

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Оренбургский государственный университет имени В.А. Бондаренко»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.40 Теоретико-числовые методы в криптографии»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность

10.05.01 Компьютерная безопасность

(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»

(наименование направленности (профиля)/специализации образовательной программы)

Квалификация

Специалист по защите информации

Форма обучения

Очная

Год набора 2026

Рабочая программа дисциплины «Б1.Д.Б.40 Теоретико-числовые методы в криптографии» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 9 от "20" марта 2026 г.

Заведующий кафедрой

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры  И.В. Влацкая
подпись расшифровка подписи

Исполнители:

Старший преподаватель должность  А.Н. Благовисная
подпись расшифровка подписи

должность подпись расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по специальности

10.05.01 Компьютерная безопасность код наименование  И.В. Влацкая
личная подпись расшифровка подписи

Заведующий отделом формирования фонда и научной обработки документов

 С.А. Биктимирова
личная подпись расшифровка подписи

Уполномоченный по качеству института

 С.Н. Морозова
личная подпись расшифровка подписи

№ регистрации _____

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 базовой части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: Б1.Д.Б.14 Алгебра

Постреквизиты дисциплины: Б1.Д.Б.38 Методы и средства криптографической защиты информации, Б1.Д.В.2 Технология построения защищенных автоматизированных систем

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
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10-В-1 Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами ОПК-10-В-2 Владеет навыками использования типовых криптографических алгоритмов ОПК-10-В-4 Умеет проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств ОПК-10-В-5 Владеет подходами к разработке и анализу безопасности криптографических протоколов	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; - алгоритмы теории чисел, применяемые в криптографических приложениях. Уметь: - решать задачи теории чисел,

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		возникающие при создании и исследовании криптографических конструкций; - адаптировать постановки классических задач теории чисел для криптографических целей; - доказывать утверждения теории чисел, связанные с задачами защиты информации; - оценивать возможности и методы более рационального способа реализации алгоритмов теории чисел, применяемых в криптографических приложениях. Владеть: - методами проверки чисел на простоту, построения больших простых чисел, дискретного логарифмирования в конечных циклических группах; - навыками постановки и решения теоретико-числовых задач криптографии.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 академических часа).

Вид работы	Трудоемкость, академических часов	
	5 семестр	всего
Общая трудоёмкость	144	144
Контактная работа:	69,25	69,25
Лекции (Л)	34	34
Практические занятия (ПЗ)	34	34
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: - выполнение индивидуального творческого задания (ИТЗ); - самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий); - изучение разделов курса в системе электронного обучения; - подготовка к практическим занятиям; - подготовка к тестам, опросам).	74,75	74,75
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	экзамен	

№ раздела	Наименование разделов	Количество часов			
		всего	аудиторная работа		
			Л	ПЗ	ЛР
1	Элементы теории делимости	14	4	2	
2	Сравнения и системы сравнений	66	16	18	
3	Многочлены над (конечными) полями	28	6	6	
4	Проверка чисел на простоту и построение больших простых чисел	16	4	2	
5	Криптографические приложения теории чисел	20	4	6	
	Итого:	144	34	34	
	Всего:	144	34	34	

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 Многочлены над (конечными) полями

Основные понятия и теоремы теории многочленов над полем. Неприводимые многочлены над конечным полем. Строение конечных полей. Порядок многочлена. Нахождение НОД. Разложение полинома на простые множители по модулю p . Разложение полинома над $\mathbb{Z}$.

№ 4 Проверка чисел на простоту и построение больших простых чисел

Понятие детерминированных, вероятностных методов проверки чисел на простоту. Метод пробных делений. Решието Эратосфена. Критерий Вильсона. Тест на основе малой теоремы Ферма. Свойства чисел Кармайкла. Тест Соловья-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-Гамаля. Криптосистема Рабина. Алгоритмы получения и проверки ЭЦП.

4.3 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 с помощью бинарного алгоритма.	2
3	2	Сравнения первой степени.	2
4	2	Системы линейных сравнений. Греко-китайская теорема об остатках (ГКТО). Алгоритм быстрого возведения в степень по модулю с использованием ГКТО.	2
5	2	Восстановление целого числа по остаткам. Определение знака целого числа, представленного вектором по смешанному модулю.	2
6	2	Квадратичные сравнения. Символы Лежандра и Якоби. Алгоритм Шэнкса.	2
7	2	Квадратичные сравнения по составному модулю	2
8	2	Первообразные корни. Алгоритмы поиска первообразных корней.	2
9	2	Индексы. Таблицы индексов.	2
10	2	Степенные сравнения и дискретное логарифмирование.	2
11	3	Многочлены над простыми конечными полями.	2
12	3	Неприводимые многочлены над конечным полем. Строение конечных полей.	4
13	4	Алгоритмы проверки простоты натурального числа.	2
14	5	Схемы разделения секрета. Протокол Диффи-Хеллмана.	2
15	5	Алгоритмы RSA, Эль-Гамала и Рабина.	2
16	5	Схемы ЭЦП на основе алгоритмов теории чисел.	2
		Итого:	34

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. Фороузан, Б. А. Математика криптографии и теория шифрования: учебное пособие: [16+] / Б. А. Фороузан. – 2-е изд., испр. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 511 с.: ил., схем. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=428998>

5.2 Дополнительная литература

1. 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.
2. 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

3. Сمارт, Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. – Москва: Техносфера, 2006. – 528 с.

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.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.

2. Пакет офисных приложений «МойОфис Образование»

3. Для работы с ресурсами Интернет – веб-браузер Яндекс <https://yandex.ru/>.

4. Автоматизированная интерактивная система сетевого тестирования - АИССТ (зарегистрирована в РОСПАТЕНТ, Свидетельство о государственной регистрации программы для ЭВМ №2011610456, правообладатель – Оренбургский государственный университет), режим доступа – <http://aist.osu.ru>.

5. Университетская платформа электронного обучения «Электронные курсы ОГУ в системе обучения Moodle». – Режим доступа: <http://moodle.osu.ru>

6. Elibrary [Электронный ресурс]: реферативная база данных, с ограниченным доступом к полным текстам статей. – Режим доступа: <https://www.elibrary.ru/>, в локальной сети ОГУ.

7. Большая Российская энциклопедия [Электронный ресурс]: универсальная энциклопедия, содержит статьи по всем областям знаний, справочники по персоналиям, словари. – Режим доступа: <https://bigenc.ru/>

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.

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