

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

«17» апреля 2025 г.
МП

П.А. Машаров

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

СОВРЕМЕННЫЕ МЕТОДЫ КРИПТОГРАФИИ

Укрупненная группа направлений
подготовки

Программа высшего образования

Направление подготовки

Профиль

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 может быть адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2025

Рабочая программа дисциплины **«Современные методы криптографии»** для обучающихся по направлению подготовки 01.04.02 Прикладная математика и информатика (Профиль: 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 2025 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 имени академика А.С. Космодамианского.
Протокол от 03.04.2025 г. № 10.

И.о. заведующего кафедрой

И.А. Моисеенко

СОГЛАСОВАНО:

Декан факультета математики и
информационных технологий
16.04.2025 г.

И.А. Моисеенко

Учебно-методическая комиссия факультета математики и информационных технологий.
Протокол от 16.04.2025 г. № 3.
Председатель

Л.И. Селякова

Руководитель основной
образовательной программы
д-р физ.-мат. наук, доц.
03.04.2025 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 (Профиль: 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	4 / 144

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	93	144	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 и навыками практической работы.

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

4.1. Компетенции

ОПК-2. Способен совершенствовать и реализовывать новые математические методы решения прикладных задач.

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

4.2. Индикаторы компетенций

ОПК-2.3. Совершенствует и адаптирует существующие математические методы решения задач в области криптографии.

ПК-2.1. Применяет и модифицирует существующие алгоритмы в процессе разработки программного обеспечения для решения задач криптографии.

4.3. Результаты обучения

ОПК-2.3.1. Знает программные комплексы и библиотеки, позволяющие оперировать целыми числами произвольной длины.

ОПК-2.3.2. Умеет оперировать данными, представляемыми в виде целых чисел произвольной длины, в контексте задач современной криптографии.

ОПК-2.3.3. 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	66	104
Криптосистема RSA	6	–	14	24	44
Атака на криптосистему RSA	2	–	2	8	12
Криптосистема Эль-Гамала	2	–	6	16	24
Генерация простых чисел	2	–	4	18	24
Раздел 3. Криптография на эллиптических кривых	3	–	6	15	24
Эллиптическая криптография	3	–	6	15	24
ИТОГО ПО КОМПОНЕНТУ ОП	17	–	34	93	144

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

ДОНЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Кафедра теории упругости и вычислительной математики
имени академика А.С. Космодамианского

Направление подготовки:	01.04.02 Прикладная математика и информатика
Профиль:	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 Блум-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.

Самостоятельная работа оценивается на основе предоставленных на проверку выполненных домашних, индивидуальных заданий с учетом своевременности их предоставления и соответствия требованиям к их выполнению.

Количество баллов за контрольную работу вычисляется как сумма баллов за все входящие в её состав задания. Каждое задание оценивается исходя из максимально возможного количества баллов с учетом правильности выполнения задания, полноты приводимых обоснований.

По результатам работы в семестре обучающийся, набравший не менее 60 баллов, имеет право получить оценку. Те, кто претендует на более высокий балл, проходят промежуточную аттестацию. Максимальное количество баллов на промежуточной аттестации – 100. Общее количество баллов за семестр вычисляется как максимальная из полученных за семестр и на промежуточной аттестации и выставляется согласно принятому порядку.

Номера разделов	Виды работ	Максимальное количество баллов
1-2	Самостоятельная работа	45
	Контрольные работы по практике	30
3	Самостоятельная работа	15
	Контрольная работа по проверке теоретических знаний	10
ИТОГО		100
Промежуточная аттестация		100
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. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в Главном корпусе ДонГУ (г. Донецк, пр. Гурова, 6). Для проведения 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. 605).

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные на платформе Moodle Центра дистанционного образования ФГБОУ ВО «ДонГУ». При изучении дисциплины могут применяться 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.

10. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

10.1. 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.

10.2. 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.

11. 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: 31.03.2025). – 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: 31.03.2025). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

3. Научная электронная библиотека «КиберЛенинка»: сайт / Ассоциация «Открытая наука». – Москва, 2014- . – URL: <https://cyberleninka.ru/> (дата обращения: 31.03.2025). – Режим доступа: свободный. – Текст: электронный.

4. Электронно-библиотечная система «Лань»: [сайт]. – URL: <https://e.lanbook.com> (дата обращения: 31.03.2025). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

5. ЭБС Юрайт: электронная библиотечная система: сайт. – Москва, 2013. – URL: <https://biblio-online.ru> (дата обращения: 31.03.2025). – 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: 31.03.2025). – 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: 31.03.2025). – 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: 31.03.2025). – Режим доступа: свободный.

12. 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).