

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



УТВЕРЖДАЮ

проректор

П.А. Машаров

» марта 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МАТЕМАТИЧЕСКИЕ МОДЕЛИ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ 7

Укрупненная группа направлений
подготовки

Программа высшего образования
Направление подготовки

Профиль подготовки

Квалификация

Форма обучения

02.00.00 Компьютерные и
информационные науки

Программа бакалавриата

02.03.02 Фундаментальная информатика и
информационные технологии

Фундаментальная информатика и
информационные технологии

Бакалавр

Очная

Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины «**Математические модели в информационных технологиях 7**» для обучающихся по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии (Профиль подготовки: Фундаментальная информатика и информационные технологии), составлена на основании Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии, утвержденного приказом Министерства образования и науки Российской Федерации от 23 августа 2017 г. № 808 (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:

дисциплины программы бакалавриата: Дискретная математика, Алгоритмы и анализ сложности, Основы программирования, Введение в объектно-ориентированное программирование.

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

«Математические основы защиты информации и информационной безопасности» магистратуры, являются основой для прохождения практик; используются при подготовке выпускной квалификационной работы.

2. ОПИСАНИЕ ДИСЦИПЛИНЫ

2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	02.03.02 Фундаментальная информатика и информационные технологии (Профиль подготовки: Фундаментальная информатика и информационные технологии)
Шифр и название в соответствии с учебным планом	Б1.В.ДВ.7.2. Математические модели в информационных технологиях 7
Часть образовательной программы	Вариативная часть: выбор обучающегося
Количество зачетных единиц / всего часов	2 / 72

2.2. Распределение часов по периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы + контроль	всего	
Очная	4	8	20	20	-	32	72	экзамен

3. ЦЕЛИ ДИСЦИПЛИНЫ

Формирование представлений о роли и месте математики и вычислительной техники в современной цивилизации и в мировой культуре, умений логически мыслить, составлять несложные информационно-математические модели, оперировать с абстрактными объектами и быть корректным в употреблении математических понятий и символов для выражения количественных и качественных отношений, воспитание высокой математической культуры.

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

4.1. Компетенции

ПК-1. Способен понимать и применять в научно-исследовательской и прикладной деятельности современный математический аппарат, основные законы естествознания,

современные языки программирования и программное обеспечение; операционные системы.

4.2. Индикаторы компетенций

ПК-1.18. Применяет классические и современные математические методы для решения фундаментальных и прикладных задач, связанных с защитой информации.

4.3. Результаты обучения

ПК-1.18.1. Знает определения и утверждения, методы решения задач, основные криптографические алгоритмы, применяемые для решения профессиональных задач.

ПК-1.18.2. Умеет выбирать и использовать необходимые математические методы и вычислительные средства, решать задачи дисциплины (создавать приложения по криптографической защите информации; использовать стандартные приложения для решения профессиональных задач).

ПК-1.18.3. Аргументированно выбирает метод решения задачи, устанавливает свойства математических объектов, закономерности между ними, доводит решение задачи до работоспособного приложения, оценивает и анализирует полученный результат, строит математические модели для решения профессиональных задач.

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
Информационная безопасность компьютерных систем	Основные понятия и определения. Основные угрозы безопасности АСОИ. Задачи информационной безопасности. Криптографические системы и требования к ним
Классические криптосистемы	Основные понятия и определения. Табличные шифры перестановок. Табличные шифры замен: системы шифрования Цезаря, Гронсфельда, шифрующие таблицы Трисемуса. Биграммный шифр Плейфейра, криптосистема Хилла, система шифрования Вижинера, шифр «двойной квадрат» Уитсона.
Современные симметричные криптосистемы	Основные классы симметричных криптографических систем. Модель сети Фейстела. Система блочного шифрования DES. Основные режимы работы алгоритма DES. Система блочного шифрования ГОСТ 28147-89. Режимы работы алгоритма ГОСТ 28147-89. Системы блочного шифрования RC6, SAFER+. Потокосые шифры RC4, WAKE
Асимметричные криптосистемы.	Общие положения асимметричных криптосистем. Однонаправленные функции. Системы шифрования Эль-Гамала и RSA

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Форма обучения – очная, курс – 4, семестр – 8

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Информационная безопасность компьютерных систем	2	2		2	6
Классические криптосистемы	6	6		10	22
Современные симметричные криптосистемы	8	8		12	28
Асимметричные криптосистемы.	4	4		8	16
ИТОГО ПО КОМПОНЕНТУ ОПОП	20	20	-	32	72

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

7.1. Контрольные вопросы

1. Основные понятия и определения информационной безопасности компьютерных систем.
2. Основные угрозы безопасности АСОИ.
3. Основные задачи информационной безопасности.
4. Криптографические системы и требования к ним.
5. Основные понятия и определения классических криптосистем.
6. Табличные шифры перестановок с ключом – размером таблицы.
7. Табличные шифры перестановок с ключом – словом или фразой, задающей перестановку.
8. Двойная перестановка.
9. Магические квадраты.
10. Полибианский квадрат.
11. Система шифрования Цезаря.
12. Аффинная система подстановок Цезаря.
13. Система Цезаря с ключевым словом.
14. Шифр Гронсфельда.
15. Шифрующие таблицы Трисемуса.
16. Биграммный шифр Плейфейра.
17. Криптосистема Хилла.
18. Система шифрования Вижинера.
19. Шифр «двойной квадрат» Уитсона.
20. Омонимические шифры.
21. Основные классы симметричных криптографических систем.
22. Модель сети Фейстела.
23. Система блочного шифрования DES.
24. Основные режимы работы алгоритма DES.
25. Система блочного шифрования ГОСТ 28147-89.
26. Режимы работы алгоритма ГОСТ 28147-89.
27. Система блочного шифрования RC6.
28. Система блочного шифрования SAFER+.
29. Самосинхронизирующиеся потоковые шифры.
30. Поточковый шифр RC4.
31. Поточковый шифр WAKE.
32. Общие положения асимметричных криптосистем. Однонаправленные функции.
33. Система шифрования RSA.
34. Система шифрования Эль-Гамала.

7.2. Темы индивидуальных заданий (примеры)

Задание 1

1. Основные понятия и определения криптологии.
2. Основные классы симметричных криптосистем
3. Табличные шифры замен.
4. Система шифрования Вижинера.

Задание 2

1. Модель сети Фейстела.
2. Режимы работы алгоритма ГОСТ 28147-89.
3. Общие положения асимметричных криптосистем.
4. Система шифрования RSA.

7.3. Образец содержания экзаменационного билета

Экзаменационный билет № _

1. Основные понятия и определения информационной безопасности.
2. Система шифрования RSA.

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 8

Номера тем	Виды работ	Максимальное количество баллов
1-4	Организационно-учебная работа в аудитории	5
	Самостоятельная работа	5
	Выполнение индивидуального задания №1	25
	Защита индивидуального задания	5
5-7	Организационно-учебная работа в аудитории	5
	Самостоятельная работа	5
	Выполнение индивидуального задания №2	25
	Защита индивидуального задания	5
ИТОГО		80
Экзамен		20
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. Романец Ю.В., Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин / Под ред. В.Ф.Шаньгина. – 2-е изд., перераб. и доп. - М.: Радио и связь, 2001. – 376 с.: ил.
2. Лось А.Б., Криптографические методы защиты информации: учебник для академического бакалавриата / А.Б. Лось, А.Ю. Нестеренко, М.И Рожков - М.: Юрайт, 2016
3. Бабаш А.В., Криптографические методы защиты информации : учебник / А.В. Бабаш, Е.К. Баранова. — М. : КНОРУС, 2016. — 190 с. — (Бакалавриат и магистратура).

11.2. Дополнительная литература

1. Мельников В.В., Защита информации в компьютерных системах – М.: Финансы и статистика, 1997. – 368 с.
2. Баричев С.Г., Основы современной криптографии. / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов – М.: «Горячая линия – Телеком», 2001. – 120 с.: ил.
3. Хорев П.Б., Методы и средства защиты информации в компьютерных системах. – М.: Издательский центр «Академия», 2005.
4. Новиков Е.А., Криптографические методы защиты информации - Учебное пособие. / Е.А. Новиков, Ю.А. Шитов – Красноярск: Сибирский федеральный университет, 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.
Научная электронная библиотека «КиберЛенинка»: сайт / Ассоциация «Открытая наука». – Москва, 2014- . – URL: <https://cyberleninka.ru/>. – Режим доступа: свободный. – Текст: электронный.
3. Электронно-библиотечная система «Лань»: [сайт]. – URL: <https://e.lanbook.com> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

4. **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.

5. **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.

6. **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.

7. **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).
5. Визуальная среда программирования Embarcadero Delphi или Delphi 7.