

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ  
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ  
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ  
«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»  
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ  
Кафедра теории упругости и вычислительной математики  
имени академика А.С. Космодамианского

УТВЕРЖДАЮ:

проректор по научно-методической  
и учебной работе

Е.И. Скафа

«21» апреля 2021 г.

МП



**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**  
**«СОВРЕМЕННЫЕ МЕТОДЫ КРИПТОГРАФИИ»**  
практико-ориентированная дисциплина

Направление подготовки:	<u>01.04.02 Прикладная математика и информатика</u>
Магистерская программа:	<u>Прикладная математика и информатика</u>
Программа подготовки:	<u>Магистратура</u>
Квалификация:	<u>Магистр</u>
Форма обучения:	<u>очная</u>

Донецк 2021



**УТВЕРЖДАЮ:**

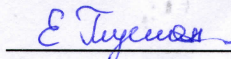
Декан факультета математики  
и информационных технологий  
И. А. Моисеенко



Рабочая программа учебной дисциплины **«Современные методы криптографии»** 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 2021г. № 13; Государственного образовательного стандарта высшего образования (ГОС ВО) Донецкой Народной Республики (ДНР) (проекта) по направлению подготовки 01.04.02 Прикладная математика и информатика; Порядка организации учебного процесса в образовательных организациях высшего профессионального образования Донецкой Народной Республики, утвержденного приказом Министерства образования и науки Донецкой Народной Республики от 10.11.2017 г. № 1171 (с изменениями и дополнениями); учебного плана и основной профессиональной образовательной программы высшего образования направления подготовки 01.04.02 Прикладная математика и информатика, магистерской программы: «Прикладная математика и информатика», разработанных в ГОУ ВПО «Донецкий национальный университет».

Разработчик:

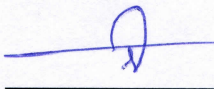
доцент кафедры теории упругости и  
вычислительной математики имени  
академика А.С. Космодамианского  
канд. физ.-мат. наук

 Е.С. Глушанков

Рабочая программа учебной дисциплины утверждена на заседании кафедры теории упругости и вычислительной математики имени академика А.С. Космодамианского

Протокол № 15 от «12» апреля 2021 г.

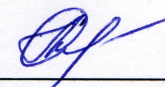
Заведующий кафедрой

 В.И. Сторожев

Рабочая программа учебной дисциплины одобрена учебно-методической комиссией факультета математики и информационных технологий

Протокол № 4 от «14» апреля 2021 г.

Председатель учебно-методической комиссии  
факультета математики и информационных технологий

 Л.И. Селякова

## 1. ОБЛАСТЬ ПРИМЕНЕНИЯ И МЕСТО ДИСЦИПЛИНЫ В УЧЕБНОМ ПРОЦЕССЕ

Учебная дисциплина «Современные методы криптографии» является практико-ориентированной дисциплиной и относится к вариативной части образовательной программы. Для изучения данной учебной дисциплины необходимы знания и умения, формируемые *предшествующей дисциплиной «Математические основы защиты информации»*, входящей в программу подготовки бакалавров.

## 2. СТРУКТУРА ДИСЦИПЛИНЫ

Характеристика учебной дисциплины	Форма обучения	
	Очная	Заочная
Направление подготовки	01.04.02 Прикладная математика и информатика	
Магистерская программа	Прикладная математика и информатика	
Программа подготовки	Магистратура	
Квалификация	Магистр	
Количество содержательных модулей и тем	4 (11)	
Дисциплина базовой / вариативной части образовательной программы	Вариативной части	
Формы контроля	1 модульный контроль, экзамен в 1-м семестре	
Год подготовки	1	×
Семестр	1	×
Количество зачетных единиц	5	×
Количество часов всего	180	×
в т.ч.:		
- лекционных	18	×
- практических или семинарских	18	×
- лабораторных	36	×
- самостоятельной работы	108	×
в т.ч. индивидуальное задание	60	×
Недельное количество часов	10	×
в т.ч.: - аудиторных	4	×
- самостоятельной работы студента	6	×

## 3. ОПИСАНИЕ ДИСЦИПЛИНЫ

**Цель изучения дисциплины «Современные методы криптографии»** – изучение различных современных методов криптографической защиты, сравнительный анализ этих методов, их надежность и эффективность с помощью традиционных способов криптографии, классической математики, методов формализованного описания систем, процессов; развитие у студентов логического обоснования выбранного метода шифрования, его математического обоснования и умения реализовать криптографический метод на ЭВМ.

**Задачи:** освоение студентами теоретических сведений (определения, теоремы, их доказательства, связи между ними и их использование в криптографии) и методов реализации криптографических систем на современных ЭВМ.

**Требования к результатам освоения дисциплины.** Процесс изучения дисциплины «Современные методы криптографии» направлен на формирование элементов следующих **компетенций** в соответствии с ФГОС ВО РФ, ГОС ВО ДНР (проект) по направлению подготовки 01.04.02 Прикладная математика и информатика и основной профессиональной образовательной программы высшего образования направления подготовки 01.04.02

Прикладная математика и информатика, магистерской программы: «Прикладная математика и информатика»:

<b>Универсальные компетенции (УК):</b>	
Наименование категории (группы) универсальных компетенций: «Системное и критическое мышление»	
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
<b>Общепрофессиональные компетенции (ОПК):</b>	
ОПК-2	Способен совершенствовать и реализовывать новые математические методы решения прикладных задач
ОПК-4	Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности
<b>Профессиональные компетенции (ПК):</b>	
ПК-4	Способен разрабатывать и руководить процессом разработки программного обеспечения для решения задач профессиональной деятельности на вычислительных системах различной архитектуры, в том числе на реконфигурируемых вычислительных системах
ПК-6	Способен использовать современные методы разработки и реализации алгоритмов для решения задач профессиональной деятельности на базе языков программирования и пакетов прикладных программ

**Индикаторы достижения компетенций и результаты обучения.** Достижение компетенций оценивается на основе таких индикаторов и соответствующих им результатов обучения:

Категории универсальных компетенций	Универсальные компетенции	Индикаторы	Результаты обучения
Системное и критическое мышление	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Применяет системный подход и осуществляет критический анализ проблемной ситуации	Рассматривает поставленную криптографическую задачу как совокупность подзадач с учетом имеющихся ресурсов, поставленной цели, а также существующих внутренних и внешних связей

Общепрофессиональные компетенции	Индикаторы	Результаты обучения
ОПК-2. Способен совершенствовать и реализовывать новые математические методы решения прикладных задач	ОПК-2.1. Оценивает достоинства и недостатки применения конкретных методов для решения поставленных прикладных задач, аргументированно обосновывая критерии оценки и сравнения методов	Способен оценивать преимущества и недостатки различных криптосистем и учитывать их при решении конкретных криптографических задач



ОПК-4. Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	ОПК-4.1. Использует и комбинирует существующие информационно-коммуникационные технологии для решения поставленных задач в области профессиональной деятельности с учетом требований информационной безопасности	Владеет современными технологиями программирования и осуществляет выбор оптимальных методов с учетом особенностей конкретных задач защиты информации
---	---	--

Профессиональные компетенции	Индикаторы	Результаты обучения
ПК-4. Способен разрабатывать и руководить процессом разработки программного обеспечения для решения задач профессиональной деятельности на вычислительных системах различной архитектуры, в том числе на реконфигурируемых вычислительных системах	ПК-4.1. Применяет и модифицирует существующие алгоритмы для решения задач профессиональной деятельности на вычислительных системах различной архитектуры, в том числе на реконфигурируемых вычислительных системах	Владеет современными методами защиты информации, шифровки/дешифровки
ПК-6. Способен использовать современные методы разработки и реализации алгоритмов для решения задач профессиональной деятельности на базе языков программирования и пакетов прикладных программ	ПК-6.3. Реализует существующие и/или модифицированные алгоритмы с помощью современных языков программирования и /или пакетов прикладных программ	Ознакомлен с современными языками программирования и прикладными пакетами программ, способен оценить возможность применения конкретного языка/пакета для решения криптографических задач

#### 4. ФОРМЫ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Дисциплина «Современные методы криптографии» предусматривает следующие формы организации учебного процесса: лекции, практические занятия, лабораторные занятия, самостоятельную работу студентов.

Материал излагается с использованием объяснительно-иллюстративных, эвристических и исследовательских методов преподавания. При проведении лекций и практических занятий используются мультимедийные презентации, раздаточные материалы.

В учебном процессе широко применяются активные и интерактивные формы проведения занятий (разбор конкретных ситуаций, дискуссия, полемика), внеаудиторная самостоятельная работа, балльно-рейтинговая система оценки успеваемости, личностно-ориентированное обучение, проблемное обучение. В учебном процессе используются интернет-ресурсы по данному курсу; рассматриваются задачи, максимально приближенные к конкретным практическим ситуациям, тесты, самостоятельная работа; контрольные работы.

Самостоятельная работа студентов предусматривает подготовку к занятиям, подготовку конспектов по отдельным вопросам изучаемых тем, изучение учебной и методической литературы.

**Тематический план «Современные методы криптографии»**

Темы	Вопросы темы
<b>Содержательный модуль 1. Введение в современную криптографию</b>	
1. Обзор сведений из теории чисел, используемых при защите информации	1.1. Обзор основных терминов, определений и задачи классической криптографии
2. Новые направления в теории защиты информации	2.1. Использование функций с секретом в асимметричных алгоритмах шифрования
<b>Содержательный модуль 2. Криптосистемы с открытым ключом</b>	
3. Стандарт асимметричного шифрования RSA*	3.1. Ключи шифрования и дешифровки. Алгоритм шифрования
4. Корректность криптосистемы, эффективность и надежность	4.1. Теорема о стойкости криптосистемы RSA
5. Ускоренный (бинарный) метод возведения в степень	5.1. Использование ключей больших степеней при шифровании асимметричных алгоритмов
6. Вероятностный тест Миллера-Рабина	6.1. Определение ключей на простоту
7. Криптосистема Эль-Гамала, ее корректность*	7.1. Алгоритмы с открытыми ключами
<b>Содержательный модуль 3. Криптография на эллиптических кривых</b>	
8. Эллиптическая криптография*	8.1. Свойства ключей, используемых в асимметричных алгоритмах шифрования
<b>Содержательный модуль 4. Электронно-цифровая подпись. Хэш-функции</b>	
9. Схемы построения электронно-цифровой подписи (ЭЦП)*	9.1. Использование ЭЦП в текстах, пересылаемых по компьютерным сетям
10. Стандартные хэш-функции*	10.1. Сжатие исходной информации с помощью хэш-функций для построения ЭЦП
11. Криптопротоколы*	11.1. Использование криптопротоколов для пересылки секретной информации

\* – практико-ориентированные темы.

**Структура дисциплины «Современные методы криптографии» по видам учебной деятельности**

Названия содержательных модулей и тем	Количество часов									
	Очная форма обучения					Заочная форма обучения				
	Всего	В Т.Ч.				Всего	В Т.Ч.			
		Лекции	Практические	Лабораторные	Самостоятельная работа		Лекции	Практические	Лабораторные	Самостоятельная работа
Содержательный модуль 1. Введение в современную криптографию										
1. Обзор сведений из теории чисел, используемых при защите информации	14	1	1	2	10	–	–	–	–	–
2. Новые направления в теории защиты информации	16	1	1	4	10	–	–	–	–	–
Итого по содержательному модулю 1	30	2	2	6	20	–	–	–	–	–

<b>Содержательный модуль 2. Криптосистемы с открытым ключом</b>										
3. Стандарт асимметричного шифрования RSA	28	2	4	2	20	–	–	–	–	–
4. Корректность криптосистемы, эффективность и надежность	13	1		2	10	–	–	–	–	–
5. Ускоренный (бинарный) метод возведения в степень	26	2	2	2	20	–	–	–	–	–
6. Вероятностный тест Миллера-Рабина	15	2	2	6	5	–	–	–	–	–
7. Криптосистема Эль-Гамала, ее корректность	19	2	1	6	10	–	–	–	–	–
<b>Итого по содержательному модулю 2</b>	<b>101</b>	<b>9</b>	<b>9</b>	<b>18</b>	<b>65</b>	–	–	–	–	–
<b>Содержательный модуль 3. Криптография на эллиптических кривых</b>										
8. Эллиптическая криптография	16	2	3	6	5	–	–	–	–	–
<b>Итого по содержательному модулю 3</b>	<b>16</b>	<b>2</b>	<b>3</b>	<b>6</b>	<b>5</b>	–	–	–	–	–
<b>Содержательный модуль 4. Электронно-цифровая подпись. Хэш-функции</b>										
9. Схемы построения электронно-цифровой подписи (ЭЦП)	12	2	2	2	6	–	–	–	–	–
10. Стандартные хэш-функции	12	4		2	6	–	–	–	–	–
11. Криптопротоколы	11	1	2	2	6	–	–	–	–	–
<b>Итого по содержательному модулю 4</b>	<b>35</b>	<b>7</b>	<b>4</b>	<b>6</b>	<b>18</b>	–	–	–	–	–
<b>Всего часов</b>	<b>180</b>	<b>18</b>	<b>18</b>	<b>36</b>	<b>108</b>	–	–	–	–	–

## 5. ТЕМАТИКА ЛЕКЦИОННЫХ, ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ ЗАНЯТИЙ

### Темы лекционных занятий

№ п/п	Название темы	Количество часов	
		Очная форма	Заочная форма
1	Введение	1	–
2	История криптографии	1	–
3	Следствие из алгоритма Эвклида	1	–
4	Криптосистемы с открытыми ключами. Новые направления в криптографии	1	–
5	Стандарт асимметричного шифрования RSA	1	–
6	Система RSA	1	–
7	Надежность RSA	2	–
8	Где брать нужные числа?	1	–
9	Тестирование простоты	1	–
10	Вероятностный тест Миллера-Рабина	1	–
11	Введение в криптосистему Эль-Гамала	1	–
12	Криптосистема Эль-Гамала	1	–
13	Введение в эллиптическую криптографию	1	–
14	Эллиптические кривые над конечными полями	1	–
15	Шифрование и дешифрование на эллиптических кривых	1	–
16	Программный комплекс шифрования на эллиптических кривых	1	–
17	Электронно-цифровая подпись	1	–
<b>Всего</b>		<b>18</b>	–

Тексты лекций приведены: см. рекомендованную литературу [2], информационные ресурсы [2].

### Темы практических занятий

№ п/п	Название темы	Количество часов	
		Очная форма	Заочная форма
1	Нахождение взаимнообратного числа по заданному модулю	2	–
2	Стандарт ассимметричного шифрования RSA	2	–
3	Бинарный метод возведения в степень	2	–
4	Алгоритм шифрования Эль-Гамала	2	–
5	Алгоритм Миллера-Рабина	2	–
6	Построение точек эллиптической кривой	2	–
7	Сложение точек эллиптической кривой	2	–
8	Шифрование с помощью эллиптической криптографии	4	–
<b>Всего</b>		<b>18</b>	<b>–</b>

Планы практических занятий с указанием рассматриваемых вопросов и выполняемых заданий приведены: см. рекомендованную литературу [1], информационные ресурсы [2].

### Темы лабораторных работ

№ п/п	Название темы	Количество часов	
		Очная форма	Заочная форма
1	Вычисление взаимнообратных чисел. НОД (a, b)	4	–
2	Решето Эратосфена	2	–
3	Ускоренный (бинарный) метод возведения в степень, RSA	6	–
4	Алгоритм Миллера-Рабина	6	–
5	Криптосистема Эль-Гамала	6	–
6	Основы эллиптической криптографии	6	–
7	Шифрование на эллиптических кривых	6	–
<b>Всего</b>		<b>36</b>	<b>–</b>

Содержание лабораторных работ и методические рекомендации к их выполнению приведены: см. рекомендованную литературу [1], информационные ресурсы [2].

## 6. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

№ п/п	Название темы	Количество часов	
		Очная форма	Заочная форма
1	Описание дисциплины	5	–
2	Краткие сведения из теории чисел, используемых в криптографии	5	–
3	Корректность системы RSA	5	–
4	Бинарный метод возведения в степень	5	–
5	Корректность системы	6	–
6	Псевдопростые числа	5	–
7	Генерирование случайного простого числа	6	–
8	Арифметические операции над точками эллиптической кривой	5	–
9	Аналог бинарного возведения в степень для скалярного умножения точек эллиптической кривой	6	–
10	Эллиптическая криптография.	5	–
11	Построение точек эллиптической кривой	5	–
12	Арбитраж ЭЦП	5	–



13	Хэш-функция – ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012	6	–
14	Типы хэш-функций	5	–
15	Проверка ЭЦП	6	–
16	Генерация ЭЦП	5	–
17	Хэш-функции. Общие сведения	5	–
18	Стандарт Security Hash Algorithm (Безопасная хэш-функция)	5	–
19	Создание и применение криптографических протоколов. Область применения	4	–
20	Пример простого криптопротокола ключевого обмена	4	–
21	Протоколы аутентификации. Простая аутентификация Применение схем одноразовых паролей	5	–
<b>Всего</b>		<b>108</b>	<b>–</b>

Содержание самостоятельной (в т.ч. индивидуальной) работы по темам и методические рекомендации по ее выполнению приведены: см. рекомендованную литературу [1, 2].

## 7. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

### Содержательный модуль 2. Криптосистемы с открытым ключом

1. Выбор ключей для асимметричных алгоритмов.
2. Корректность системы RSA. Доказательство взаимнообратности алгоритмов шифрования и дешифровки.
3. Бинарный метод возведения в степень.
4. Вероятностный тест Миллера-Рабина.
5. Использование алгоритма Эвклида и его следствия при определении дешифрующих ключей.
6. Криптосистема Эль-Гамала. Выбор ключей.
7. Выбор ключей для асимметричных алгоритмов.

## 8. ОБРАЗЕЦ ЗАДАНИЯ МОДУЛЬНОГО КОНТРОЛЯ

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Образовательная программа: магистратура

Направление подготовки: 01.04.02 Прикладная математика и информатика

Магистерская программа: Прикладная математика и информатика

Очная форма обучения. Семестр: 1

Учебная дисциплина: Современные методы криптографии

### Модульная контрольная работа

#### Вариант № 1

1. Криптосистема Эль-Гамала, Выбор ключей, шифрование.
2. Проверить число 49 на простоту по методу Миллера-Рабина по двум основаниям  $x = 2$ ; 3.

## 9. КРИТЕРИИ ОЦЕНИВАНИЯ ЗАДАНИЯ МОДУЛЬНОГО КОНТРОЛЯ

Номер задания	Количество баллов
Задание 1	20
Задание 2	20
<b>Всего</b>	<b>40</b>

## 10. ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Образовательная программа: магистратура

Направление подготовки: 01.04.02 Прикладная математика и информатика

Магистерская программа: Прикладная математика и информатика

Очная форма обучения. Семестр: 1

Учебная дисциплина: Современные методы криптографии

### Экзаменационный билет № 1

1. Тестирование простоты.
2. Эллиптические кривые над конечными полями.
3. Проверить число 49 на простоту по методу Миллера-Рабина по двум основаниям  $x = 2; 3$ .

Утверждено на заседании теории упругости и вычислительной математики имени академика А.С. Космодаманского, протокол № \_\_\_\_ от «\_\_\_\_» \_\_\_\_\_ 20\_\_ г.

Заведующий кафедрой

Экзаменатор

\_\_\_\_\_ ФИО

\_\_\_\_\_ ФИО

## 11. КРИТЕРИИ ОЦЕНИВАНИЯ ЭКЗАМЕНАЦИОННОГО ЗАДАНИЯ

Номер задания	Количество баллов
Задание 1	30
Задание 2	30
Задание 3	40
<b>Всего</b>	<b>100</b>

## 12. КРИТЕРИИ ОЦЕНИВАНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Самостоятельная работа (включая выполнение СРС и ИРС) оценивается в 55 баллов. В разрезе отдельных тем оценивание осуществляется следующим образом.

### Оценивание СРС и ИРС по дисциплине «Современные методы криптографии»

Названия содержательных модулей и тем	СРС	ИРС
<b>Содержательный модуль 1. Введение в современную криптографию</b>		
1. Обзор сведений из теории чисел, используемых при защите информации	–	2
2. Новые направления в теории защиты информации	–	3
<b>Итого по 1-му содержательному модулю</b>	<b>–</b>	<b>5</b>

<b>Содержательный модуль 2. Криптосистемы с открытым ключом</b>		
3. Стандарт ассиметричного шифрования RSA	1	3
4. Корректность криптосистемы, эффективность и надежность	1	3
5. Ускоренный (бинарный) метод возведения в степень	1	3
6. Вероятностный тест Миллера-Рабина	1	3
7. Криптосистема Эль-Гамала, ее корректность	1	3
<b>Итого по 2-му содержательному модулю</b>	<b>5</b>	<b>15</b>
<b>Содержательный модуль 3. Криптография на эллиптических кривых</b>		
8. Эллиптическая криптография	5	10
<b>Итого по 3-му содержательному модулю</b>	<b>5</b>	<b>10</b>
<b>Содержательный модуль 4. Электронно-цифровая подпись. Хэш-функции</b>		
9. Схемы построения электронно-цифровой подписи (ЭЦП)	2	3
10. Стандартные хэш-функции	1	4
11. Криптопротоколы	2	3
<b>Итого по 4-му содержательному модулю</b>	<b>5</b>	<b>10</b>
<b>Всего баллов</b>	<b>15</b>	<b>40</b>

### 13. КРИТЕРИИ ОЦЕНИВАНИЯ ОБЩЕЙ УСПЕВАЕМОСТИ

Общая оценка знаний студентов по дисциплине проводится по 100-балльной шкале согласно таким критериям, приведенным в таблице ниже. *Организационно-учебная работа студента* в аудитории оценивается на основе таких критериев как посещаемость занятий, активность во время проведения лекционных и практических занятий (вопросы лектору по теме лекционного материала, участие в обсуждении пройденного материала и т.п.).

<b>Содержательные модули</b>	<b>Вид работы</b>	<b>Баллы</b>
Содержательный модуль 1	Организационно-учебная работа студента в аудитории	1
	Самостоятельная работа	5
	<b>Итого</b>	<b>6</b>
Содержательный модуль 2	Организационно-учебная работа студента в аудитории	2
	Самостоятельная работа	20
	<b>Итого</b>	<b>22</b>
Содержательный модуль 3	Организационно-учебная работа студента в аудитории	1
	Самостоятельная работа	15
	<b>Итого</b>	<b>16</b>
Содержательный модуль 4	Организационно-учебная работа студента в аудитории	1
	Самостоятельная работа	15
	Модульная контрольная работа	40
	<b>Итого</b>	<b>56</b>
<b>Экзамен</b>		<b>100</b>
<b>Общий итог</b>		<b>100</b>

#### Порядок оценивания учебных достижений обучающихся

Оценка по шкале ECTS	Оценка по 100-балльной шкале	Оценка по государственной шкале	
		экзамен, дифференцированный зачет	зачет
A	90-100	5 (отлично)	зачтено
B	80-89	4 (хорошо)	зачтено
C	75-79	4 (хорошо)	зачтено

D	70-74	3 (удовлетворительно)	зачтено
E	60-69	3 (удовлетворительно)	зачтено
FX	35-59	2 (неудовлетворительно) с возможностью повторной аттестации	не зачтено
F	0-34	2 (неудовлетворительно) с возможностью повторной сдачи при условии обязательного набора дополнительных баллов	не зачтено

#### 14. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в Главном учебном корпусе (г. Донецк, пр. Гурова, 6) университета. Для проведения лекционных и практических занятий требуется аудитория, оборудованная меловой или маркерной доской, 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, материально-техническую базу учебных лабораторий кафедры теории упругости и вычислительной математики имени академика А.С. Космодамианского.

В процессе обучения студенты имеют возможность использовать учебные материалы по дисциплине «Современные методы криптографии», размещенные на платформе Moodle Центра дистанционного образования ГОУ ВПО «ДонНУ». С использованием ресурсов платформы дистанционного образования также осуществляется текущий контроль знаний студентов на основе тестирования и проверки результатов самостоятельной работы.

#### 15. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонНУ	Наличие электронной версии в ЭБС
<b>Основная литература</b>			
1.	Практический курс по современным методам криптографии: учебно-методическое пособие / Сост.: Л.Н. Шкодина, А.И. Занько. – Донецк: ДонНУ, 2019. – 86 с.	–	+
2.	Современные методы криптографии: учебное пособие / Сост.: Л.Н. Шкодина, А.И. Занько. – Донецк: ДонНУ, 2019. – 119 с.	–	+
<b>Дополнительная литература</b>			
3.	Бородин А.И. Теория чисел. – К.: Выща шк., 1992. – 288 с.	25	–
4.	Вербіцький О.В. Вступ до криптології. – Львів: Видавн. наук.-техн. літ-ри. – 1998. – 247 с.	1	–
5.	Мао В. Современная криптография: теория и практика. – М.: Вильямс, 2005. – 763 с.	2	–
6.	ван Тилборг Х.К.А. Основы криптологии: Проф. руководство и интерактивный учебник. – М.: Мир, 2006. – 471 с.	4	–



## **16. ИНФОРМАЦИОННЫЕ РЕСУРСЫ**

1. Электронно-библиотечная система Донецкого национального университета: <http://library.donnu.ru/> (дата обращения: 01.04.2021).
2. Современные методы криптографии: электрон. учеб.-метод. комплекс по дисциплине в LMS Moodle: <http://dl-test.donnu-support.ru/course/view.php?id=517> (дата обращения: 01.04.2021).

## **17. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ**

1. Windows 7 PRO (корпоративная лицензия ДОННУ № 46484614);
2. Microsoft Office (корпоративная лицензия ДОННУ № 46472919);
3. Microsoft Visual Studio (лицензия программы DreamSpark для высших учебных заведений).