

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

21 мая 2024 г.

Рабочая программа дисциплины

Методы защиты информации

Направление подготовки (специальности)
02.04.01 Математика и компьютерные науки

Направленность (профиль)
«Компьютерная математика»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 12 апреля 2024 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2024 г.

1. Цели освоения дисциплины

Целью освоения дисциплины является знакомство с основами криптографических методов защиты информации. В курсе изучаются симметричное шифрование и шифрование с открытым ключом. Рассматриваются примеры криптографических систем, решающих те или иные криптографические задачи.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Методы защиты информации» относится к части образовательной программы, формируемой участниками образовательных отношений, и является элективной дисциплиной. Для освоения желательны базовые знания по курсу «Теории чисел».

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
Профессиональные компетенции		
ПК-2 Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования	И-ПК-2.1 Владеет современными методами разработки и реализации алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования И-ПК-2.2 Умеет разрабатывать и реализовывать алгоритмы математических моделей на базе языков и пакетов прикладных программ моделирования И-ПК-2.3 Имеет практический опыт разработки и реализации алгоритмов на базе языков и пакетов прикладных программ моделирования	Знать: - основные понятия и теоремы теории чисел, понятие делимости, свойства делимости, арифметику остатков, алгоритм Евклида, расширенный алгоритм Евклида, кольцо вычетов и его свойства, понятие сравнения, асимптотический закон распределения простых чисел. - основные задачи, возникающие в криптографии. - симметричные системы шифрования, системы шифрования с открытым ключом Уметь: - решать задачи на делимость целых чисел, применять алгоритм Евклида, расширенный алгоритм Евклида, проводить вычисления в кольце вычетов, - решать некоторые типы сравнений и систем сравнений, применять основные криптографические системы для шифрования данных Владеть навыками: применения изученного математического аппарата для решения задач теории чисел, шифрования с помощью основных криптографических протоколов

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **3** зачетных единиц, **108** акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа					самостоятельная работа	
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Основы теории чисел. Делимость. Свойства	1	2	2				10	Домашняя работа
2	Простые числа. Основная теорема арифметики. Асимптотический закон распределения простых чисел	1	2	2				8	Домашняя работа
3	Кольца вычетов. Теория сравнений	1	2	2				8	Домашняя работа
4	Основные понятие криптографии. Симметричное шифрование и шифрование с открытым ключом	1	2	2				8	Домашняя работа
5	Криптосистемы Диффи- Хэллмана, Шамира, Эль- Гамала, RSA	1	2	2				10	Домашняя работа
6	Протоколы электронной подписи	1	2	2				10	Домашняя работа
7	Протоколы идентификации	1	2	2		2		8	Домашняя работа
8	Электронные деньги	1	2	2		2		8	Домашняя работа
							0,3	1,7	зачет
	ИТОГО		16	16		4	0.3	71,7	

Содержание разделов дисциплины:

Тема 1. Основы теории чисел. Делимость. Свойства

Основы теории чисел. Свойства делимости. Деление с остатком. Алгоритм Евклида. Расширенный алгоритм Евклида.

Тема 2. Простые числа. Основная теорема арифметики. Асимптотический закон распределения простых чисел

Простые числа. Основная теорема арифметики. Числовые мультипликативные функции. Асимптотический закон распределения простых чисел

Тема 3. Кольца вычетов. Теория сравнений

Группы, кольца, поля. Кольца вычетов. Свойства. Обратимые элементы и делители нуля. Первообразные корни. Функция Эйлера и ее свойства. Сравнения по модулю. Общие свойства сравнений. Решение линейных сравнений с одним неизвестным. Системы линейных

сравнений. Китайская теорема об остатках. Квадратичные сравнения. Вычеты и невычеты. Символ Лежандра и символ Якоби.

Тема 4. Основные понятия криптографии. Симметричное шифрование и шифрование с открытым ключом

Основные понятия криптографии. Симметричное шифрование и шифрование с открытым ключом. Классические шифры. Современные симметричные шифры.

Тема 5. Криптосистемы Диффи-Хэллмана, Шамира, Эль-Гамала, RSA

Тема 6. Протоколы электронной подписи

Протоколы электронной подписи, основанные на различных криптосистемах.

Тема 7. Протоколы идентификации

Тема 8. Электронные деньги

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:
для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- издательская система LaTeX;
- Adobe Acrobat Reader.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»

http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

- Электронная библиотечная система «Лань» <https://e.lanbook.com>

- Электронная библиотечная система «Юрайт» <https://urait.ru>

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Мартынов, Л. М. Алгебра и теория чисел для криптографии / Л. М. Мартынов. — 3-е изд., стер. — Санкт-Петербург : Лань, 2024. — 456 с. — ISBN 978-5-507-48774-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/362942>
2. Масленников М. Е. Практическая криптография. / М. Е. Масленников - СПб.: БХВ-Петербург, 2003. - 456с.

б) дополнительная литература

1. В. В. Яценко Введение в криптографию - М.: МЦНМО: «ЧеРо», 2000. https://library.samdu.uz/files/5ef5e9f7c2b02d90200f92776db5bbc3_Введение_в_криптографию_by_Под_общ_ред_Яценко_В_В_2012.pdf
2. Венбо Мао. Современная криптография. Теория и практика – М.: Вильямс, 2005. <https://djvu.online/file/OKDfqIc1p9QY2?ysclid=lldts8a0dq404612198>
3. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В Основы криптографии. - М. Гелиос АРВ, 2002
<https://djvu.online/file/BIEH6b3hL9cCn?ysclid=lldtrczj6h239172333>

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор(ы):

Доцент кафедры алгебры и математической логики,
к.ф.-м.н.

М.А. Заводчиков

**Приложение № 1 к рабочей программе дисциплины
«Методы защиты информации»**

**Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине**

**1. Типовые контрольные задания и иные материалы,
используемые в процессе текущего контроля успеваемости**

Задания для самостоятельной работы

1. Число n не делится на 3. Делится ли число $2n$ на 3?
 2. Число n четно. Верно ли, что число $3n$ делится на 6?
 3. Число $15n$ делится на 6. Верно ли, n делится на 6?
 4. Целые числа m и n таковы, что $m + 3n$ делится на 13. Докажите, что $11m + 7n$ делится на 13.
 5. В ряд записаны числа $1, \dots, n$. Можно ли между ними поставить знаки плюс или минус так, чтобы значение выражения равнялось 0?
 6. При каких n число $(n-1)!$ делится нацело на n .
 7. Докажите, что при любом натуральном n число $7n - 1$ делится на 6.
 8. Докажите, что при любом натуральном n число $5n + 3$ делится на 4.
 9. Докажите, что при любом четном натуральном n число $7n - 5n$ делится на 24.
 10. Докажите, что $5n + 8n - 2n+1$ делится на 3 при любом натуральном n .
 11. Докажите, что $1n + 3n + 5n + 7n$ делится на 4 при любом натуральном n .
 12. Докажите, что $13 + 23 + \dots + 993$ делится на 100.
 13. Докажите, что если $a^3 + b^3 + c^3$ делится на 7 ($a, b, c \in \mathbb{Z}$), то abc делится на 7.
 14. Докажите, что число, имеющее нечётное число делителей - точный квадрат.
 15. Известно, что $ab + cd$ делится на $a + c$. Докажите, что $ad + bc$ делится на $a + c$.
-
1. Найдите НОД и НОК чисел а) $29 \cdot 33 \cdot 54$ и $23 \cdot 32 \cdot 72$.
 2. Найдите НОД(324,576). Найдите НОК. Найдите линейное представление.
 3. Найдите НОД(1024,576). Найдите НОК. Найдите линейное представление.
 4. Найдите НОД(5040,2184). Найдите НОК. Найдите линейное представление.
 5. Найдите НОД(30030,34969). Найдите НОК. Найдите линейное представление.
 6. Найдите НОД(324,576,144). Найдите НОК.
 7. Найдите НОД(324,576,30030). Найдите НОК.
 8. Найдите НОД(324,576,30030,34969). Найдите НОК.
 9. Число $a = 1775 + 30621 \cdot 1733 - 1735$, число $b =$
 10. При каких натуральных n будут взаимно простыми числа $7n+6$ и $2n+3$?
 11. Существует ли такая пара целых чисел x и y , что $6x + 8y = 1$?
 12. Докажите, что два нечетных последовательных числа взаимно просты.
 13. Доказать, что если $(a, b) = 1$, то или $(a+b, a-b) = 1$, или $(a+b, a-b) = 2$.
 14. Дробь ba несократима. Будет сократимой дробь $aa+b$?

15. Докажите, что $(a, b) = (5a + 3b, 13a + 8b)$.
16. Докажите, что наименьшее общее кратное чисел $1, 2, \dots, 2n$ равно наименьшему общему кратному чисел $n + 1, n + 2, \dots, 2n$.
1. Найдите все простые числа, которые отличаются на 17.
2. Докажите, что любое простое число, большее 3, можно записать в одном из двух видов: $6n + 1$ либо $6n - 1$, где n – натуральное число.
3. Является ли число $49 + 610 + 320$ простым?
4. Докажите, что $p^2 - 1$ делится на 24, если p – простое число и $p > 3$.
5. Найдите все простые числа, меньшие 150.
6. Найдите все простые числа от 150 до 250.
7. Укажите интервал длиной 100, в котором нет простых чисел.
8. Является ли число 1231 простым?
9. Является ли 1423 простым?
10. Существуют ли а) 5, б) 6 простых чисел, образующих арифметическую прогрессию?
11. Докажите, что 3, 5 и 7 являются единственной тройкой простых чисел-близнецов.
12. Существует ли такое число n , что $n - 1996, n, n + 1996$ – простые?
13. Верно ли, что многочлен $f(n) = n^2 + n + 41$ принимает только простые значения.
14. Найдите все простые числа, которые нельзя записать в виде суммы двух составных.
15. Три простых числа p, q, r , большие 3, образуют арифметическую прогрессию.

1. В кольце Z_{24} перечислите все обратимые элементы. Найдите все пары взаимно обратных элементов. Выпишите делители нуля.
2. В кольце Z_{45} найдите обратный элемент к элементу 17.
3. В кольце Z_{196} найдите обратный элемент к элементу 73.
4. В кольце Z_{841} найдите обратный элемент к элементу 91.
5. В кольце Z_{841} найдите обратный элемент к элементу 7.
6. Образует ли множество делителей нуля группу относительно сложения?
7. Образует ли множество делителей нуля группу относительно умножения?
8. Может ли произведение обратимого класса вычетов на необратимый класс вычетов быть обратимым?

1. Решить сравнение $2x \equiv -5 \pmod{3}$,
2. Решить сравнение $6x \equiv 39 \pmod{51}$,
3. Решить сравнение $93x \equiv 2 \pmod{17}$,
4. Решить сравнение $2x \equiv 3 \pmod{6}$,
5. Решить сравнение $24x \equiv 18 \pmod{36}$,
6. Решить сравнение $12x \equiv 7 \pmod{16}$,
7. Решить сравнение $12x \equiv 5 \pmod{13}$,
8. Решить сравнение $12x \equiv 8 \pmod{16}$,
9. Решить сравнение $x^2 - 2x + 3 \equiv 0 \pmod{4}$,
10. Решить сравнение $x^5 - 2x^3 + 13x - 1 \equiv 0 \pmod{4}$,
11. Решить сравнение $5x^2 + x + 4 \equiv 0 \pmod{10}$,
12. Решить сравнение $x^2 \equiv 1 \pmod{3}$,
13. Решить сравнение $x^3 \equiv 1 \pmod{4}$,
14. Докажите теорему: сравнение $f(x) \equiv 0 \pmod{p}$ степени $n \geq p$ равносильно сравнению $g(x) \equiv 0 \pmod{p}$, где $g(x)$ – остаток от деления $f(x)$ на $x^p - x$.

15. Примените предыдущую задачу для решения сравнений:

a) $x^5 + 2x^4 - 2x^3 - 2x^2 + 2x - 1 \equiv 0 \pmod{3}$,

b) $x^7 - 3x^6 + x^5 - x^3 + 4x^2 - 4x + 2 \equiv 0 \pmod{5}$,

c) $x^{14} - x^{13} - x^2 + 2x + 1 \equiv 0 \pmod{13}$.

Самостоятельная работа 1

(проверка сформированности ПК-2, индикатор ИД-ПК-2_1)

1. Используя шифр Цезаря зашифруйте фразу КРИПТОГРАФИЯ.
2. Используя таблицу Виженера зашифруйте фразу КРИПТОГРАФИЯ.
3. Используя гаммирование по модулю 2, зашифруйте число 25 с ключом 13.
4. Используя гаммирование по модулю 2, зашифруйте слово КРИПТОГРАФИЯ с ключом 100(можно использовать стандартную кодировку символов Windows).
5. Разбив сообщение на блоки длины 4, зашифруйте сообщение КРИПТОГРАФИЯ с помощью перестановки (2314).

Самостоятельная работа 2

(проверка сформированности ПК-2, индикатор ИД-ПК-2_2)

1. Найти все допустимые варианты выбора параметра g в системе Диффи-Хеллмана при $p = 11$.
2. Вычислить секретные ключи Y_A , Y_B и общий ключ Z_{AB} для системы Диффи-Хеллмана с параметрами: $p = 23$, $g = 5$, $X_A = 5$, $X_B = 7$.
3. Для шифра Шамира с заданными параметрами p , s_A , s_B найти недостающие параметры и описать процесс передачи сообщения m от A к B : $p = 19$, $s_A = 5$, $s_B = 7$, $m = 4$.
4. Для шифра Эль-Гамала с заданными параметрами p , g , s_B , k найти недостающие параметры и описать процесс передачи сообщения m пользователю B : $p = 19$, $g = 2$, $s_B = 5$, $k = 7$, $m = 5$.

Самостоятельная работа 3

(проверка сформированности ПК-2, индикатор ИД-ПК-2_3)

1. В системе RSA с заданными параметрами P_A , Q_A , d_A найти недостающие параметры и описать процесс передачи сообщения m пользователю A : $P_A = 5$, $Q_A = 11$, $d_A = 3$, $m = 12$.
2. Пользователю системы RSA с параметрами $N = 187$, $d = 3$ передано зашифрованное сообщение $e = 100$. Расшифровать это сообщение, взломав систему RSA пользователя.
3. Абоненты некоторой сети применяют подпись Эль-Гамала с общими параметрами $p = 23$, $g = 5$. Для указанных секретных параметров абонентов найти открытый ключ u и построить подпись для сообщения m : $x = 11$, $k = 3$, $m = h = 15$.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Зачет выставляется по результатам контрольной работы при условии правильного решения студентом не менее 70% всех заданий.

Пример зачетной контрольной работы.

Часть I

1. Найдите остаток от деления числа 310000 на 13.
2. Выпишите все делители нуля в кольце Z_{24} . Выпишите все обратимые элементы.
3. Найдите обратный элемент к 41 в кольце Z_{136} .
4. Вычислите значение функции Эйлера $\phi(1156)$.

5. Найдите две последние цифры числа 171000, пользуясь функцией Эйлера.

Часть II

1. Вычислить секретные ключи Y_A , Y_B и общий ключ Z_{AB} для системы Диффи–Хеллмана с параметрами:

$p = 17$, $g = 3$, $X_A = 10$, $X_B = 5$.

2. Для шифра Эль-Гамала с заданными параметрами p , g , s_B , k найти недостающие параметры и описать процесс передачи сообщения m пользователю В:

$p = 23$, $g = 7$, $s_B = 3$, $k = 15$, $m = 5$.

3. В системе RSA с заданными параметрами P_A , Q_A , d_A найти недостающие параметры и описать процесс передачи сообщения m пользователю А:

$P_A = 7$, $Q_A = 13$, $d_A = 5$, $m = 30$.

4. Для указанных открытых ключей у пользователей системы Эль-Гамала с общими параметрами $p = 19$, $g = 7$ проверить подлинность подписанных сообщений:

а. $y = 6$: $(5, 17, 1)$, $(5, 11, 3)$, $(5, 17, 10)$.

**Приложение № 2 к рабочей программе дисциплины
«Методы защиты информации»**

Методические указания для студентов по освоению дисциплины

В магистратуру студенты приходят с разной алгебраической подготовкой. Поэтому первая часть курса посвящена математическим основам. От студентов требуется качественно прорешивать задачи домашней работы. Все темы по теории чисел, включенные в курс, содержательно используются во второй части курса. Основной формой изложения являются лекции. На практических занятиях разбираются типовые задачи по соответствующей теме.