

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Оренбургский государственный университет»

Кафедра математики и цифровых технологий

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.3 Теоретико-числовые методы в криптографии»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

02.03.01 Математика и компьютерные науки

(код и наименование направления подготовки)

Цифровые технологии

(наименование направленности (профиля) образовательной программы)

Квалификация

Бакалавр

Форма обучения

Очная

Год набора 2025

Рабочая программа дисциплины «Б1.Д.В.3 Теоретико-числовые методы в криптографии» рассмотрена и утверждена на заседании кафедры

Кафедра математики и цифровых технологий

наименование кафедры

протокол № 6 от "19" февраля 2025г.

Заведующий кафедрой

Кафедра математики и цифровых технологий

наименование кафедры

подпись

А.Е. Шухман

расшифровка подписи

Исполнители:

Старший преподаватель

должность

подпись

А.Н. Благовисная

расшифровка подписи

должность

подпись

расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по направлению подготовки

02.03.01 Математика и компьютерные науки

код наименование

личная подпись

А.Е. Шухман

расшифровка подписи

Заведующий отделом формирования фонда и научной обработки документов

личная подпись

расшифровка подписи

Уполномоченный по качеству института

личная подпись

расшифровка подписи

№ регистрации _____

© Благовисная А.Н., 2025
© ОГУ, 2025

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

- формирование у обучающихся теоретических знаний, практических умений и навыков применения методов теории чисел, необходимых для решения задач в области защиты информации.

Задачи:

- изучение математических основ и базовых конструкций теории чисел, используемых при исследовании и построении современных алгоритмов, методов и моделей защиты информации;
- овладение основными математическими методами и алгоритмами теории чисел, применяемыми в решении проблем построения криптографических конструкций;
- приобретение навыков решения теоретических и практических задач защиты информации математическими методами.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательным дисциплинам (модулям) вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: Б1.Д.Б.16 Алгебра и теория чисел, Б1.Д.Б.18 Дискретная математика и математическая логика, Б1.Д.Б.22 Основы программирования, Б1.Д.Б.34 Дополнительные разделы алгебры

Постреквизиты дисциплины: Б1.Д.В.Э.3.1 Программирование WEB-приложений, Б1.Д.В.Э.4.1 Методы алгебраической геометрии в криптографии, Б1.Д.В.Э.4.2 Криптографические протоколы

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ПК*-1 Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий	ПК*-1-В-1 Обладает базовыми знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий ПК*-1-В-2 Умеет находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности, в математике и информатике ПК*-1-В-3 Имеет практический опыт научно-исследовательской деятельности в математике и информатике	Знать: - основы теории делимости в кольце целых чисел, теории числовых сравнений и сравнений с неизвестными, теории первообразных корней и индексов; - формулировки классических задач теории чисел, используемых в криптографических приложениях; - формулировки утверждений и теорем разделов теории чисел, связанных с задачами защиты информации. Уметь: - решать задачи теории чисел, возникающие при создании и исследовании криптографических конструкций; - адаптировать постановки классических задач теории чисел для криптографических целей; - доказывать утверждения и теоремы разделов теории чисел, связанных с задачами защиты информации.

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		Владеть: - методами проверки чисел на простоту, построения больших простых чисел, дискретного логарифмирования в конечных циклических группах; - навыками постановки теоретико-числовых задач криптографии; - различными методами вывода основных результатов теории чисел.
ПК*-2 Способен использовать современные методы разработки и реализации конкретных алгоритмов на основе математических моделей на базе языков программирования и пакетов прикладных программ моделирования	ПК*-2-В-1 Знает современные методы разработки и реализации алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования ПК*-2-В-2 Умеет разрабатывать и реализовывать алгоритмы математических моделей на базе языков и пакетов прикладных программ моделирования ПК*-2-В-3 Имеет практический опыт разработки и реализации алгоритмов на базе языков и пакетов прикладных программ моделирования	Знать: - алгоритмы теории чисел, применяемые в криптографических приложениях. Уметь: - оценивать возможности и методы более рационального способа реализации алгоритмов теории чисел, применяемых в криптографических приложениях. Владеть: - навыками реализации алгоритмов теории чисел, применяемых в криптографических приложениях.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц (216 академических часов).

Вид работы	Трудоемкость, академических часов		
	6 семестр	7 семестр	всего
Общая трудоёмкость	108	108	216
Контактная работа:	34,25	35,25	69,5
Лекции (Л)	18	18	36
Практические занятия (ПЗ)	16		16
Лабораторные работы (ЛР)		16	16
Консультации		1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25	0,5
Самостоятельная работа: - выполнение расчетно-графического задания (РГЗ); - решение типовых задач; - самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий; - изучение разделов курса в системе электронного обучения; - подготовка к лабораторным занятиям; - подготовка к практическим занятиям; - подготовка к тестам, опросам;	73,75	72,75	146,5

Вид работы	Трудоемкость, академических часов		
	6 семестр	7 семестр	всего
- подготовка к рубежному контролю; - подготовка к промежуточной аттестации).			
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	зачет	экзамен	

Разделы дисциплины, изучаемые в 6 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Элементы теории делимости	28	4	2		22
2	Сравнения и системы сравнений	80	14	14		52
	Итого:	108	18	16		74

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
3	Алгоритмы теории чисел, применяемые в криптографии	38	6		8	24
4	Проверка чисел на простоту и построение больших простых чисел	38	6		4	28
5	Криптографические приложения теории чисел	32	6		4	22
	Итого:	108	18		16	74
	Всего:	216	36	16	16	148

4.2 Содержание разделов дисциплины

№ 1 Элементы теории делимости

Делимость целых чисел. Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. Расширенный алгоритм Евклида и линейное представление наибольшего общего делителя. Обобщенный алгоритм Евклида. Линейные диофантовы уравнения. Простые и составные числа. Бесконечность множества простых чисел. Основная теорема арифметики о разложении целых чисел на простые сомножители. Важнейшие функции теории чисел: $[x]$, $\{x\}$, мультипликативные функции, функция Мёбиуса, функция Эйлера.

№ 2 Сравнения и системы сравнений

Числовые сравнения и их свойства. Полная и приведенная система вычетов, свойства. Теорема Эйлера, малая теорема Ферма. Кольцо классов вычетов, обратимые элементы, делители нуля, мультипликативная группа кольца, ее строение. Методы нахождения мультипликативных обратных элементов, основанные на расширенном алгоритме Евклида и малой теореме Ферма.

Сравнения первой степени: анализ, способы решения. Системы линейных сравнений. Китайская теорема об остатках, ее использование при упрощении вычислений.

Теория сравнений второй степени, символ Лежандра, его свойства, символ Якоби. Алгоритм Шэнкса. Квадратичные сравнения по составному модулю.

Первообразные корни и индексы. Существование первообразного корня по простому модулю; первообразные корни по модулям p и $2p$; отыскание первообразных корней. Индексы по модулям p и $2p$; таблицы индексов. Решение степенных сравнений.

№ 3 Алгоритмы теории чисел, применяемые в криптографии

Понятие сложности алгоритма. Реализация и оценка сложности алгоритма Евклида и его модификаций. Реализация и оценка сложности алгоритмов поиска мультипликативных обратных элементов. Реализация и оценка сложности алгоритмов решения линейных сравнений первой степени и их систем. Реализация и оценка сложности алгоритмов возведения в степень по модулю. Реализация алгоритма поиска символа Якоби. Реализация и оценка сложности алгоритмов поиска решения квадратичных сравнений.

№ 4 Проверка чисел на простоту и построение больших простых чисел

Понятие детерминированных, вероятностных методов проверки чисел на простоту. Метод пробных делений. Решето Эратосфена. Критерий Вильсона. Тест на основе малой теоремы Ферма. Свойства чисел Кармайкла. Тест Соловея-Штрассена. Тест Рабина-Миллера. Полиномиальный тест распознавания простоты. Числа Мерсенна и проверка чисел Мерсенна на простоту.

№ 5 Криптографические приложения теории чисел

Схемы разделения секрета. Протокол Диффи-Хеллмана. Алгоритм RSA. Алгоритм Эль-Гамала. Криптосистема Рабина. Алгоритмы получения и проверки ЭЦП.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	3	Реализация алгоритма Евклида и его модификаций.	2
2	3	Реализация алгоритмов возведения в степень по модулю. Реализация алгоритмов поиска мультипликативных обратных.	2
3	3	Реализация алгоритмов решения линейных сравнений первой степени и их систем.	2
4	3	Реализация алгоритма поиска символа Якоби. Реализация алгоритмов поиска решения квадратичных сравнений.	2
5, 6	4	Реализация детерминированных и вероятностных тестов простоты.	4
7	5	Реализация схем разделения ключей и схем распределения ключей.	2
8	5	Реализация алгоритмов шифрования и схем цифровых подписей.	2
		Итого:	16

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	НОД целых чисел. Алгоритм Евклида и его модификации. Линейные диофантовы уравнения.	2
2	2	Мультипликативные обратные элементы в кольцах вычетов. Возведение в степень по модулю.	2
3	2	Сравнения первой степени.	2
4	2	Системы линейных сравнений.	2
5	2	Квадратичные сравнения.	2
6	2	Первообразные корни.	2
7	2	Индексы.	2
8	2	Степенные сравнения.	2
		Итого:	16

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. – СПб.: Лань, 2004. – 176 с.
2. Сمارт, Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. – Москва: Техносфера, 2006. – 528 с.

5.2 Дополнительная литература

1. Глухов М.М. Введение в теоретико-числовые методы криптографии: учеб. пособие для вузов / М.М. Глухов [и др.]. – СПб.: Лань, 2011. – 400 с.
2. Отрыванкина, Т.М. Алгоритмы компьютерной алгебры: практикум / Т.М. Отрыванкина; М-во образования и науки Рос. Федерации, Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования «Оренбург. гос. ун-т», каф. приклад. математики. – Оренбург: ОГУ, 2007. – 26 с.
3. Пихтилькова, О.А. Сравнения и системы сравнений [Электронный ресурс]: методические указания для обучающихся по образовательной программе высшего образования по направлению подготовки 02.03.01 Математика и компьютерные науки / О.А. Пихтилькова, А.Н. Благовисная; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования «Оренбург. гос. ун-т». – Электрон. текстовые дан. (1 файл: 1.13 Мб). – Оренбург: ОГУ, 2018. – 48 с. – Загл. с тит. экрана. – Adobe Acrobat Reader 6.0. – Режим доступа: http://artlib.osu.ru/web/books/metod_all/63792_20180314.pdf
4. Лабораторные работы по дисциплине «Теоретико-числовые методы в криптографии» [Электронный ресурс]: методические указания для обучающихся по образовательным программам высшего образования по направлению подготовки 02.03.01 Математика и компьютерные науки / сост.: А.Н. Благовисная, Е.В. Мещерина; М-во науки и высш. образования Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования «Оренбург. гос. ун-т», Каф. математики и цифровых технологий. – Электрон. текстовые дан. (1 файл: 1.02 Мб). – Оренбург: ОГУ, 2024. – 52 с. – Загл. с тит. экрана. – Adobe Acrobat Reader 6.0. – Режим доступа: http://artlib.osu.ru/web/books/metod_all/203184_20240424.pdf

5.3 Периодические издания

1. Вестник компьютерных и информационных технологий: журнал. – М.: Агентство «Роспечать», 2017-2024.
2. Информационные технологии: журнал. – М.: Агентство «Роспечать», 2017-2024.

5.4 Интернет-ресурсы

1. <http://eqworld.ipmnet.ru/indexr.htm> – международный научно-образовательный сайт «Мир математических уравнений», который содержит обширную учебную физико-математическую библиотеку и предназначен для широкого круга ученых, преподавателей вузов, инженеров, аспирантов и студентов в различных областях математики и других наук; все ресурсы сайта являются бесплатными для его пользователей).
2. <https://znanierussia.ru/> – сайт Российского общества «Знание», который содержит интеллектуальный контент о достижениях в области науки, культуры и искусства и других сферах жизни.
3. <https://arxiv.org/> – крупнейший бесплатный архив электронных публикаций научных статей и их препринтов по физике, математике, астрономии, информатике и биологии.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.
2. Пакет офисных приложений LibreOffice.
3. Программа для просмотра сайтов Яндекс.Браузер, свободно распространяемая, входит в реестр отечественного ПО.
4. Автоматизированная интерактивная система сетевого тестирования (АИССТ) (регистрационный номер в РОСПАТЕНТ №2011610456). Режим доступа: <https://osu.aistt.ru/>
5. Университетская платформа электронного обучения «Электронные курсы ОГУ в системе обучения Moodle» (<http://moodle.osu.ru>)
6. «DION» (Конфигурация «DION EDU») – платформа для проведения онлайн мероприятий и видеоконференций.
7. Elibrary [Электронный ресурс]: реферативная база данных, с ограниченным доступом к полным текстам статей – Режим доступа: <https://www.elibrary.ru/>, в локальной сети ОГУ.
8. Math-Net.ru [Электронный ресурс]: общероссийский математический портал, включающий информационно-справочную систему по публикациям в отечественных математических журналах. – Режим доступа: <http://www.mathnet.ru/>.
9. Система программирования Python, свободно распространяемая по лицензии PSFL.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется компьютерный класс, оснащенный компьютерной техникой.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой подключенной к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ОГУ.