сведения* 1. Нахождение решений сравнений первой степени и систем таких сравнений. 2. Китайская теорема об остатках. *Практическая часть* 1. Программно реализовать нахождение решения сравнений первой степени.
Лабораторная работа №4. Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.	*Теоретические сведения* Квадратичные сравнения. Символ Лежандра. Решение квадратичных сравнений по простому модулю. Символ Якоби и его свойства. Тест Соловея-Штрассена на простоту. Решение квадратичных сравнений по составному модулю. Квадраты и псевдоквадраты. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации. Числа Блюма. BBS-генератор. Криптосистемы Блюма-Гольдвассер, Гольдвассер-Микали. *Практическая часть* Реализовать программно применение одной из указанных тем.

Лабораторная работа №5. Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа.	*Теоретические сведения* Циклическая группа Z* p (Up). Порождающий элемент и дискретный логарифм. Задача дискретного логарифмирования. Криптосистемы Диффи-Хэллмана и Эль-Гамаля. Теоремы Сэлфриджа и Поклингтона. (n-1) – тесты на простоту. Доказуемо простые числа общего вида. Числа Ферма, теорема Пепина, тест Пепина. Числа Мерсенна и тест ЛукасаЛемера. Теорема Диемитко и процедура генерации простых чисел ГОСТ Р34.10-94 *Практическая часть* Реализовать один из указанных методов
Лабораторная работа №6. Алгоритмы криптоанализа шифров с открытым ключом.	*Теоретические сведения* Элементы теории сложности. Алгоритмы факторизации. Метод пробных делений, метод Ферма, метод квадратичного решета, ро-метод Полларда, р—1 – метод Полларда, методы случайных квадратов. Алгоритмы дискретного логарифмирования. Метод прямого поиска, ро-метод Полларда, метод исчисления индексов, «шаг младенца-шаг великана». *Практическая часть* Реализовать один из указанных методов
Лабораторная работа №7.	*Теоретические сведения*
Конечные группы и поля многочленов.	Многочлены над Zp, Zn. Сложение, умножение, факторизация многочленов. Не приводимые многочлены. Поля Галуа. *Практическая часть* По вводимым данным сформировать Многочлены над Zp, Zn. Реализовать сложение, умножение, факторизацию многочленов.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

- вопросы к экзамену.

Перечень вопросов к экзамену

1. Простые числа. Основы теории делимости. Простые алгоритмы выявления простоты числа, алгоритм нахождения всех простых чисел, не превосходящих заданного числа.
2. Области использования непрерывных дробей в криптографии.
3. Важнейшие функции теории чисел.
4. Основные проблемы и понятия криптографии.
5. Преобразование y=ax+b (mod) m. Его использование для генерации псевдослучайных последовательностей.
6. Алгоритм Евклида, расширенный алгоритм Евклида. Цепные дроби.
7. Асимптотический закон распределения простых чисел. Мультипликативные функции. Функция Эйлера.
8. Теоремы Ферма и Эйлера. тест Ферма на простоту.
9. Полная система вычетов, приведенная система вычетов. Zn, Zp, Z*n, Z* p Обратный элемент в Zn Алгебраические структуры на целых числах.
10. Криптосистема RSA. Понижение степени сравнения.
11. Нахождение решений сравнений первой степени и систем таких сравнений.

12. Китайская теорема об остатках.
13. Алгоритмы нахождения символов Лежандра и Якоби.
14. Квадратичные сравнения. Закон взаимности. Существование решений квадратичного сравнения по простому модулю.
15. Решение квадратичных сравнений по простому модулю. Символ Якоби и его свойства.
16. Тест Соловея-Штрассена на простоту.
17. Тест Миллера-Рабина.
18. Существование и количество решений квадратичного сравнения по составному модулю.
19. Решение квадратичных сравнений по составному модулю. Квадраты и псевдоквадраты.
20. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации. Числа Блюма. BBS-генератор.
21. Криптосистемы Блюма-Гольдвассер, Гольдвассер-Микали.
22. Циклическая группа Z* p (Up).
23. Порождающий элемент и дискретный логарифм. Задача дискретного логарифмирования. Криптосистемы Диффи-Хэллмана и Эль-Гамаля.
24. Теоремы Сэлфриджа и Поклингтона. (n-1) – тесты на простоту. Доказуемо простые числа общего вида.
25. Числа Ферма, теорема Пепина, тест Пепина. Числа Мерсенна и тест Лукаса-Лемера.
26. Теорема Диемитко и процедура генерации простых чисел ГОСТ Р34.10-94.
27. Элементы теории сложности. Оценки сложности по времени, по объему требуемой памяти. Полиномиальная сложность.
28. субэкспоненциальная сложность, экспоненциальная сложность алгоритмов.
29. Сложность элементарных операций.
30. Факторизация, дискретное логарифмирование.
31. Алгоритмы факторизации.
32. Алгоритмы дискретного логарифмирования.
33. Сложение и умножение многочленов.
34. Разложение многочленов на сомножители. Неприводимые многочлены.
35. Различие понятий – кодирование и шифрование.
36. От каких характеристик кода зависит его корректирующая способность.
37. Сравните коды Хэмминга и циклические коды по эффективности контроля целостности информации.
38. Теоретико-числовые проблемы, лежащие в основе двухключевых криптосистем – факторизация, дискретное логарифмирование. Алгоритмы факторизации. Метод пробных делений, метод Ферма, метод квадратичного решета, ро-метод Полларда, р—1 – метод Полларда, методы случайных квадратов. Примеры, оценки сложности указанных алгоритмов. Алгоритмы дискретного логарифмирования.
39. Метод прямого поиска, ро-метод Полларда, метод исчисления индексов, «шаг младенца-шаг великана». Примеры, оценки сложности указанных алгоритмов.
40. Многочлены над Zp, Zn.
41. Сложение, умножение, факторизация многочленов.
42. Не приводимые многочлены.
43. Поля Галуа.
44.

Соотношение показателей, критериев и шкалы оценивания результатов обучения:

Компетенция		Шкала и критерии оценивания уровня освоения компетенции

	Показатель сформированности компетенции	5	4	3	2
ОПК-8, ОПК-10	Знает: – теоретико-числовые методы защиты информации.	Сформированные знания	Сформированные знания, но содержащие отдельные пробелы	Неполные знания	Фрагментарные знания или их отсутствие
	Умеет: – реализовывать алгоритмы защиты данных на основе теоретико-числовых методов.	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений
	Владеет: – навыками построения математических моделей элементов	Сформированные навыки	Успешные навыки, но содержащие отдельные пробелы	Успешные, но не системные навыки	Фрагментарные навыки или их отсутствие