

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Оренбургский государственный университет»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«С.1.Б.40 Теоретико-числовые методы в криптографии»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность

10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №4 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация

Специалист по защите информации

Форма обучения

Очная

Год набора 2020

Рабочая программа дисциплины «С.1.Б.40 Теоретико-числовые методы в криптографии» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 1 от "31" августа 2020г.

Заведующий кафедрой

Кафедра компьютерной безопасности и математического обеспечения информационных систем

И.В. Влацкая
наименование кафедры подпись расшифровка подписи

Исполнители:

доцент

должность

Е.И. Ряполова
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

расшифровка подписи

И.В. Влацкая

Заведующий отделом комплектования научной библиотеки

личная подпись

Н.Н. Грицай
расшифровка подписи

Уполномоченный по качеству факультета

личная подпись

И.В. Крючкова
расшифровка подписи

№ регистрации 110567

1 Цели и задачи освоения дисциплины

Согласно Федеральному государственному образовательному стандарту по специальности 10.05.01 Компьютерная безопасность выпускник должен быть готов, в частности, к разработке математических моделей защищаемых процессов. Многие средства криптографической защиты базируются на теоретико-числовых методах.

В связи с этим целью 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 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *С.1.Б.12 Алгебра, С.1.Б.38 Криптографические методы защиты информации*

Постреквизиты дисциплины: *С.1.В.ОД.4 Технология построения защищенных автоматизированных систем*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: - математические основы моделирования процессов передачи данных. Уметь: - выбирать подходящие методы для решения задач профессиональной деятельности.	ОПК-1 способностью анализировать физические явления и процессы при решении профессиональных задач
Знать: - основы теории делимости в кольце целых чисел; - теорию числовых сравнений; - теорию сравнений с неизвестными; - теорию первообразных корней и методы решения задачи дискретного логарифмирования; - способы представления данных в системах компьютерной алгебры; - арифметику «длинных» чисел; - алгебру многочленов одной переменной над конечным полем; - алгоритмы проверки чисел и многочленов на простоту; - алгоритмы построения больших простых чисел; - алгоритмы разложения чисел и многочленов на множители; - алгоритмы дискретного логарифмирования в конечных циклических группах. Уметь: - находить НОД и НОК целых чисел, многочленов; - решать в целых числах линейные уравнения и их системы; - отделять простые числа в заданном диапазоне; - осуществлять факторизацию числа; - проверять числа на простоту; - решать сравнения первой степени с одним неизвестным; - решать системы сравнений первой степени с одним неизвестным; - решать	ОПК-2 способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятности, математической статистики, теории информации, теоретико-числовых методов

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
полиномиальные сравнения по простому и составному модулям; - вычислять значения символа Лежандра и символа Якоби; - строить первообразные корни по заданным модулям. Владеть: навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов; методами теории чисел и современной алгебры для решения теоретических и прикладных задач криптографии.	
Знать: - историю теории чисел и ее роль в современной криптографии; - теоретико-числовые алгоритмы, применяемые в симметричных и асимметричных системах шифрования данных Уметь: - работать с научной литературой, нормативными документами Владеть: - навыками анализа и обобщения передового опыта в сфере профессиональной деятельности	ПК-1 способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности
Знать: - связь вычислительной сложности теоретико-числовых задач и стойкости криптоалгоритмов на их основе; - криптографические приложения теории чисел. Уметь: - реализовывать основные алгоритмы; - решать с их помощью задачи в области криптографии; - осуществлять анализ вычислительной стойкости. Владеть: навыками решения прикладных криптографических задач теоретикочисловыми методами.	ПК-2 способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований
Знать: методы анализа безопасности компьютерных систем Уметь: - анализировать выбранные средства защиты данных на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности... Владеть: способами выявления угроз безопасности компьютерных систем	ПК-3 способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности
Знать: - теоретико-числовые методы защиты информации Уметь: - реализовывать алгоритмы защиты данных на основе теоретикочисловых методов Владеть: - навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов	ПК-4 способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 академических часов).

Вид работы	Трудоемкость, академических часов	
	5 семестр	всего
Общая трудоёмкость	180	180

Вид работы	Трудоемкость, академических часов	
	5 семестр	всего
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:	110,75	110,75
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 $\mathbb{Z}$. 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	36	6	8		22
5	Многочлены над (конечными) полями	40	8	8		24
6	Основы компьютерной алгебры	34	6	8		20
7	Криптографические приложения теории чисел и теории многочленов (обзор)	12	2			10
	Итого:	180	34	34		112
	Всего:	180	34	34		112

4.2 Содержание разделов дисциплины

Раздел №1. Повторение. Теория делимости в $\mathbb{Z}$. 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 $\mathbb{Z}$.

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-Гамала. 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", 2020

2 Вестник компьютерных и информационных технологий: журнал. - М. : Агентство "Роспечать", 2020

3 Информационные технологии: журнал. - М. : Агентство "Роспечать", 2020

5.4 Интернет-ресурсы

1 <https://www.coursera.org/learn/metody-i-sredstva-zashity-informacii> – «Coursera», MOOK: Методы и средства защиты информации

2 Технорма / Документ [Электронный ресурс] : [система программных продуктов] / ООО Глосис-Сервис, ФБУ КВФ Интерстандарт. – Версия 1.11.36. - Электрон. дан. и прогр. - [Москва; Санкт-Петербург], [1999–2013]. – Загл. с экрана.

3 ProQuest Dissertations & Theses A&I [Электронный ресурс] : база данных диссертаций. – Режим доступа : <https://search.proquest.com/>.

4 Web of Science [Электронный ресурс]: реферативная база данных / компания Clarivate Analytics. – Режим доступа : <http://apps.webofknowledge.com/>. – Загл. с экрана.

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. Microsoft Visual Studio – среда разработки приложений.
4. <http://www.mathnet.ru/> – общероссийский математический портал
5. <https://elibrary.ru/defaultx.asp> – российский информационный портал в области науки, технологии, медицины и образования

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.