

Министерство науки и высшего образования
Российской Федерации

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

Факультет математики и информационных технологий
Кафедра прикладной математики и теории систем управления



П.А. Машаров

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Укрупненная группа направлений
подготовки
Программа высшего образования
Направление подготовки

Магистерская программа

Квалификация
Форма обучения

02.00.00 Компьютерные и
информационные науки
Программа магистратуры
02.04.02 Фундаментальная информатика и
информационные технологии
Фундаментальная информатика и
информационные технологии
Магистр
Очная


Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины **«Математические основы защиты информации и информационной безопасности»** для обучающихся по направлению подготовки 02.04.02 Фундаментальная информатика и информационные технологии (Магистерская программа: Фундаментальная информатика и информационные технологии), составлена на основании Федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 02.04.02 Фундаментальная информатика и информационные технологии, утвержденного приказом Министерства образования и науки Российской Федерации от 23 августа 2017 г. № 811 (с изм. и доп.), Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06 апреля 2021 г. № 245 (с изм. и доп.), в соответствии с учебным планом, утвержденным Ученым советом ФГБОУ ВО «ДонГУ» для набора 2024 года.

Разработчик:

доцент кафедры прикладной математики и теории систем управления

 Л.А. Рыбалко

Рабочая программа одобрена на заседании кафедры прикладной математики и теории систем управления.

Протокол от 26.03.2024 г. № 8

Заведующий кафедрой



Д.В. Шевцов

СОГЛАСОВАНО:

Декан факультета математики и информационных технологий
28.03.2024 г.



И.А. Моисеенко

Учебно-методическая комиссия факультета математики и информационных технологий.

Протокол от 28.03.2024 г. № 3.

Председатель



Л. И. Селякова

Руководитель основной профессиональной образовательной программы,
д-р техн. наук, доц.
26.03.2024 г.



Д.В. Шевцов

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Требования к предварительной подготовке обучающихся, предшествующие и сопутствующие дисциплины, на которых основывается изучение данной:

базовая подготовка по математике в объеме программы средней школы;

дисциплины программы бакалавриата: Дискретная математика, Основы программирования, Введение в объектно-ориентированное программирование, Языки программирования, Прикладные информационные технологии 1-8, Математические модели в информационных технологиях 1-8.

1.2. Дисциплины, курсовые работы и практики, для которых освоение данной дисциплины необходимо как предшествующее:

Производственная практика: научно-исследовательская работа (обязательная),
Производственная практика: преддипломная практика (обязательная), написание магистерской диссертации.

2. ОПИСАНИЕ ДИСЦИПЛИНЫ

2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	02.04.02 Фундаментальная информатика и информационные технологии (Магистерская программа: Фундаментальная информатика и информационные технологии)
Шифр и название в соответствии с учебным планом	Б1.Б.4. Математические основы защиты информации и информационной безопасности
Часть образовательной программы	Базовая часть
Количество зачетных единиц / всего часов	6/ 216

2.2. Распределение часов по периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы+контроль	всего	
Очная	2	3	17	51		148	216	экзамен

3. ЦЕЛИ ДИСЦИПЛИНЫ

Углубленная подготовка в области криптографии, основных классов асимметричных криптографических систем; овладение навыками компьютерной реализации алгоритмов защиты информации; овладение современным математическим аппаратом для дальнейшего использования в науке и приложениях; формирование у студентов научного подхода.

4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ КОМПОНЕНТА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, ИХ ИНДИКАТОРЫ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

4.1. Компетенции

ОПК-1. Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий.

4.2. Индикаторы компетенций

ОПК-1.1. Применяет классические и современные математические методы для решения фундаментальных и прикладных задач, связанных с криптографической защитой информации.

4.3. Результаты обучения

ОПК-1.1.1. Знает определения и утверждения, методы решения задач, современные алгоритмы криптографических систем, применяемые для решения профессиональных задач.

ОПК-1.1.2. Умеет выбирать и использовать необходимые математические методы и вычислительные средства, решать задачи дисциплины (алгоритмы быстрого возведения в степень, факторизации чисел, вычисления дискретного логарифма и других математических задач).

ОПК-1.1.3. Аргументированно выбирает алгоритм решения задачи, устанавливает свойства математических объектов, закономерности между ними, доводит решение задачи до числового результата, оценивает и анализирует полученный результат, строит математические модели для решения профессиональных задач.

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
Введение в информационную безопасность	Основные понятия, методы, сервисы и угрозы информационной безопасности. Классификация криптографических методов защиты информации.
Системы шифрования с открытым ключом. Метод RSA	Особенности систем с открытым ключом. Модулярная арифметика. Функция Эйлера $\varphi(n)$. Алгоритм RSA. Расширенный алгоритм Евклида. Алгоритм быстрого возведения в степень по модулю. Генерация простых чисел. Решето Эратосфена. Метод пробных делений. Решето Аткина. Тест Покинтона. Символ Лежандра. Тест простоты Миллера–Рабина.
Криптостойкость RSA. Алгоритмы факторизации	Метод Ферма. $(p - 1)$ –метод Полларда. $(p + 1)$ –метод Вильямса. p –метод Полларда. p –метод Полларда для вычисления дискретного логарифма
Криптографические методы, основанные на задаче дискретного логарифмирования в конечном поле	Протокол Диффи–Хеллмана. Электронная цифровая подпись и ее свойства. Односторонние функции. Хеш-функции. Алгоритм создания электронной цифровой подписи. Алгоритм построения ЭЦП Эль-Гамала
Эллиптические кривые и их приложения в криптографии	Определение эллиптической кривой. Эллиптические кривые в проективных координатах. Эллиптические кривые в якобиановых проективных координатах. Число точек эллиптической кривой. Алгоритм факторизации Ленстры ECF. Рекордные разложения метода ECFM

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6.1. Форма обучения – очная, курс – 2, семестр – 3

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Введение в информационную безопасность	2	2		9	13
Системы шифрования с открытым ключом. Метод RSA	4	12		31	47
Криптостойкость RSA. Алгоритмы факторизации	4	14		37	55
Криптографические методы, основанные на задаче дискретного логарифмирования в конечном поле	3	10		29	42
Эллиптические кривые и их приложения в криптографии	4	13		42	59
ИТОГО ПО КОМПОНЕНТУ ОПОП	17	51		148	216

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Контрольные вопросы

- Основные понятия, методы, сервисы и угрозы информационной безопасности.
- Классификация криптографических методов защиты информации.
- Особенности систем с открытым ключом. Модулярная арифметика. Функция Эйлера $\varphi(n)$.
- Алгоритм RSA.
- Простые числа. Теорема о бесконечном множестве простых чисел. Оценка распределения простых чисел на множестве натуральных чисел.
- Тесты Ферма и Соловея-Штрассена простоты чисел.
- Тест Миллера-Рабина простоты чисел.
- Алгоритм Евклида для нахождения наибольшего общего делителя. Расширенный алгоритм Евклида.
- Бинарные алгоритмы вычисления степени большого числа.
- Генерация простых чисел. Решето Эратосфена. Метод пробных делений.
- Китайская теорема об остатках.
- Квадратичные вычеты.
- Алгоритмы разложения большого числа на множители. Эвристики Флойда и Брента.
- Метод Ферма. $(p - 1)$ -метод Полларда.
- $(p + 1)$ -метод Вильямса. p -метод Полларда.
- Определение дискретного логарифма.
- Алгоритмы вычисления квадратного корня.
- Математические основы криптосистем на эллиптических кривых.
- Выбор параметров эллиптической кривой.
- Определение эллиптической кривой. Эллиптические кривые в проективных координатах.
- p -метод Полларда для вычисления дискретного логарифма.
- Протокол Диффи-Хеллмана. Электронная цифровая подпись и ее свойства.
- Односторонние функции. Хеш-функции.
- Алгоритм создания электронной цифровой подписи. Алгоритм построения ЭЦП Эль-Гамала.
- Число точек эллиптической кривой.
- Алгоритм факторизации Ленстры ECF

7.2. Темы индивидуальных заданий (примеры)

Пункт 1 – реферат.

Пункты 2 - 4 содержат теоретическую часть и программную реализацию в виде исполнимого под управлением ОС Windows *.exe-файла.

Время выполнения каждого пункта – 2 неделя.

В конце срока выполнения предоставляется полный отчет о задании.

Индивидуальное задание №1

1. Введение в информационную безопасность.
 - а) Основные понятия информационной безопасности.
 - б) Методы и сервисы информационной безопасности.
2. Алгоритмы модулярной арифметики.
 - а) Алгоритм Евклида. Расширенный алгоритм Евклида и вычисление обратных по модулю величин.
3. Генерация простых чисел
 - а) Решето Эратосфена.
 - б) Вероятностный тест простоты Соловея–Штрассена.
4. Алгоритмы факторизации.
 - а) $(p-1)$ -метод Полларда (первая и вторая стадии)

Индивидуальное задание №2

Криптосистемы на эллиптических кривых.

1. Математические основы.
2. Выбор параметров кривой.
3. Построение криптосистем. Алгоритмы эффективной реализации операций.
4. Программная реализация.

7.3. Темы письменных работ (типы задач)

Контрольные работы по темам:

Вычислите $\varphi(7)$, $\varphi(15)$, $\varphi(64)$, $\varphi(64 \cdot 27 \cdot 11)$.

Вычислите НОД(16, 24), НОД(161, 242).

Решите уравнения $37x + 10y = 1$; $25x + 44y = 1$

Вычислите $2^{27} \bmod 1729$; $5^{27} \bmod 1729$

Вычислить обратную величину с помощью расширенного алгоритма Евклида и с использованием функции Эйлера: $5^{-1} \bmod 28$; $6^{-1} \bmod 43$

С помощью критерия примитивности и простоты проверить на простоту число 143.

С помощью теста Миллера–Рабина проверить на простоту число 257 с количеством проверок $r=4$.

Используя тесты Поклингтона и Миллера–Рабина проверить на простоту число 815183.

Вычислить символы Лежандра: $\left(\frac{15}{5}\right)$; $\left(\frac{15}{7}\right)$; $\left(\frac{3}{6}\right)$; $\left(\frac{79}{11}\right)$

Используя методы Ферма, $(p-1)$ -метод Полларда, $(p+1)$ -метод Вильямса и p -метод Полларда выполнить пробное разложение числа 7967 на множители.

Вычислить $\log_3 15 \bmod 17$.

Решить уравнение $3^x = 15 \bmod 43$.

Контрольная работа по проверке теоретических знаний – по всем темам, с использованием указанных выше контрольных вопросов.

7.4. Образец содержания экзаменационного билета (при наличии экзамена по дисциплине)

Экзаменационный билет № _

1. Классификация криптографических методов защиты информации.
2. Дискретный логарифм. ρ -метод Полларда для вычисления дискретного логарифма.
3. Вычислить $2^{-1} \bmod 41$.

В случае ведения учебного процесса с использованием электронного обучения и дистанционных образовательных технологий, содержание билета может отличаться от приведенного.

8. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Общая оценка знаний обучающихся по дисциплине проводится по 100-балльной шкале исходя из максимума, приведенного в таблице ниже. Организационно-учебная работа в аудитории оценивается на основе таких критериев как посещаемость занятий, своевременное и качественное выполнение домашних заданий, активность во время проведения лекционных и практических занятий (участие в обсуждении текущего и пройденного материала, решение задач и т.п.).

8.1. Семестр 3

Номера разделов	Виды работ	Максимальное количество баллов
1-5	Организационно-учебная работа в аудитории	10
	Самостоятельная работа	10
	Выполнение индивидуального задания №1	25
	Выполнение индивидуального задания №2	25
ИТОГО		70
Экзамен		30
Общий итог за семестр		100

Соответствие баллов оценке

Количество баллов из 100	ECTS	Оценка по пятибалльной шкале	
		Экзамен, дифференцированный зачет	Зачет
90-100	A	отлично	зачтено
80-89	B	хорошо	зачтено
75-79	C		зачтено
70-74	D	удовлетворительно	зачтено
60-69	E		зачтено
35-59	FX	неудовлетворительно	не зачтено
0-34	F		не зачтено

9. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- 1) для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

- письменные задания оформляются увеличенным шрифтом.

2) для глухих и слабослышащих:

- лекции оформляются в виде электронного документа;

- письменные задания выполняются на компьютере в письменной форме;

- экзамен проводится в письменной форме на компьютере; возможно проведение в форме тестирования.

3) для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

1) для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;

- в форме электронного документа;

2) для глухих и слабослышащих:

- в печатной форме;

- в форме электронного документа.

3) для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;

- в форме электронного документа.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в Главном корпусе ДонГУ (г. Донецк, пр. Гурова, 6). Для проведения лабораторных занятий требуется аудитория, оборудованная меловой или маркерной доской, мультимедийный проектор и экран, ноутбук, комплект учебной мебели для студентов, рабочее место преподавателя, выход в Интернет – проводной или с использованием Wi-Fi.

Для самостоятельной работы используются текстовые и электронные ресурсы Научной библиотеки университета и других электронных библиотечных баз данных, учебно-методическое обеспечение, представленное в учебно-методическом кабинете Главного корпуса (ауд.401).

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные на платформе Moodle Центра дистанционного образования ФГБОУ ВО «ДонГУ». При изучении дисциплины применяются электронное обучение и дистанционные образовательные технологии.

С использованием ресурсов платформы дистанционного образования осуществляется текущий контроль знаний обучающихся на основе тестирования и проверки результатов самостоятельной работы.

11. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

11.1. Основная литература

1. Бабаш А.В., Криптографические методы защиты информации: учебник / А.В. Бабаш, Е.К. Баранова. — М.: КНОРУС, 2016. — 190 с. — (Бакалавриат и магистратура).
2. Ишмухаметов Ш.Т., Математические основы защиты информации. Электронное учебное пособие для студентов института вычислительной математики и информационных технологий: / Ш.Т. Ишмухаметов, Р.Г. Рубцова - Казань 2012. — 139 с.
3. Романец Ю.В., Защита информации в компьютерных системах и сетях. / Ю.В. Романец, П.А.Тимофеев, В.Ф. Шаньгин - 2-е изд., перераб. и доп. — М.: Радио и связь, 2001 — 376 с.: ил.
4. Маховенко Е.Б., Теоретико-числовые методы в криптографии: Учебное пособие / Е.Б. Маховенко. — М.: Гелиос АРВ, 2006. — 320 с., ил.

11.2. Дополнительная литература

1. Рябко Б. Я. Криптографические методы защиты информации: учеб. пособие для студентов вузов, обучающихся по специальностям: 201000 (210404) - "Многоканал. телекоммуникац. системы", 201100 (210405) - "Радиосвязь, радиовещание и телевидение ", 201800 (210403) - "Защищ. системы связи" / Б. Я. Рябко, А. Н. Фионов. - М.: Горячая линия-Телеком, 2005. - 229 с..
2. Мельников В.В., Защита информации в компьютерных системах / В.В. Мельников — М.: Финансы и статистика, 1997. — 368 с
3. Воронков Б.Н. Криптографические методы защиты информации: Учебное пособие для вузов / Б.Н. Воронков - Издательско-полиграфический центр Воронежского государственного университета, 2008.

12. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. **Национальная электронная библиотека (НЭБ):** федеральная государственная информационная система / Министерство Культуры РФ; Российская государственная библиотека. — Москва, 2019- . — URL: <https://rusneb.ru/> (дата обращения: 01.09.2023). — Режим доступа: свободный, подписка. Необходима установка программного обеспечения. — Текст: электронный.
2. **eLIBRARY.RU:** научная электронная библиотека: сайт. — Москва, 2000- . — URL: <https://elibrary.ru> (дата обращения: 01.09.2023). — Режим доступа: для авторизов. пользователей. —Текст: электронный.
3. Научная электронная библиотека **«КиберЛенинка»:** сайт / Ассоциация «Открытая наука». — Москва, 2014- . — URL: <https://cyberleninka.ru/>. — Режим доступа: свободный. — Текст: электронный.
4. Электронно-библиотечная система **«Лань»:** [сайт]. — URL: <https://e.lanbook.com> (дата обращения: 01.09.2023). — Режим доступа: для авторизов. пользователей. — Текст: электронный.
5. **ЭБС Юрайт:** электронная библиотечная система: сайт. — Москва, 2013. — URL: <https://biblio-online.ru> (дата обращения: 01.09.2023). — Режим доступа: для авторизов. пользователей. — Текст: электронный.
6. **Электронно-библиотечная система ДонГУ:** сайт / ФГБОУ ВО «ДонГУ». — Донецк, 2016- . — URL: <http://library.donnu.ru/> (дата обращения: 01.09.2023). — Режим доступа: свободный. — Текст: электронный.
7. **Электронный каталог** Научной библиотеки ДонГУ: раздел сайта / НБ ДонГУ. — Текст: электронный // ЭБС ДонГУ: сайт. — URL: <http://library.donnu.ru/catalog/>

(дата обращения: 01.09.2023). – Режим доступа: поиск свободный, электронные документы – для пользователей ДонГУ.

8. **Электронный архив ДонГУ:** раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://repo.donnu.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный.

13. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонГУ № 46484614)
2. Microsoft Office (корпоративная лицензия ДонГУ № 46472919)
3. Microsoft Visual Studio (лицензия программы Dream Spark для высших учебных заведений)
4. Антивирус Касперского, Adobe Acrobat Reader, xPDF (лицензии GPL, Apache, BSD для свободного программного обеспечения).