ПП 2023

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»
Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ
Декан факультета
Миронов С. В.
_____
«15» июня 2023 г.

Рабочая программа дисциплины
Теоретико-числовые методы в криптографии

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Квалификация выпускника
Специалист по защите информации

Форма обучения
Очная

Саратов,
2023

Статус	ФИО	Подпись	Дата
Преподаватель-разработчик	Молчанов В. А.		15.06.2023 г.
Председатель НМК	Кондратова Ю. Н.		15.06.2023 г.
Заведующий кафедрой	Абросимов М. Б.		15.06.2023 г.
Специалист Учебного управления			

1. Цели освоения дисциплины

Целью освоения дисциплины является овладение теоретико-числовыми методами и алгоритмами, повышающими стойкость криптографических систем, такими как:

- методы решения систем линейных уравнений над конечными полями;
- алгоритмы арифметических операций с большими целыми числами;
- вычисления в кольцах вычетов;
- алгоритмы полиномиальной арифметики;
- алгоритмы проверки простоты целых чисел;
- методы факторизации чисел;
- алгоритмы дискретного логарифмирования;
- методы разложения многочленов на множители над конечными полями;
- вычисления, использующие эллиптические кривые.

Задачами дисциплины являются: углубление математического образования и развитие практических навыков в области прикладной математики и информатики; формирование у студентов научного представления об основных положениях, понятиях и достижениях современной теории чисел; изучение теоретических основ информатики и криптографии; освоение современных теоретико-числовых методов, обосновывающих безопасность криптосистем с открытым ключом.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к обязательной части Блока 1 «Дисциплины (Модули)» учебного плана ООП и направлена на формирование у обучающихся общепрофессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Математический анализ», «Алгебра», «Геометрия», «Математическая логика и теория алгоритмов», «Дискретная математика», «Теория информации», «Методы и средства криптографической защиты информации».

Компетенции, сформированные при изучении данной дисциплины, используются при изучении дисциплин «Введение в криптоанализ».

3. Результаты обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.	ОПК-8.1.1 знает строение мультипликативной группы колец вычетов; способы представления действительных чисел цепными дробями; основные свойства символов Лежандра и	Знать алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	Якоби; критерии простоты и их использование для факторизации натуральных чисел; алгоритмы проверки чисел на простоту; построения больших простых чисел; ОПК-8.2.1 умеет строить большие простые числа; применять алгоритмы проверки чисел на простоту; построения больших простых чисел; применять алгоритмы разложения чисел на множители; ОПК-8.3.1 владеет навыками применения теории чисел в криптографии и других дисциплинах.	конечных циклических группах Уметь применять алгоритмы проверки чисел на простоту; построения больших простых чисел; применять алгоритмы дискретного логарифмирования и разложения чисел на множители Владеть навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.
ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	ОПК-10.1.3 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; базовые понятия теории эллиптических кривых; ОПК-10.2.3 умеет эффективно производить операции с большими числами, а также в кольцах вычетов, кольцах многочленов и конечных полях; исследовать и решать сравнения в кольцах вычетов; использовать достаточные условия простоты для построения больших простых чисел; оценивать теоретическую сложность применяемых алгоритмов; ОПК-10.3.3 владеет навыками эффективного	Знать основные задачи и методы современной теории чисел и алгоритмы их применения в криптографии. Уметь корректно применять теоретико-числовой аппарат при построении симметричных и асимметричных криптографических алгоритмов. Владеть навыками программирования эффективных вычислений в кольцах вычетов и в кольцах многочленов.

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	вычисления в кольцах вычетов и в кольцах многочленов; методами построения быстрых вычислительных алгоритмов алгебры и теории чисел.	
ОПК-2.1. Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации.	ОПК-2.1.1 знает основные алгоритмы, реализующие современные математические методы защиты информации; ОПК-2.1.2 умеет применять алгоритмы, реализующие современные математические методы защиты информации; ОПК-2.1.3 владеет навыками разработки алгоритмов, реализующие современные математические методы защиты информации.	Знать основные методы современной теории чисел и принципы работы с программными средствами прикладного, системного и специального назначения Уметь использовать компьютерные технологии при построении криптографических систем на основе симметричных и асимметричных криптографических алгоритмов Владеть навыками использования эффективных вычислений в кольцах вычетов и в кольцах многочленов при работе с программными средствами прикладного, системного и специального назначения.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Лабораторные занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	5	6	7	8	9	10
1	Арифметические операции	9	1	2	2	–	–	2	Опрос на 2-й неделе

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Лабораторные занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	5	6	7	8	9	10
	над целыми числами и многочленами								
2	Непрерывные дроби		2	2	2	–	–	2	Опрос на 3-й неделе
3	Квадратичные вычеты		3	2	2	–	–	2	Опрос на 4-й неделе
4	Дискретное преобразование Фурье		4	2	2	–	–	2	Опрос на 5-й неделе
5	Решение систем линейных уравнений над конечными полями		5	2	2	–	2	2	Опрос на 6-й неделе
6	Проверка чисел на простоту		6-7	4	4	–	–	2	Опрос на 7-й неделе
7	Построение больших простых чисел		8	2	2	–	–	2	Опрос на 8-й неделе
8	Факторизация целых чисел		9-10	4	4	–	–	4	Опрос на 10-й неделе
9	Применение эллиптических кривых для проверки простоты и факторизации целых чисел.		11-12	4	4	–	–	4	Опрос на 12-й неделе
10	Дискретное логарифмирование в конечном поле.		13-14	4	4	–	–	4	Опрос на 14-й неделе
11	Факторизация		15-16	4	4	–	–	4	Опрос на 16-

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Лабораторные занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	5	6	7	8	9	10
	многочленов над конечными полями								й неделе
12	Элементы теории решеток		17–18	4	4	–	2	2	*Контрольная работа* на 17-й неделе
	Промежуточная аттестация - 36								**Экзамен**
	ИТОГО – 108ч.			**36**	**36**	**–**	**4**	**32**	

Содержание дисциплины

Арифметические операции над целыми числами и многочленами. Сложность арифметических операций. Свойства функции оценки сложности. Сложность арифметических операций с целыми числами. Сложность алгоритма Евклида. Сложность операций в кольце вычетов. Приложения модулярной арифметики.

Непрерывные дроби. Определение непрерывной дроби. Подходящие дроби, свойства подходящих дробей. Представление действительных чисел непрерывными дробями. Приложения непрерывных дробей.

Квадратичные вычеты. Определение квадратичного вычета. Задачи существования квадратичных вычетов и вычисления квадратных корней. Определение и свойства символов Лежандра и Якоби. Вычисление квадратных корней по простому модулю. Вычисление квадратных корней по составному модулю. Целые числа Блюма. Генератор псевдослучайных чисел BBS. Вероятностное шифрование.

Дискретное преобразование Фурье. Определение и свойства дискретного преобразования Фурье. Вычисление дискретного преобразования Фурье. Дискретное преобразование Фурье и умножение многочленов. Дискретное преобразование Фурье и деление многочленов. Применение дискретного преобразования Фурье в алгоритме Полларда-Штрассена

Решение систем линейных уравнений над конечными полями. Решение систем линейных уравнений методом Гаусса. Алгоритм Ланцоша. Алгоритм Видемана.

Проверка чисел на простоту. Распределение простых чисел. Элементарные методы проверки простоты чисел. Решето Эратосфена. Критерий Вильсона. Тест на основе малой теоремы Ферма. Свойства чисел Кармайкла. Тест Соловея-Штрассена. Тест Рабина-Миллера. Полиномиальный тест распознавания простоты.

Построение больших простых чисел. Критерий Люка. Теорема Поклингтона. Теорема Диемитко. Метод Маурера. Метод Михалеску. (n+1)-методы. Числа Мерсенна.

Факторизация целых чисел. Метод Ферма. ρ-1- метод Полларда. ρ-метод Полларда. Алгоритм Полларда-Штрассена. Методы Шенкса. Алгоритм Диксона. Алгоритм Брилхарта-Моррисона. Метод квадратичного решета.

Применение эллиптических кривых для проверки простоты и факторизации целых чисел. Эллиптические кривые и их свойства. Алгоритм Ленстры для факторизации целых чисел с помощью эллиптических кривых. Вычисление порядка группы точек эллиптической кривой над конечным полем. Тестирование чисел на простоту с помощью эллиптических кривых.

Дискретное логарифмирование в конечном поле. Задача дискретного логарифмирования в конечном поле. Протокол Диффи – Хеллмана. Алгоритм Гельфонда. Алгоритм Полига – Хеллмана. Алгоритм Хеллмана – Рейнери. ρ-метод Полларда для дискретного логарифмирования.

Факторизация многочленов над конечными полями. Вероятностный алгоритм решения алгебраических уравнений в конечных полях. Алгоритм Берлекэмпа. Метод Кантора – Цассенхауза. Вероятностный алгоритм проверки неприводимости многочленов над конечными полями.

Элементы теории решеток. Решетки и базисы. Процесс ортогонализации Грама-Шмидта. Алгоритм Ленстры-Ленстры-Ловаша. Задача об укладке ранца. Ранцевые алгоритмы шифрования с открытым ключом.

План лабораторных занятий

На лабораторных занятиях студенты под руководством преподавателя самостоятельно выполняют задания лабораторных работ с практической реализацией основных теоретико-числовых алгоритмов в форме компьютерных программ с использованием языков программирования высокого уровня.

№ занятия	Тема	Задания для лабораторного практикума
1	**2**	**3**
1-2	Арифметические операции над целыми числами и многочленами	№1
3	Непрерывные дроби	№2
4	Квадратичные вычеты	№3
5-6	Дискретное преобразование Фурье	№4
7	Решение систем линейных уравнений над конечными полями	№ 5
8-9	Проверка чисел на простоту	№ 6

№ занятия	Тема	Задания для лабораторного практикума
1	**2**	**3**
10	Построение больших простых чисел	№ 7
11-12	Факторизация целых чисел.	№ 8
13-14	Дискретное логарифмирование в конечном поле.	№ 9
15-16	Факторизация многочленов над конечными полями	№ 10
17-18	Элементы теории решеток	№ 11

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе следующих образовательных технологий:

1) организационная технология балльно-рейтингового обучения;

2) проектная творческая и научно-исследовательская деятельность, знакомство с образовательными ресурсами научно-исследовательской библиотеки СГУ и с Интернет-ресурсами;

3) активизация работы обучающихся с различными информационным технологиям, включая мультимедийные лекции и лабораторные занятия в компьютерной лаборатории.

Иная контактная работа представляет собой индивидуальные консультации, оказываемые очно и дистанционно с использованием информационных и телекоммуникационных технологий с учётом образовательных возможностей обучающихся.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве. При этом основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья, т.е. все студенты обучаются в смешенных группах, имеют возможность постоянно общаться со сверстниками, благодаря чему легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

В рамках самостоятельной работы студенты:

1) Изучают дополнительную литературу по предмету.

2) Детально рассматривают изучаемый материал по соответствующим разделам дисциплины, ссылки на источники для самостоятельной работы студентов даются при чтении лекций.

3) Выполняют задания по лабораторным работам.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для лабораторных занятий и методические указания по их выполнению, варианты заданий для контрольной работы, тесты, контрольные вопросы, вопросы для проведения промежуточной аттестации (экзамен). Фонд оценочных средств оформлен в качестве приложения к учебной рабочей программе дисциплины «Теоретико-числовые методы в криптографии».

7. Данные для учета успеваемости студентов в БАРС

Таблица 1 – Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
9	5	30	0	15	0	20	30	**100**

Программа оценивания учебной деятельности студента

9 семестр

Лекции

Посещаемость за один семестр – от 0 до 5 баллов.

Лабораторные занятия

Самостоятельность при выполнении работы, активность работы в аудитории, правильность выполнения заданий, уровень подготовки к занятиям – от 0 до 30 баллов.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Оценивается качество выполнение заданий в рамках самостоятельной работы, хорошие отчеты о проделанной работе – от 0 до 15 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Контрольная работа – от 0 до 20 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой устный *экзамен.*

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 21 до 30 баллов;

ответ на «хорошо» оценивается от 11 до 20 баллов;

ответ на «удовлетворительно» оценивается от 6 до 10 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 5 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за девятый семестр по дисциплине «Теоретико-числовые методы в криптографии» составляет **100** баллов.

Таблица 2.2 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Теоретико-числовые методы в криптографии» в оценку (экзамен)

86-100 баллов	«отлично»
71-85 баллов	«хорошо»
50-70 баллов	«удовлетворительно»
0-49 баллов	«неудовлетворительно»

8. Учебно-методическое и информационное обеспечение дисциплины

а) литература:

1) Введение в теоретико-числовые методы криптографии [Электронный ресурс] : учеб. пособие / М. М. Глухов [и др.]. - Москва : Лань, 2022. - 394 с. : табл. - (Учебники для вузов. Специальная литература). - ISBN 978-5-8114-1116-0 : Б. ц. URL: https://e.lanbook.com/book/1540. Загл. с экрана. Яз. рус.

2) Бухштаб, А. А. Теория чисел [Электронный ресурс] : учеб. пособие / А. А. Бухштаб. - Москва : Лань", 2022. - 384 с. : ил. ; 21 см. - (Классическая учебная литература по математике) (Учебники для вузов. Специальная литература). - Библиогр. в тексте. - ISBN 978-5-8114-0847-4 : Б. ц. URL: https://e.lanbook.com/book/65053. Загл. с экрана. Яз. рус.

3) Молдовян, А. А. Криптография [Текст] : учебное пособие / А. А. Молдовян, Н. А. Молдовян, Б. Я. Советов. - Санкт-Петербург : Лань, 2001. - 218, [6] с. : ил. - (Учебники для вузов. Специальная литература). - Библиогр. - ISBN 5-8114-0246-5 (в пер.).

4) Черемушкин, А. В. Лекции по арифметическим алгоритмам в криптографии [Текст] : учеб. пособие / А. В. Черемушкин. - Москва : МЦНМО, 2002. - 103, [1] с. - Библиогр.: с. 100-103 (59 назв.). - ISBN 5-94057-060-7.

б) программное обеспечение и Интернет-ресурсы:

1) Лицензионное программное обеспечение: Visual C++ 4.2, Visual Studio 2010, Visual Studio 2012, Visual Studio 2013, Visual Studio 2015

2) Свободное программное обеспечение: Java Developers Kit, NetBeans IDE, Eclipse, CPython, Jython, IronPython.

9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходима лекционная аудитория с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения лабораторных занятий необходим компьютерный класс со стандартным программным обеспечением и доступом к сети Интернет.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 Компьютерная безопасность, специализация «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

Автор

Профессор кафедры теоретических основ компьютерной безопасности и криптографии доктор физико-математических наук, профессор В. А. Молчанов

Программа одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «15» июня 2023 года, протокол № 14.