

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



П.А. Машаров

« 29 » марта 2024 г.
МП

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

СОВРЕМЕННЫЕ МЕТОДЫ КРИПТОГРАФИИ

Укрупненная группа направлений
подготовки

Программа высшего образования
Направление подготовки

Магистерская программа
Квалификация
Форма обучения

01.00.00 Математика и механика

Программа магистратуры
01.04.02 Прикладная математика и
информатика

Прикладная математика и информатика
Магистр
Очная

Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины «Современные методы криптографии» для обучающихся по направлению подготовки 01.04.02 Прикладная математика и информатика (Магистерская программа: Прикладная математика и информатика), составлена на основании Федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 01.04.02 Прикладная математика и информатика, утвержденного приказом Министерства образования и науки Российской Федерации от 10 января 2018 г. № 13 (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 имени
академика А.С. Космодамианского
канд. физ.-мат. наук



Е.С. Глушанков

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: Языки и методы программирования, Математические основы защиты информации.

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

практики: Производственная практика: преддипломная практика.

2. ОПИСАНИЕ ДИСЦИПЛИНЫ

2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	01.04.02 Прикладная математика и информатика (Магистерская программа: Прикладная математика и информатика)
Шифр и название в соответствии с учебным планом	Б1.В.ОД.1. Современные методы криптографии
Часть образовательной программы	Вариативная часть: выбор вуза
Количество зачетных единиц / всего часов	5 / 180

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	1	1	17	34	17	112	180	экзамен

3. ЦЕЛИ ДИСЦИПЛИНЫ

Целями дисциплины «Современные методы криптографии» являются освоение студентами теоретических сведений в области современной криптографии, ознакомление с современными методами асимметричного шифрования и дешифрования данных, подкрепленное современным математическим аппаратом.

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

4.1. Компетенции

ОПК-4. Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.

ПК-2. Способен разрабатывать и руководить процессом разработки программного обеспечения для решения задач профессиональной деятельности.

4.2. Индикаторы компетенций

ОПК-4.3. Адаптирует существующие информационно-коммуникационные технологии для решения задач в области криптографии.

ПК-3.1. Применяет и модифицирует существующие алгоритмы для решения задач криптографии.

4.3. Результаты обучения

ОПК-4.3.1. Знает программные комплексы и библиотеки, позволяющие оперировать целыми числами произвольной длины.

ОПК-4.3.2. Умеет оперировать данными, представляемыми в виде целых чисел произвольной длины.

ОПК-4.3.3. Владеет навыками работы с битовыми представлениями чисел в памяти электронно-вычислительной машины.

ПК-2.1.1. Знает основные алгоритмы классической и современной криптографии.

ПК-2.1.2. Умеет применять криптографические алгоритмы и/или их комбинации для решения конкретных задач защиты информации.

ПК-2.1.3. Владеет методами асимметрической криптографии.

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
Раздел 1. Введение в современную криптографию	
Сведения из теории чисел	Простые числа. Алгоритм Евклида. Кольцо остатков. Функция Эйлера. Малая теорема Ферма. Китайская теорема об остатках. Первообразные корни.
Раздел 2. Криптосистемы с открытым ключом	
Криптосистема RSA	Генерация ключей для алгоритма RSA. Шифрование по RSA. Дешифрование по RSA. Числа RSA. Корректность системы RSA. Надёжность системы RSA.
Атака на криптосистему RSA	Атака Винера на криптосистему RSA. Обзор атак на криптосистему RSA.
Криптосистема Эль-Гамала	Генерация ключей для алгоритма Эль-Гамала. Шифрование по Эль-Гамалу. Дешифрование по Эль-Гамалу. Корректность системы Эль-Гамала.
Генерация простых чисел	Псевдопростые числа. Вероятностный тест Миллера-Рабина. Генераторы псевдослучайных чисел. Криптографически стойкие генераторы псевдослучайных чисел. Алгоритм BBS (Блум-Блюма-Шуба). Генерация псевдослучайных простых чисел для задач криптографии.
Раздел 3. Криптография на эллиптических кривых	

Эллиптическая криптография	Эллиптические кривые над полем \mathbb{R} . Эллиптические кривые над конечными полями. Шифрование на эллиптических кривых.
----------------------------	--

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Раздел 1. Введение в современную криптографию	2	2	–	12	16
Сведения из теории чисел	2	2	–	12	16
Раздел 2. Криптосистемы с открытым ключом	12	26	14	80	132
Криптосистема RSA	6	14	8	30	58
Атака на криптосистему RSA	2	2		10	14
Криптосистема Эль-Гамала	2	6	4	20	32
Генерация простых чисел	2	4	2	20	28
Раздел 3. Криптография на эллиптических кривых	3	6	3	20	32
Эллиптическая криптография	3	6	3	20	32
ИТОГО ПО КОМПОНЕНТУ ОПОП	17	34	17	112	180

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

7.1. Контрольные вопросы

Раздел 1

1. Простые числа.
2. Алгоритм Евклида.
3. Кольцо остатков.
4. Функция Эйлера.
5. Малая теорема Ферма.
6. Китайская теорема об остатках.
7. Первообразные корни.

Раздел 2

8. Генерация ключей для алгоритма RSA.
9. Шифрование по RSA.
10. Дешифрование по RSA.
11. Числа RSA.
12. Корректность системы RSA.
13. Надёжность системы RSA.
14. Атака Винера на криптосистему RSA.
15. Генерация ключей для алгоритма Эль-Гамала.
16. Шифрование по Эль-Гамалу.
17. Дешифрование по Эль-Гамалу.
18. Корректность системы Эль-Гамала.
19. Псевдопростые числа. Вероятностный тест Миллера-Рабина.
20. Генераторы псевдослучайных чисел.
21. Криптографически стойкие генераторы псевдослучайных чисел.
22. Алгоритм BBS (Блум-Блюма-Шуба).

23. Генерация псевдослучайных простых чисел для задач криптографии.

Раздел 3

24. Эллиптические кривые над полем \mathbb{R} .

25. Эллиптические кривые над конечными полями.

26. Шифрование на эллиптических кривых.

7.2. Темы письменных работ (типы задач)

Контрольные работы по практике по темам:

- алгоритмы RSA и Эль-Гамала (шифрование и дешифрование);
- криптостойкий генератор псевдослучайных простых чисел (алгоритм BBS, тест

Миллера-Рабина);

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

7.3. Темы индивидуальных заданий

- алгоритм RSA (шифрование и дешифрование);
- атака Винера на RSA;
- алгоритм Эль-Гамала (шифрование и дешифрование);
- криптостойкий генератор псевдослучайных простых чисел (алгоритм BBS, тест Миллера-Рабина);
- алгоритм на эллиптических кривых (шифрование и дешифрование);

7.4. Образец содержания экзаменационного билета

ФГБОУ ВО «ДОНЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра теории упругости и вычислительной математики

имени академика А.С. Космодамианского

Направление подготовки:	01.04.02 Прикладная математика и информатика
Магистерская программа:	Прикладная математика и информатика
Программа подготовки:	магистратура
Семестр:	1
Учебная дисциплина:	«Современные методы криптографии»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Тест Миллера-Рабина: теорема, алгоритм.
2. Криптографически стойкий генератор псевдослучайных чисел. Алгоритм Блума-Блюма-Шуба.
3. Эллиптические кривые над конечными полями. Сложение точек эллиптической кривой. Криптосистема, основанная на эллиптических кривых: шифрование, дешифрование.
4. Расшифровать криптотекст «100106081301», если известно, что исходный текст на гавайском языке был зашифрован по алгоритму RSA с открытым ключом $\{e = 3, n = 15\}$.
5. Зашифровать по алгоритму Эль-Гамала с ключом $p = 17$ гавайское слово «haneli» («сто»). Другие элементы открытого и закрытого ключей задать самостоятельно. Последовательность сессионных ключей определяется (зацикленной) последовательностью простых чисел, удовлетворяющих условиям, накладываемым на сессионные ключи. Проверить корректность криптотекста, осуществив его расшифрование.

Гавайский алфавит

Буква	a	e	i	o	u	h	k	l	m	n	p	w	'
Код	01	02	03	04	05	06	07	08	09	10	11	12	13

Утверждено на заседании кафедры теории упругости и вычислительной математики имени академика А.С. Космодамианского.

Протокол № __ от «__» _____ 20__ года.

Заведующий кафедрой _____

Экзаменатор _____

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.

По результатам работы в семестре обучающийся, набравший не менее 60 баллов, имеет право получить оценку. Те, кого набранные баллы не устраивают, сдают индивидуальные задания, выполняют зачетную контрольную работу. Максимальное количество баллов за экзамен – 75. Оценка за семестр вычисляется как максимальная из полученных за семестр и на экзамене и выставляется согласно принятому порядку.

Номера разделов	Виды работ	Максимальное количество баллов
1-2	Индивидуальные задания	45
	Контрольные работы по практике	30
3	Индивидуальное задание	15
	Контрольная работа по проверке теоретических знаний	10
ИТОГО		100
Экзамен		75
Общий итог за семестр		100

Соответствие баллов оценке

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

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 и практических занятий 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 лабораторных занятий требуется аудитория, оборудованная меловой или маркерной доской / сенсорным экраном / мультимедийный проектор с экраном и 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 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. Практический курс по современным методам криптографии : учеб.-метод. пособие / сост.: Л.Н. Шкодина, А.И. Занько. – Донецк: ДонНУ, 2019. – 86 с.
2. Современные методы криптографии : учеб. пособие / сост.: Л.Н. Шкодина, А.И. Занько. – Донецк: ДонНУ, 2019. – 119 с.

11.2. Дополнительная литература

3. Бородин А.И. Теория чисел. – К.: Вища шк., 1992. – 288 с.
4. Мао В. Современная криптография: теория и практика. – М.: Вильямс, 2005. – 763 с.
5. ван Тилборг Х.К.А. Основы криптологии: Проф. руководство и интерактивный учебник. – М.: Мир, 2006. – 471 с.

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://hero.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).