Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

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 2023

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 № 7 от "9" марта 2023 г.

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

Исполнители:
Доцент *должность* *подпись* Е.И. Ряполова *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность *код наименование* *личная подпись* И.В. Влацкая *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
личная подпись Н.Н. Бигалиева *расшифровка подписи*

Уполномоченный по качеству факультета
личная подпись И.В. Крючкова *расшифровка подписи*

№ регистрации 152599

© Ряполова Е.И., 2023
© ОГУ, 2023

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: является систематизация и расширение знаний студентов в области целых чисел и многочленов над конечными полями, овладение методами теории чисел, имеющими криптографические приложения.

Задачи освоения дисциплины состоят в изучении теории чисел, теории многочленов над конечными полями, основ компьютерной алгебры и решении задач из перечисленных областей, востребованных криптографией.

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:** способы представления действительных чисел цепными дробями, критерии простоты и их использование для факторизации натуральных чисел, алгоритмы проверки чисел на простоту; построения больших **Уметь:** применять алгоритмы разложения чисел на множители **Владеть:** навыками применения теории чисел в криптографии и других дисциплинах

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);* *- написание реферата (Р);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю и т.п.)*	**74,75**	**74,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 5 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Повторение. Теория делимости в Z. Простые и составные числа	18	2	4		12
2	Арифметические функции	16	4			12
3	Сравнения и их свойства. Сравнения с одной переменной. Системы сравнений	24	6	6		12
4	Первообразные корни и индексы	26	6	8		12
5	Многочлены над (конечными) полями	28	8	8		12
6	Основы компьютерной алгебры	26	6	8		12
7	Криптографические приложения теории чисел и теории многочленов (обзор)	6	2			4
	Итого:	144	34	34		76
	Всего:	144	34	34		76

4.2 Содержание разделов дисциплины

Раздел №1. Повторение. Теория делимости в Z. Простые и составные числа Свойства делимости целых чисел; простые числа; решето Эратосфена; теорема Евклида о бесконечности множества простых чисел. Основная теорема арифметики о разложении целых чисел на простые сомножители; наибольший общий делитель и наименьшее общее кратное. Оценки Чебышева для функции числа простых чисел, не превосходящих x.

Раздел №2. Арифметические функции Арифметические функции: целая и дробная часть числа. Разложение числа n! на простые множители. Мультипликативные функции. Функция Эйлера и

ее свойства; сумма делителей и число делителей. Оценки среднего значения арифметических функций.

Раздел №3. Сравнения и их свойства. Сравнения с одной переменной. Системы сравнений Повторение: Числовые сравнения, их основные свойства. Вычеты и классы вычетов по модулю m; кольца классов вычетов; полная система вычетов; приведенная система вычетов. Теоремы Эйлера и Ферма. Сравнения первой степени с одним неизвестным, простейшие приемы решений. Квадратичные вычеты и невычеты; число решений сравнения: критерий Эйлера для квадратичных вычетов и невычетов. Степенные вычеты и невычеты n-ой степени; число степенных вычетов; критерий для отыскания степенных вычетов; решение двучленных сравнений с помощью вычетов. Системы сравнений; их решения. Сравнения n-ой степени по составному модулю; сведение сравнения по составному модулю к системе сравнений по простому модулю; сравнения второй степени: сведение сравнения второй степени к двучленному сравнению. Символ Лежандра и его свойства; закон взаимности квадратичных вычетов; сравнения второй степени по составному модулю.

Раздел №4. Первообразные корни и индексы Первообразные корни и индексы: показатель числа по модулю m; свойства показателей; теорема о существовании первообразного корня по простому модулю; первообразные корни по модулям p и 2p; теорема об отыскании первообразных корней; индексы по модулям p и 2p; таблицы индексов; двучленные сравнения n-ой степени; существование решений.

Раздел №5. Многочлены над (конечными) полями Повторение: 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 Z.

Раздел №6. Основы компьютерной алгебры Компьютерная алгебра (КА) как наука, ее отличительные особенности. Системы компьютерной алгебры (обзор).Представление данных в системах КА: представление целых чисел, дробей, вещественных чисел, представление полиномов. Возможности оптимизации вычислительных операций. Целые числа произвольной точности, алгоритмы для сложения, вычитания, умножения и деления. Восстановление целого числа по остаткам. Деление в модулярной арифметике. Кольцо многочленов над кольцом с единицей. Сложность умножения двух многочленов. Интерполяция многочленов.

Раздел №7. Криптографические приложения теории чисел и теории многочленов (обзор) Алгоритм RSA. Вероятностные тесты простоты. Задача разделения секрета. Алгоритм Эль-Гамаля. Псевдослучайные последовательности над полем.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Генерация простых чисел в заданном диапазоне. Методы факторизации составных чисел, алгоритмы проверки простоты натурального числа	2
2	1	Греко-китайская теорема. Восстановление целого числа по остаткам. Определение знака целого числа, представленного вектором по смешанному модулю.	2
3	3	Символ Лежандра, символ Якоби. Сравнения второй степени по составному модулю.	2
4	3	Метод Ферма нахождения больших множителей натурального числа. Задача RSA.	4

5	4	Первообразные корни и индексы. Дискретное логарифмирование	8
6	5	Значение многочлена в точке. Корни многочлена. Интерполяция многочленов. Нахождение НОД. Разложение полинома на простые множители по модулю p. Порядок многочлена.	8
7	6	Период псевдослучайной последовательности.	6
8	6	Задача о безопасном хранении ключа	2
		Итого:	34

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Виноградов И.М. Основы теории чисел [Текст] : учебник для вузов / И.М. Виноградов.- СПб.: Лань, 2009. - 176 с.

2. Вычислительно сложные задачи теории чисел [Текст] : учебное пособие / Е. А. Гречников [и др.]; Мос. гос. ун-т им. М. В. Ломоносова. - Москва : Изд-во Моск. ун-та, 2012.

5.2 Дополнительная литература

1. Колосов В.А. Теоремы и задачи алгебры, теории чисел и комбинаторики: Учеб. пособие для вузов / В.А. Колосов. - М.: Гелиос АРВ, 2001. - 256 с.

2. Матрос Д.Ш., Поднебесова Г.Б. Элементы абстрактной и компьютерной алгебры. – М.: Академия, 2004.

5.3 Периодические издания

1 Информатика и системы управления: журнал. - М. : Агентство "Роспечать", 2022
2 Вестник компьютерных и информационных технологий: журнал. - М. : Агентство "Роспечать", 2022
3 Информационные технологии: журнал. - М. : Агентство "Роспечать", 2022

5.4 Интернет-ресурсы

5.4 Интернет-ресурсы

1. www.citforum.ru/ - портал аналитических и научных статей в области информационных технологий;
2. www.rsdn.ru - сайт Российской сети разработчиков ПО, содержит статьи по современным средствам программирования;
3. «Меры и средства защиты информации от несанкционированного доступа» [Электронный ресурс]: онлайн-курс на платформе https://openedu.ru/ - «Открытое образование»/ Разработчик курса: Университет ИТМО, режим доступа: https://openedu.ru/course/mipt/ISMMAUA/?session=urfu_spring_2023
4. «Защита информации» [Электронный ресурс]: онлайн-курс на платформе https://openedu.ru/ - «Открытое образование»/ Разработчик курса: Университет ИТМО, режим доступа: https://openedu.ru/course/hse/DATPRO/?session=2022

5. «Специализация IT Fundamentals for Cybersecurity » [Электронный ресурс]: онлайн-курс на платформе https://www.coursera.org / Разработчик курса: The Hong Kong University of science and technology режим доступа: https://www.coursera.org/specializations/it-fundamentals-cybersecurity

6. Теоретико - числовые методы в крипотографии [Электронный ресурс] : электронный курс в системе Moodle / Е.И. Ряполова, Оренб. гос. ун-т. – Электрон. дан. – Оренбург: ОГУ, [2022-2023].– Режим доступа: Электронные курсы ОГУ в системе обучения moodle. – https://moodle.osu.ru/course/view.php?id=8215

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система Microsoft Windows
2. Open Office/LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Интегрированная система решения математических, инженерно-технических и научных задач PTC MathCAD 14.0
4. Система автоматизированного проектирования Autocad: Электронные лицензии для образовательных целей доступны бесплатно после регистрации аккаунта преподавателя/студента. Режим доступа: https://www.autodesk.com/education/free-software/featured
5. Среда разработки программного обеспечения на языке Object Pascal для компилятора Free Pascal: Lazarus.

Доступна бесплатно. Разработчики: Cliff Baeseman, Shane Miller, Michael A. Hess и др. Режим доступа: http://www.lazarus-ide.org/

6. Интегрированная среда разработки на Javas IntelliJ IDEA Community. Доступна бесплатно после регистрации преподавателя. Разработчик: компания JetBrains. Режим доступа: https://www.jetbrains.com/student/

6 Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерными и мультимедийными средствами. Рабочие станции студентов и преподавателя объединены в локальную компьютерную сеть с возможностью выхода в Интернет.

Лекционные занятия проводятся в аудиториях, оснащенных мультимедийным оборудованием.

Лабораторные занятия проходят в компьютерных классах, в которых установлено оборудование:

- системные блоки модели Intel Celeron;
- системные блоки модели Intel Pentium Core 2 Duo;
- мониторы модели Samsung 793 DF.