ГОУ ВПО «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
«22» апреля 2020 г.
МП

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ «СОВРЕМЕННЫЕ МЕТОДЫ КРИПТОГРАФИИ»

Направление подготовки:	01.04.02 Прикладная математика и информатика
Магистерская программа:	Прикладная математика и информатика
Образовательная программа:	академическая магистратура
Квалификация:	магистр
Форма обучения:	очная, очно-заочная, заочная нужное подчеркнуть

Донецк 2020

УТВЕРЖДАЮ:
Декан факультета математики
и информационных технологий
_____ И. А. Моисеенко
«16» апреля 2020 г.
МП

Программа составлена на основании Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) направления подготовки 01.04.02 Прикладная математика и информатика, утвержденного приказом Министерства образования и науки Российской Федерации от «12» марта 2015 г. № 228;
Порядка организации учебного процесса в образовательных организациях высшего профессионального образования Донецкой Народной Республики, утвержденного приказом Министерства образования и науки ДНР № 1171 от «10» ноября 2017 г.;
учебного плана и основной образовательной программы Прикладная математика и информатика, направления подготовки 01.04.02 Прикладная математика и информатика, разработанных в ГОУ ВПО «Донецкий национальный университет».

Разработчик:
Доцент кафедры теории упругости и
вычислительной математики имени
академика А.С. Космодамианского _____ Л.Н. Шкодина

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

Протокол № 11 от «9» апреля 2020 г.
Заведующий кафедрой _____ В.И. Сторожев

Программа учебной дисциплины одобрена учебно-методической комиссией факультета математики и информационных технологий
Протокол № 8 от «15» апреля 2020 г.

Председатель учебно-методической
комиссии факультета _____ Л.И. Селякова

1. ОБЛАСТЬ ПРИМЕНЕНИЯ И МЕСТО ДИСЦИПЛИНЫ В УЧЕБНОМ ПРОЦЕССЕ

Курс «Современные методы криптографии» является дисциплиной вариативной части по направлению подготовки 01.04.02 Прикладная математика и информатика (магистерская программа: прикладная математика и информатика).

Дисциплина реализуется на факультете математики и информационных технологий кафедрой теории упругости и вычислительной математики.

Этот курс, опираясь на математическую (математический анализ, численные методы, алгебра и геометрия, программирование и др.), философскую, психолого-педагогическую подготовку (психология, педагогика) студентов, закладывает фундамент для преддипломной практики и написания магистерской диссертации.

Полученные знания используются студентами во время выполнения научно-исследовательской работы при написании магистерской диссертации.

2. СТРУКТУРА ДИСЦИПЛИНЫ

Характеристика учебной дисциплины		
Направление подготовки	01.04.02 Прикладная математика и информатика	
Магистерская программа	прикладная математика и информатика	
Образовательная программа	академическая магистратура	
Квалификация	магистр	
Количество содержательных модулей	4	
Дисциплина базовой / вариативной части образовательной программы	дисциплина вариативной части	
Формы контроля (МК, экзамен, зачет)	1 модульный контроль, 1 экзамен	
Показатели	очная форма обучения	заочная форма обучения
Количество зачетных единиц (кредитов)	5	
Год подготовки	1	
Семестр	1	
Количество часов	180	
- лекционных	18	
- практических, семинарских	18	
- лабораторных	36	
- самостоятельной работы	108	
в т.ч. индивидуальное задание		
Недельное количество часов,	10	
в т.ч. аудиторных	4	

3. ОПИСАНИЕ ДИСЦИПЛИНЫ

Цели и задачи

Целью изучения дисциплины «Современные методы криптографии***»*** являются:

– 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;

Основными задачами изучения дисциплины являются:

– 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 направления подготовки 01.04.02 «Прикладная математика и информатика» и основной образовательной программы высшего профессионального образования направления подготовки 01.04.02 Прикладная математика и информатика (магистерская программа: прикладная математика и информатика):

а) ***общекультурных (ОК):*** способность к абстрактному мышлению, анализу, синтезу (ОК-1); готовность к саморазвитию, самореализации, использованию творческого потенциала (ОК-3);

б) ***общепрофессиональных (ОПК):*** способность использовать и применять углубленные знания в области прикладной математики и информатики (ОПК-4);

в) профессиональных (ПК):

***проектная и производственно-технологическая деятельность*:** способностью разрабатывать и применять математические методы, системное и прикладное программное обеспечение для решения задач научной и проектно-технологической деятельности (ПК-3).

В результате изучения учебной дисциплины студент должен:

знать:

– определения и термины теории защиты информации;

– современные методы криптографии – криптосистемы с открытыми ключами: RSA, Эль-Гамаля и др.;

– современные алгоритмы защиты информации;

– ускоренный метод возведения в степень;

– математический аппарат, на котором базируется современная теория защиты информации - операции в классе вычетов, тесты простоты;

уметь:

– преобразовывать открытый текст в криптограмму современными методами;

– использовать методы тестирования чисел на простоту;

составлять программы для преобразования открытого текста в криптотекст и наоборот.

владеть:

– навыками работы с современными языками программирования для реализации криптографических алгоритмов на ЭВМ.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И ФОРМЫ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА

Порядковый номер и тема	Краткое содержание темы
Содержательный модуль 1	
Тема 1. Обзор сведений из теории чисел, используемых при защите информации	Обзор основных терминов, определений и задачи классической криптографии,
Тема 2. Новые направления в теории защиты информации	Использование функций с секретом в асимметричных алгоритмах шифрования
Содержательный модуль 2	
Тема 3. Стандарт ассиметричного шифрования RSA, примеры	Ключи шифрования и дешифровки. Алгоритм шифрования.
Тема 4. Корректность криптосистемы,	Теорема о стойкости криптосистемы RSA,

эффективность и надежность	
Тема 5. Ускоренный (бинарный) метод возведения в степень	Использование ключей больших степеней при шифровании асимметричных алгоритмов
Тема 6. Криптоситсема Эль-Гамаля, ее корректность	Алгоритмы с открытыми ключами
Содержательный модуль 3	
Тема 7. Эллиптическая криптография	Свойства ключей, используемых в асимметричных алгоритмах шифрования
Тема 8. Вероятностный тест Миллера-Рабина. Примеры	Определение ключей на простоту
Содержательный модуль 4	
Тема 9. Схемы построения ЭЦП	Использование в текстах, пересылаемых по компьютерным сетям ЭЦП
Тема 10. Стандартные хэш-функции	Сжатие исходной информации с помощью хэш-функций для построения ЕЦП
Тема 11. Криптопротоколы	Использование для пересылки секретной информации криптопротоколов

Тематический план

Содержательный модуль 1												
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	индивидуальн		лекции	практические	лабораторные	самостоятельн	индивидуальн
Тема 1. Обзор сведений из теории чисел, используемых при защите информации	14	1	1	2	10							
Тема 2. Новые направления в теории защиты информации	16	1	1	4	10							
Итого по содержательному модулю 1	**30**	**2**	**2**	**6**	**20**							
Тема 3. Стандарт ассиметричного шифрования RSA, примеры	28	2	4	2	20							
Тема 4. Корректность криптосистемы, эффективность и надежность	13	1		2	10							
Тема 5. Ускоренный (бинарный) метод возведения в степень	26	2	2	2	20							
Тема 6.	19	2	1	6	10							

Криптоситсема Эль-Гамаля, ее корректность												
Итого по содержательному модулю 2	**84**	**7**	**7**	**12**	**60**							
Тема 7. Эллиптическая криптография	16	2	3	6	5							
Тема 8. Вероятностный тест Миллера-Рабина. Примеры	15	2	2	6	5							
Итого по содержательному модулю 3	**31**	**4**	**5**	**12**	**10**							
Тема 9. Схемы построения ЭЦП	12	2	2	2	6							
Тема 10. Стандартные хэш-функции	12	4		2	6							
Тема 11. Криптопротоколы	11	1	2	2	6							
Итого по содержательному модулю 4	**35**	**7**	**4**	**6**	**18**							
Всего по дисциплине	**180**	**18**	**18**	**36**	**108**							

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРОВЕДЕНИЯ ЛЕКЦИОННЫХ, ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Темы лекционных занятий

№ п/п	***Название темы***	***Количество часов***
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	Введение в криптосистему Эль-Гамаля	1
9	Криптосистема Эль-Гамаля	1
10	Где брать нужные числа?	1
11	Тестирование простоты	1
12	Вероятностный тест Миллера-Рабина	1
13	Введение в эллиптическую криптографию	1
	Эллиптические кривые над конечными полями	1
	Шифрование и дешифрование на эллиптических кривых	1
	Программный комплекс шифрования на эллиптических кривых	1
	Электронно-цифровая подпись	1

	ВСЕГО	**18**

Темы лабораторных занятий

№ п/п	*Название темы*	*Количество часов*
1.	Вычисление взаимнообратных чисел. НОД (a, b)	4
2.	Решето эратосфена	3
3.	Ускоренный (бинарный) метод возведения в степень, RSA	6
4.	Алгоритм Миллера-Рабина	6
5.	Криптосистема эль-гамаля	6
6.	Основы эллиптической криптографии	5
7.	Шифрование на эллиптических кривых	6
	ВСЕГО	**36**

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

№ п/п	*Название темы*	*Количество часов*
1.	Нахождение взаимнообратного числа по модулю 29.	2
2.	Стандарт ассимметричного шифрования RSA	3
3	Бинарный метод возведения в степень	2
4	Алгоритм шифрования Эль-Гамаля-	2
5	Алгоритм Миллера-Рабина	2
6	Построение точек эллиптической кривой	2
7	Сложение точек эллиптической кривой	2
8	Шифрование с помощью эллиптической криптографии	3
	ВСЕГО	**18**

6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Организация самостоятельной работы студентов

(*соответственно данным в таблице тематического плана*)

№ п/п	*Название темы*	*Количество часов*
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 Р34.-94	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 крипто протокола ключевого обмена	4
21.	Протоколы аутентификации. Простая аутентификация Применение схем одноразовых паролей	5
	ВСЕГО	**108**

7. ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ

(*если предусмотрено программой*)

Индивидуальная работа

Пусть задана эллиптическая кривая $y^2 = x^3 + x + 1$. Для этой кривой раньше была простроена группа точек $E_{23}(1,1)$. В этой группе найдем:

1) сумму точек $P = (3,10)$ и $Q = (9,7)$; 2) $2P = P + P$, для точки $P = (3,10)$.

1. Так как $P \neq Q$, то величина λ вычисляется по первой ветви в формуле (3)

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \bmod 23 = \frac{7-10}{9-3} \bmod 23 = \frac{-3}{6} \bmod 23 =$$

$$= -\frac{1}{2} \bmod 23 = -2^{-1} \bmod 23 = -12 \bmod 23 = 11,$$

$$x_3 = \left(\lambda^2 - x_1 - x_2\right) \bmod 23 = \left(11^2 - 3 - 9\right) \bmod 23 =$$

$$= (121 - 12) \bmod 23 = 109 \bmod 23 = 17,$$

$$y_3 = \left(\lambda(x_1 - x_3) - y_1\right) \bmod 23 = \left(11(3-17) - 10\right) \bmod 23 =$$

$$= -(154 - 10) \bmod 23 = -164 \bmod 23 = 20 \bmod 23.$$

Получили $P + Q = (3,10) + (9,7) = (17,20)$.

2. В этом случае находим $2 \cdot P = 2 \cdot (3,10)$ и величина λ находится по второй ветви в формуле (3). Учтем, что в нашей кривой величина $b = 1$.

$$\lambda = \frac{3x_1^2 + b}{2y_1} \bmod 23 = \frac{3 \cdot 3^2 + 1}{2 \cdot 10} \bmod 23 = \frac{27+1}{20} \bmod 23 =$$

$$= \frac{28}{20} \bmod 23 = \frac{5}{20} \bmod 23 = \frac{1}{4} \bmod 23 = 4^{-1} \bmod 23 = 6.$$

Теперь определим координаты x_3 и y_3

$$x_3 = \left(\lambda^2 - x_1 - x_2\right) \bmod 23 = \left(6^2 - 3 - 3\right) \bmod 23 = 30 \bmod 23 = 7,$$

$$y_3 = \left(\lambda\left(x_1 - x_3\right) - y_1\right) \bmod 23 = \left(6\left(3 - 7\right) - 10\right) \bmod 23 = -34 \bmod 23 = 12.$$

Таким образом, $2 \cdot P = 2 \cdot (3, 10) = (7, 12)$.

Полученные результаты $(17, 20)$ и $(7, 12)$ также являются точками группы $E_{23}(1, 1)$.

После построения группы точек $E_p(b, c)$ и нахождения генерирующей точки $G = (\bar{x}, \bar{y})$ необходимо сопоставить выбранный алфавит для шифрования точкам группы. Обмен информацией между участниками A и B осуществляется следующим образом. Участник B выбирает личный ключ n_b меньше p и генерирует открытый ключ $P_b = n_b * G$. Чтобы зашифровать и послать сообщение P_m пользователю B, участник A выбирает случайное положительное число $k < p$ и зашифровывает сообщение по формуле

$$E(P_m) = C_m = \left(C_m^1, C_m^2\right) = \{k \cdot G,\ P_m + kP_b\}. \quad (4)$$

Здесь участник A использует открытый ключ участника B: P_b.

Чтобы дешифровать полученное сообщение $E(P_m)$, участник B проводит следующие вычисления:

$$D(C_m) = C_m^2 - n_b C_m^1 = P_m + kP_b - n_b(k \cdot G) = \\ = P_m + k(n_b \cdot G) - n_b(k \cdot G) \equiv P_m. \quad (5)$$

Пользователь A зашифровал сообщение P_m с помощью добавления к нему $k \cdot P_b$. Никто кроме этого пользователя не знает ключа k, поэтому хотя P_b является открытым ключом, никто не сможет убрать маску $k \cdot P_b$.

В лабораторной работе вначале для группы точек $E_{23}(1,1)$ составить подпрограммы сложения двух разных точек и умножения точки на целое число. Отладить подпрограммы на приведенном примере. Затем заменить группу точек $E_{23}(1,1)$ группой $E_{211}(0,-4)$, что соответствует кривой $y^2 = x^3 - 4$, $(b = 0,\ c = -4)$ и $G = (2, 2)$. Вычислить произведение $100 \cdot (2, 2)$.

8. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

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-Гамаля. Выбор ключей.
7. Выбор ключей для асимметричных алгоритмов

9. ОБРАЗЕЦ МОДУЛЬНОГО КОНТРОЛЯ

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Факультет математики и информационных технологий

Направление подготовки:	*01.04.02 Прикладная матеамтика и информатика*
Магистерская программа:	*прикладная матеамтика и информатика*
Программа подготовки:	*академическая магистратура*
Семестр	*1*
Учебная дисциплина	*Современные методы криптографии*

МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА
ВАРИАНТ №1

1. Криптосистема Эль-Гамаля, Выбор ключей, шифрование.
2. Проверить число n на простоту по методу Миллера-Рабина по двум основаниям x=2,3 (n=49)

Утверждено на заседании кафедрой теории упругости и вычислительной математики имени академика А.С. Космодамианского, протокол № ___ от “__” _____ 20__ г.

Зав. кафедрой _____
Преподаватель _____

Критерии оценивания модульного контроля

Номер задания	***Количество баллов***
Задание 1	20
Задание 2	20
Всего	***40***

10. ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Теоретические вопросы к экзамену

1. История криптографии
2. Следствие из алгоритма Эвклида
3. Криптосистемы с открытыми ключами. Новые направления в криптографии
4. Стандарт асимметричного шифрования RSA
5. Система RSA
6. Надежность RSA
7. Введение в криптосистему Эль-Гамаля
8. Криптосистема Эль-Гамаля
9. Где брать нужные числа?
10. Тестирование простоты
11. Вероятностный тест Миллера-Рабина
12. Введение в эллиптическую криптографию
13. Эллиптические кривые над конечными полями
14. Шифрование и дешифрование на эллиптических кривых
15. Программный комплекс шифрования на эллиптических кривых
16. Электронно-цифровая подпись
17. Алгоритм эцп – DSS

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Факультет математики и информационных технологий

Направление подготовки: ***01.04.02 Прикладная матеамтика и информатика***
Магистерская программа: ***прикладная матеамтика и информатика***
Программа подготовки: ***академическая магистратура***
Семестр ***I***
Учебная дисциплина ***Современные проблемы криптографии***

БИЛЕТ №1

1. Тестирование простоты
2. Эллиптические кривые над конечными полями
3. Пример.

Утверждено на заседании кафедрой теории упругости и вычислительной математики имени академика А.С. Космодамианского, протокол № ___ от "__" _____ 20__ г.

Зав. кафедрой _____
Экзаменатор _____

Критерии оценивания экзамена

Номер задания	***Количество баллов***
Задание 1	30
Задание 2	30
Задание 3	40
Всего	**100 баллов**

11. ОБРАЗЕЦ ТЕСТОВОГО ЗАДАНИЯ

Не предусмотрено программой.

12. КРИТЕРИИ ОЦЕНИВАНИЯ

По курсу предполагается проведение промежуточной аттестации в виде модульного контроля, выполнение индивидуальной работы и экзамена. Экзамен сдают студенты с целью повышения рейтинга.

Распределение баллов, которые могут получить студенты в процессе изучения дисциплины

Организационно учебная работа студента	**СРС**		**Всего**
	Индивидуальная работа	**Модульный контроль**	
Max 20 баллов	max 40 баллов	max 40 баллов	100 баллов

Шкала соответствия баллов национальной шкале

Оценка по шкале ECTS	**Оценка по 100-балльной шкале**	**Оценка по государственной шкале (экзамен, дифференцированный зачет)**	**Оценка по государственной шкале (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 сдачи	не зачтено
F	0-34	2 (неудовлетворительно) с возможностью повторной сдачи при условии обязательного набора дополнительных баллов	не зачтено

13. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Лекционные занятия проводятся в аудитории, оснащенной мультимедийной техникой и доской. Лабораторные и практические занятия проводятся в компьютерном классе, оборудованном доступом к сети Интернет, столами, доской.

14. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

№ п/п	**Наименование**	**Кол-во экземпляров в библиотеке ДонНУ**	**Наличие электронной версии в ЭБС**
	Основная литература		
1.	Основы интернет-технологий : учеб. пособие / Е. В. Авдюшина и др. ; Донецкий нац. ун-т. - Донецк : ДонНУ, 2013. - 154 с.	19	+
2.	Практический курс по современным методам криптографии [Электронный ресурс]: учебно-методическое пособие / Сост.: Л.Н.Шкодина, А.И.Занько; ГОУ ВПО «Донецкий национальный университет». – Донецк: ДонНУ, 2017. – Электронные данные	0	+
3.	Современные методы криптографии [Электронный ресурс]: учебное пособие / Сост.: Л.Н.Шкодина, А.И.Занько; ГОУ ВПО «Донецкий национальный университет». – Донецк: ДонНУ, 2017. – Электронные данные	0	+
	Дополнительная литература		
4.	Бородин, А.И. Теория чисел: учеб. пособие для ун-тов по спец. "Математика" / А.И.Бородин. - Киев: Выща шк., 1992. - 288 с.	25	-
5.	Вербицький, О.В. Вступ до криптології. Видавн. наук.-техн. літератури. Львів. – 1998. – 247 с.	1	-
6.	Калоеров, С.А. Программирование на С++: учеб. пособие / С.А.Калоеров; Донецкий нац. ун-т. – Изд. 3-е. – Донецк: Уго-Восток, 2009. – 298 с.	101	-
7.	Коноплева, И. А. Информационные технологии : учебное пособие / И. А. Коноплева, О. А. Хохлова, А. В. Денисов. - 2-е изд. - Москва : Проспект, 2014. - 327 с.	3	-

8.	Мао, В. Современная криптография: теория и практика / Венбо Мао; [пер. с англ. и ред. Д.А.Клюшина]; Компания Hewlet-packard. - М.: Вильямс, 2005. - 763 с.	2	-
9.	Методические указания к выполнению лабораторных работ по курсу "Управление информацией и знаниями" : для студентов направления подготовки 6.050101 "Компьютерные науки" специальности 7.05010104 "Системы искусственного интеллекта" / [сост. Т. В. Шарий] ; ДонНУ. Физ.-техн. фак. Каф. компьютерных технологий. - Донецк : ДонНУ, 2013. - 48 с. (1 экз.).	1	-
10.	Михеева, Е. В. Информационные технологии в профессиональной деятельности : учеб. пособие / Е. В. Михеева. - Москва : Проспект, 2013. - 448 с.	3	-
11.	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.	1	-
12.	Основы криптографии : (письменная справка) / [сост. Н. А. Фесенко] ; ДонНУ. Науч. б-ка. Справ.-библиогр. отд. - Донецк : ДонНУ, 2015. - 16 с. (1 экз.)	1	+
13.	Прийменко, С. А. Компьютерные сети : учеб. пособие / С. А. Прийменко, Р. Н. Нескородев, Я. А. Арчаков ; Донецкий нац. ун-т. - Донецк : ДонНУ, 2013. - 97 с. (12 экз.).	12	+
14.	Рублинецкий, В.И. Введение в компьютерную криптологию / Харьк. гуманит. ин-т "Нар. укр. акад.". - Харьков: ОКО, 1997. - 128 с.	1	-
15.	Рябко, Б.Я. Криптографические методы защиты информации: учеб. пособие для студентов вузов, обучающихся по специальностям: 201000 (210404) - "Многоканал. телекоммуникац. системы", 201100 (210405) - "Радиосвязь, радиовещание и телевидение", 201800 (210403) - "Защищ. системы связи" / Б.Я.Рябко, А.Н.Фионов. - М.: Горячая линия-Телеком, 2005. - 229 с. (5 экз.)	5	-
16.	Скобелев, В.Г. Введение в криптологию: учеб. пособие / В.Г.Скобелев; Донецкий нац. ун-т. - Донецк: Юго-Восток, 2008. - 175 с. (15 экз.)	15	-
17.	Теоретические основы компьютерной безопасности: Учеб. пособие для вузов по специальности «Компьютерная безопасность и др.» / П.Н.Девянин, О.О.Михальский, Д.И.Правиков и др. М.: Радио и связь, 2000. – 192 с. (16 экз.)	16	-
18.	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. (4 экз.+ электрон. опт. диск (CD-ROM)).	4	-

19.	Шкодина, Л.Н. Построение хэш-функции и создание электронно-цифровой подписи с использованием симметричного и ассиметричного шифров / Л.Н.Шкодина // Вестник ДонНУ. Сер.А. Естественные науки, 2016, Вып.3. – С.50-54. (1 экз.)	1	-
20.	Бородин, А.И. Теория чисел: учеб. пособие для ун-тов по спец. "Математика" / А.И.Бородин. - Киев: Выща шк., 1992. - 288 с.	25	-
21.	Вербицький, О.В. Вступ до криптології. Видавн. наук.-техн. літератури. Львів. – 1998. – 247 с. (1 экз.)	1	-

15. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

http://vak.mondnr.ru/ Высшая Аттестационная комиссия при Министерстве образования и науки Донецкой Народной Республики
http://vak.ed.gov.ru/ ВЫСШАЯ АТТЕСТАЦИОННАЯ КОМИССИЯ (ВАК) при Министерстве науки и высшего образования Российской Федерации
http://vak.ed.gov.ru/87 Перечень рецензируемых научных изданий
http://mondnr.ru/ – Министерство образования и науки Донецкой Народной Республики
http://mondnr.ru /– Министерство образования и науки Донецкой Народной республики
https://www.donippo.org/ – ГОУ ДПО «Донецкий республиканский институт дополнительного педагогического образования»
http://ippo-vm.at.ua/ – Отдел математики Донецкого РИДПО
http://resobrnadzor.ru/ – Республиканская служба по контролю и надзору в сфере образования и науки

16. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДОННУ № 46484614);
2. Microsoft Office (корпоративная лицензия ДОННУ лицензия № 46472919);
3. Microsoft Visual Studio (лицензия программы DreamSpark для высших учебных заведений);
4. Лицензии GPL, Apache, BSD для свободного программного обеспечения: FreeLab, Scilab, R Studio, Python, Eclipse, Free Pascal, Tries Mode, Prolog, Антивирус Касперского, Linux Fedora, Libre Office, Adobe Acrobat Reader, xPDF, Blender, КОМПАС-3D LT, Paint.NET, Gimp.

Рабочая программа рассмотрена и переутверждена на заседании кафедры теории упругости и вычислительной математики имени академика А.С. Космодамианского с изменениями (без изменений) на 20____ год.
Протокол № ___ от “___” _____ 20__ г.

Заведующий. кафедрой _____ В.И. Сторожев

Рабочая программа рассмотрена и переутверждена на заседании кафедры теории упругости и вычислительной математики имени академика А.С. Космодамианского с изменениями (без изменений) на 20____ год.
Протокол № ___ от “___” _____ 20__ г.

Заведующий. кафедрой _____ В.И. Сторожев