

Министерство науки и высшего образования  
Российской Федерации

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

Факультет математики и информационных технологий  
Кафедра теории упругости и вычислительной математики  
имени академика А.С. Космодамианского

УТВЕРЖДАЮ  
проректор



П.А. Машаров

« 29 » марта 2024 г.  
МП

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

### МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Укрупненная группа направлений  
подготовки  
Программа высшего образования

01.00.00 Математика и механика

Программа бакалавриата

Направление подготовки

01.03.02 Прикладная математика и  
информатика

Профиль подготовки

Прикладная математика и информатика

Квалификация

Бакалавр

Форма обучения

Очная

Рабочая программа адаптирована для лиц  
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины «**Математические основы защиты информации**» для обучающихся по направлению подготовки 01.03.02 Прикладная математика и информатика (Профиль: Прикладная математика и информатика), составлена на основании Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 01.03.02 Прикладная математика и информатика, утвержденного приказом Министерства образования и науки Российской Федерации от 10 января 2018 г. № 9 (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 теории упругости и  
вычислительной математики им. акад.  
А.С. Космодамианского,  
канд. физ.-мат. наук



М.Н. Пачева

Рабочая программа одобрена на заседании кафедры теории упругости и вычислительной математики им. акад. А.С. Космодамианского.  
Протокол от 26.03.2024 г. № 10

Врио заведующего кафедрой



Р.Н. Нескородев

СОГЛАСОВАНО:

Декан факультета математики и  
информационных технологий  
28.03.2024 г.



И.А. Моисеенко

Учебно-методическая комиссия факультета математики и информационных технологий.  
Протокол от 27.03.2024 г. № 3.  
Председатель



Л. И. Селякова

Руководитель основной профессиональной  
образовательной программы,  
д-р физ.-мат. наук, доцент  
26.03.2024 г.



Р.Н. Нескородев

## 1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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

дисциплины программы бакалавриата: Математический анализ, Алгебра и геометрия, Дискретная математика, Языки и методы программирования, Теория вероятностей и математическая статистика.

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

Производственная практика: преддипломная практика, Выполнение и защита выпускной квалификационной работы.

## 2. ОПИСАНИЕ ДИСЦИПЛИНЫ

### 2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	01.03.02 Прикладная математика и информатика (Профиль: Прикладная математика и информатика)
Шифр и название в соответствии с учебным планом	Б1.Б.31. Математические основы защиты информации
Часть образовательной программы	Базовая часть
Количество зачетных единиц / всего часов	3 / 108

### 2.2. Распределение часов по формам и периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы + контроль	всего	
Очная	3	6	17	34	–	57	108	зачет

## 3. ЦЕЛИ ДИСЦИПЛИНЫ

Освоение теоретических основ методов защиты информации от несанкционированного доступа и методов реализации криптографических систем на ЭВМ. Формирование представления об основных алгебраических структурах, используемых в криптографии.

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

Компетенции	Индикаторы	Результаты обучения
ОПК-5 Способен разрабатывать алгоритмы и компьютерные программы,	ОПК-5.5. Умеет использовать и модифицировать существующие	ОПК-5.5.1. Знает основные понятия и методы защиты информации, некоторые криптографические алгоритмы.

пригодные для практического применения	алгоритмы защиты информации.	ОПК-5.5.2. Умеет реализовывать некоторые криптографические алгоритмы, выполнять генерацию и передачу ключей. ОПК-5.5.3. Владеет способностью применять основные концепции в области защиты информации.
--	------------------------------	---

## 5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
Раздел 1.	
Введение в теорию защиты информации	<ol style="list-style-type: none"> <li>1. Основные понятия информационной безопасности.</li> <li>2. Сервисы и методы информационной безопасности.</li> <li>3. Понятие угрозы.</li> <li>4. Классификация криптографических методов защиты информации.</li> <li>5. Краткий исторический обзор развития методов защиты информации.</li> </ol>
Симметричные криптосистемы и их свойства	<ol style="list-style-type: none"> <li>1. Шифры замены.</li> <li>2. Шифры перестановки.</li> <li>3. Поточные криптосистемы.</li> <li>4. Блочные криптосистемы.</li> </ol>
Математические модели информационной безопасности	<ol style="list-style-type: none"> <li>1. Формальные модели шифров.</li> <li>2. Математические модели открытого текста.</li> <li>3. Критерии распознавания открытого текста.</li> </ol>
Арифметика остатков	<ol style="list-style-type: none"> <li>1. Введение в теорию чисел.</li> <li>2. Вычеты и их свойства.</li> <li>3. Алгоритм Эвклида и расширенный алгоритм Эвклида.</li> <li>4. Взаимно обратные числа в классе вычетов.</li> </ol>
Методы криптоанализа симметричных криптосистем	<ol style="list-style-type: none"> <li>1. Задачи и принципы криптоанализа.</li> <li>2. Метод полного перебора.</li> <li>3. Методы криптоанализа с использованием теории статистических решений.</li> </ol>
Теория стойкости криптосистем	<ol style="list-style-type: none"> <li>1. Совершенно стойкие криптосистемы.</li> <li>2. Идеально стойкие криптосистемы.</li> <li>3. Практическая стойкость криптосистем.</li> </ol>

## 6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 6.1. Форма обучения – очная, курс – 3, семестр – 6

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Раздел 1.	<b>17</b>	<b>34</b>	–	<b>57</b>	<b>108</b>
Введение в теорию защиты информации	2	4	–	4	10
Симметричные криптосистемы и их свойства	4	12	–	10	26

Математические модели информационной безопасности	2	2	–	10	14
Арифметика остатков	4	6	–	10	<b>20</b>
Методы криптоанализа симметричных криптосистем	2	6	–	10	18
Теория стойкости криптосистем	3	4	–	13	20
<b>ИТОГО ПО КОМПОНЕНТУ ОПОП</b>	<b>17</b>	<b>34</b>	–	<b>57</b>	<b>108</b>

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

### 7.1. Контрольные вопросы

#### Раздел 1

1. Методы информационной безопасности.
2. Классификация криптографических методов защиты информации.
3. Наивная криптография. Шифр Цезаря и частотола.
4. Классические шифры Плейфейера, Виженера.
5. Общий шифр перестановок.
6. Матричный шифр обхода.
7. Математическая модель шифра.
8. Математическая модель открытого текста.
9. Алгоритм Евклида и его следствие.
10. Конгруэнции и их свойства. Кольцо остатков.
11. Кольцо матриц. Нахождение обратной матрицы в качестве дешифрующего ключа.
12. Аффинный шифр 1-го порядка. Пример.
13. Аффинный шифр 2-го порядка. Пример.
14. Задачи и принципы криптоанализа.
15. Метод полного перебора.
16. Частотный анализ, его применение ко взлому шифра.
17. Криптографическая стойкость криптосистем
18. Методы оценки стойкости криптосистем

### 7.2. Темы письменных работ (типы задач)

Контрольные работы по практике:

- зашифровать текст аффинным шифром 1-го порядка;
- зашифровать текст с использованием общего шифра перестановки;
- дешифровать криптотекст с использованием шифра сдвига.
- определить число, обратное к  $a$  относительно умножения, по  $\text{mod } b$  ( $a^{-1} \text{ mod } b$ ).
- с использованием алгоритма Евклида определить  $\text{НОД}(a, b)$ .

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

## 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.).

Номера разделов	Виды работ	Максимальное количество баллов
1	Организационно-учебная работа в аудитории	5
	Самостоятельная работа	60
	Контрольные работы по практике	15
	Контрольная работа по теоретическому материалу	20
ИТОГО		100
Зачет		
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), в Учебно-практическом вычислительном центре ДонГУ (г. Донецк, пр. Гурова, 6, корпус 12).

Для проведения лекций требуется аудитория, оборудованная меловой или маркерной доской / сенсорным экраном / мультимедийный проектор с экраном и ноутбуком, комплект учебной мебели для студентов, рабочее место преподавателя.

Для проведения практических занятий требуется аудитория, оборудованная меловой или маркерной доской / сенсорным экраном / мультимедийный проектор с экраном и ноутбук, комплект учебной мебели для студентов, рабочее место преподавателя.

Для проведения лабораторных занятий требуется аудитория, оборудованная маркерной доской или сенсорным экраном / мультимедийный проектор с экраном и ноутбук, персональные компьютеры, 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 аудиториях Главного корпуса (ауд. 511, 605, 610).

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. Бородин А.И. Теория чисел: учеб. пособие для ун-тов по спец. "Математика" / А.И.Бородин. - Киев: Выща шк., 1992. - 288 с.



2. Методические указания к лабораторным работам по криптографии / [сост.: Л. Н. Шкодина, М. Н. Пачева, А. И. Занько] ; ГОУ ВПО "Донецкий национальный университет". - Донецк : ГОУ ВПО "ДонНУ", 2018. - 42 с.
3. Практический курс по современным методам криптографии [Электронный ресурс] : учебно-методическое пособие / ГОУ ВПО "Донецкий национальный университет" ; сост.: Л. Н. Шкодина, А. И. Занько. - 2-е изд. - Донецк : ДонНУ, 2019.
4. Скобелев В.Г. Введение в криптологию: учеб. пособие / В.Г. Скобелев; Донецкий нац. ун-т. - Донецк: Юго-Восток, 2008. - 175 с.

#### 11.2. Дополнительная литература

5. Калоеров С.А. Программирование на С++: учеб. пособие / С.А.Калоеров; Донецкий нац. ун-т. – Изд. 3-е. – Донецк: Уго-Восток, 2009. – 298 с.
6. Молдовян Н.А. Введение в криптосистемы с открытым ключом: [проблематика криптографии, элементы теории чисел, двухключевые криптосистемы, системы электронной цифровой подписи с составным модулем, открытое распределение ключей и открытое шифрование, управление ключами и протоколы] / Н.А.Молдовян, А.А. Молдовян. – Санкт-Петербург: БХВ-Петербург, 2005. - 286 с.
7. Тилборг ван Хенк К. А. Основы криптологии: Проф. руководство и интерактивный учебник / Х.К.А. ван Тилборг; Пер. с англ. Д.С.Ананичева, И.О.Корякова; Под ред. И.О.Корякова. - М.: Мир, 2006. - 471 с.
8. Шкодина, Л. Н. Современные методы криптографии [Электронный ресурс] : учебное пособие / Л. Н. Шкодина. А. И. Занько. - Донецк : ДонНУ, 2020.

### 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).