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 «МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Направление подготовки:	01.03.02 Прикладная математика и информатика
Образовательная программа:	бакалавриат
Квалификация:	Академический бакалавр
Форма обучения:	очная, очно-заочная, заочная, в том числе с ускоренным сроком обучения нужное подчеркнуть

Донецк 2020

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

Программа учебной дисциплины «Математические основы защиты информации» составлена на основании Государственного образовательного стандарта высшего профессионального образования (ГОС ВПО) Донецкой Народной Республики (ДНР) по направлению подготовки 01.03.02 Прикладная математика и информатика, утвержденного приказом Министерства образования и науки ДНР от «04» апреля 2016 г. № 280;
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 высшего профессионального образования направления подготовки 01.03.02 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

Учебная дисциплина «Математические основы защиты информации» относится вариативной части профессионального блока и состоит из одного модуля.

В рамках преподавания дисциплины изучаются классические криптографические алгоритмы.

Содержание дисциплине основывается на базе дисциплин:

Б.2.Б.1, Б2.Б.1, Б2.Б.2 Математический анализ

ПБ. Б.17 Численные методы

Б2.Б.4 Алгебра и геометрия

Б2.Б.8 Программирование

Является основой для следующих дисциплин:

ПБ.ВО.1 Современные методы криптографии,

Б2.Б.П.19 Курсовая работа

2. СТРУКТУРА ДИСЦИПЛИНЫ

Характеристика учебной дисциплины				
Направление подготовки	01.03.02 Прикладная математика и информатика			
Профиль				
Образовательная программа	бакалавриат			
Квалификация	Академический бакалавр			
Количество содержательных модулей	4 (11)			
Дисциплина базовой / вариативной части образовательной программы	Вариативная часть профессионального блока			
Формы контроля (МК, экзамен, зачет)	модульный контроль, экзамен			
Показатели	очная форма обучения		заочная форма обучения	
	нормат. срок	ускор. срок	нормат. срок	ускор. срок
Количество зачетных единиц (кредитов)	4	4		
Год подготовки	3	2		
Семестр	6	4		
Количество часов	144	144		
- лекционных	34	34		
- практических, семинарских				
- лабораторных	34	34		
- самостоятельной работы	76	76		
в т.ч. индивидуальное задание				
Недельное количество часов,				
в т.ч. аудиторных	4	4		

3. ОПИСАНИЕ ДИСЦИПЛИНЫ

Цели и задачи

Цели:

- изучение различных 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 «Математические основы защиты информации» направлен на формирование элементов следующих компетенций в соответствии с ГОС ВПО ДНР по направлению подготовки 01.03.02 «Прикладная математика и информатика» и основной образовательной программы высшего профессионального образования направления подготовки 01.03.02 «Прикладная математика и информатика»:

а) общекультурных (ОК):

- способность к самоорганизации и самообразованию (ОК-7);

б) общепрофессиональных (ОПК):

- способность использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с прикладной математикой и информатикой (ОПК-1);
- способность к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям (ОПК-3);
- способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4);

в) профессиональных (ПК):

- способность работать в составе научно-исследовательского и производственного коллектива и решать задачи профессиональной деятельности (ПК-4);
- способность к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения (ПК-7);
- способность составлять и контролировать план выполняемой работы, планировать необходимые для выполнения работы ресурсы, оценивать результаты собственной работы (ПК-9).

В результате освоения дисциплины студент должен знать:

- определения и термины криптографии;
- классические методы шифрования – шифры простой замены, частотный анализ, полиграммные шифры, шифрование блоками;
- современные методы криптографии – подача текста в цифровой форме, шифры одноразового блокнота, DES;
- элементарные математические алгоритмы криптографии:
  - алгоритм Эвклида;
  - разложение на простые множители;
  - кольцо остатков, матриц, вероятностные алгоритмы;
- математический аппарат, на котором базируется современная криптография;
- первичные корни, квадратичные остатки, тесты простоты.

уметь:

- преобразовывать открытый текст в криптограмму методами простой замены;
- применять частотный анализ для взлома несложных криптосистем;
- использовать схему Виженера с ключом для тайнописи;
- шифровать текст в цифровой форме современными методами с помощью математического аппарата;
- составлять программы для преобразования открытого текста в криптотекст и наоборот.

Иметь навыки (приобрести опыт):

- 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: «Элементарная криптография»	
Тема 1. Криптография, ее понятия и терминология	Рассматриваются основные термины, определения и задачи криптографии.
Тема 2. Элементарные шифры. Частотный анализ.	Исторический обзор криптографических методов.
Содержательный модуль 2: «Классическая криптография	
Тема 3. Шифры Плейфера, Виженера.	Рассматриваются криптографические методы примерно 14–19 веков, их надежность, криптостойкость. Шифры Плейфера, Виженера.
Тема 4. Шифры перестановок. Матричный шифр обхода.	Изучаются на конкретных примерах вопросы криптоанализа методов. Шифр перестановки, матричный шифр обхода
Тема 5. Подача материала в цифровой форме, шифр одноразового блока. Причины успешного криптоанализа	Изучается представление информации в цифровой форме, шифр ШОБ
Содержательный модуль 3 «Математические основы криптографических методов»	
Тема 6. Общие характеристики ШОБ и криптосистемы DES. Структура системы DES. Система DES	Изучается компьютерная криптосистема DES и ее структура и компьютерная реализация
Тема 7. Математический подход к криптографическим алгоритмам и его следствие. Алгоритм Эвклида. Следствие теоремы Эвклида	Применение алгоритма Эвклида и его следствия для нахождения взаимно- обратных ключей в алгоритмах шифрования
Тема 8. Конгруэнции, их свойства. Кольцо остатков. Взаимообратные ключи в кольце остатков	Кольцо остатков, арифметические операции в нем, доказательство свойств
Содержательный модуль 4 «Аналитические шифры»	
Тема 9. Кольцо матриц. Обратная матрица как дешифрующий ключ	Рассматриваются криптографические аналитические шифры, вводится кольцо матриц, обратная матрица в этом множестве как дешифрующий ключ
Тема 10. Аффинные шифры 1-го порядка. Подходы к взлому шифров	Выбор ключей в кольце остатков, вскрытие шифров без знания ключей
Тема 11. Линейный шифр k-го по-	Использование в качестве ключей матриц к-го по-

рядка. Аффинный шифр k-го порядка.	рядка. Примеры вскрытия шифра без знания ключа
Тема 12. Примеры шифрования с матричными ключами.	Примеры на монограммные линейный и аффинный шифры

Тематический план

Названия содержательных модулей и тем	Содержательный модуль 1																					
	Количество часов																					
	Очная форма обучения											Заочная форма обучения										
	Нормативный срок обучения						Ускоренный срок обучения						Нормативный срок обучения						Ускоренный срок обучения				
	всего	в т.ч.					всего	в т.ч.					всего	в т.ч.					всего	в т.ч.			
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	самостоятельная работа	индивидуальная работа
Тема 1. Криптография, ее понятия и терминология	**2**	**2**					**2**	**2**															
Тема 2. Элементарные шифры. Частотный анализ.	**14**	**2**		**2**	**10**		**14**	**2**		**2**	**10**												
Итого по содержательному модулю 1	**16**	**4**		**2**	**10**		**16**	**4**		**2**	**10**												

Названия содержательных модулей и тем	Содержательный модуль 2																					
	Количество часов																					
	Очная форма обучения											Заочная форма обучения										
	Нормативный срок обучения						Ускоренный срок обучения						Нормативный срок обучения						Ускоренный срок обучения					
	всего	в т.ч.					всего	в т.ч.					всего	в т.ч.					всего	в т.ч.				
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	самостоятельная работа	индивидуальная работа
Тема 3. Шифры Плейфейера, Виженера	**9**	**2**		**2**	**5**		**9**	**2**		**2**	**5**												
Тема 4. Шифры перестановок. Матричный шифр обхода	**14**	**2**		**2**	**10**		**14**	**2**		**2**	**10**												
Тема 5. Подача материала в цифровой форме, шифр одноразового блока. Причины успешного криптоанализа	**16**	**4**		**2**	**10**		**16**	**4**		**2**	**10**												
Итого по содержательному модулю 2	**39**	**8**		**6**	**25**		**39**	**8**		**6**	**25**												

Названия содержательных модулей и тем	Содержательный модуль 3																				
	Количество часов																				
	Очная форма обучения											Заочная форма обучения									
	Нормативный срок обучения						Ускоренный срок обучения						Нормативный срок обучения						Ускоренный срок обучения				
	всего	в т.ч.					всего	в т.ч.					всего	в т.ч.					всего	в т.ч.			
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	самостоятельная работа	индивидуальная работа
Тема 6. Общие характеристики ШОБ и криптосистемы DES. Структура системы DES. Система DES	**13**	**4**		**4**	**5**		**13**	**4**		**4**	**5**												
Тема 7. Математический подход к криптографическим алгоритмам и его следствие. Алгоритм Эвклида. Следствие теоремы Эвклида	**24**	**6**		**8**	**5**		**24**	**6**		**8**	**5**												
Тема 8. Конгруэнции, их свойства. Кольцо остатков. Взаимообратные ключи в кольце остатков	**18**	**4**		**4**	**10**		**18**	**4**		**4**	**10**												
Итого по содержательному модулю 3	**55**	**14**		**16**	**25**		**55**	**14**		**16**	**25**												

Названия содержательных модулей и тем	Содержательный модуль 4																					
	Количество часов																					
	Очная форма обучения											Заочная форма обучения										
	Нормативный срок обучения						Ускоренный срок обучения						Нормативный срок обучения						Ускоренный срок обучения				
	всего	в т.ч.					всего	в т.ч.					всего	в т.ч.					всего	в т.ч.			
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	самостоятельная работа	индивидуальная работа
Тема 9. Кольцо матриц. Обратная матрица как дешифрующий ключ	**2**	**2**					**2**	**2**															
Тема 10. Афинные шифры 1-го порядка. Подходы к взлому шифров	**14**	**2**		**2**	**10**		**14**	**2**		**2**	**10**												
Тема 11. Линейный шифр k-го порядка. Афинный шифр k-го порядка.	**12**	**2**		**4**	**6**		**12**	**2**		**4**	**6**												
Тема 12. Примеры шифрования с матричными ключами.	**6**	**2**		**4**			**6**	**2**		**4**													
Итого по содержательному модулю 4	**34**	**8**		**10**	**16**		**34**	**8**		**10**	**16**												
Всего по дисциплине	**144**	**34**		**34**	**76**		**144**	**34**		**34**	**76**												

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

Темы лекционных занятий

№ п/п	*Название темы*	*Количество часов*
1	Криптография, ее понятия и терминология	2
2	Элементарные шифры. Частотный анализ	2
3	Шифры Плейфейера, Виженера	2
4	Шифры перестановок. Матричный шифр обхода.	2
5	Подача материала в цифровой форме. Шифр одноразового блокнота. Причины успешного криптоанализа.	4
6	Общие характеристики ШОБ и криптосистемы DES. Структура системы DES. Система DES.	4
7	Математический подход к криптографическим алгоритмам и его следствие. Алгоритм Евклида. Следствие теоремы Евклида.	6
8	Конгруэнции, их свойства. Кольцо остатков. Взаимообратные ключи в кольце остатков	4
9	Кольцо матриц. Обратная матрица как дешифрующий ключ	2
10	Аффинные шифры 1-го порядка. Подходы к взлому шифров	2
11	Линейный шифр k-го порядка. Афинный шифр k-го порядка.	2
12	Примеры шифрования с матричными ключами.	2
	ВСЕГО	**34**

Темы (практических, лабораторных, семинарских) занятий

№ п/п	*Название темы*	*Количество часов*
1	Элементарные шифры. Частотный анализ.	2
2	Шифры Плейфейера, Виженера.	2
3	Шифры перестановок. Матричный шифр.	2
4	Подача материала в цифровой форме. Шифр одноразового блокнота. Причины успешного криптоанализа.	2
5	Общие характеристики ШОБ и криптосистемы DES. Структура системы DES. Система DES.	4
6	Математический подход к криптографическим алгоритмам и его следствие. Алгоритм Евклида. Следствие теоремы Евклида.	8
7	Конгруэнции, их свойства. Кольцо остатков. Взаимообратные ключи в кольце остатков	4
9	Аффинные шифры 1-го порядка. Подходы к взлому шифров	2
10	Линейный шифр k-го порядка. Афинный шифр k-го порядка.	4
11	Примеры шифрования с матричными ключами.	4
	ВСЕГО	**34**

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	Элементарная криптография.	2
2	Элементарные шифры. Частотный анализ.	8
3	Шифры Плейфейера, Виженера.	5
4	Шифры перестановок. Матричный шифр.	10
5	Подача материала в цифровой форме. Шифр одноразового блокнота. Причины успешного криптоанализа.	10
6	Общие характеристики ШОБ и криптосистемы DES. Структура системы DES. Система DES.	5
7	Математический подход к криптографическим алгоритмам и его следствие. Алгоритм Евклида. Следствие теоремы Евклида.	5
8	Конгруэнции, их свойства. Кольцо остатков. Взаимообратные ключи в кольце остатков	5
9	Аффинные шифры 1-го порядка. Подходы к взлому шифров	10
10	Линейный шифр k-го порядка. Афинный шифр k-го порядка.	10
11	Примеры шифрования с матричными ключами.	6
	ВСЕГО	**76**

7. ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ – не предусмотрено программой

8. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1. Наивная криптография. Шифр Цезаря и частокола.
2. Классические шифры Плейфейера, Виженера.
3. Частотный анализ, его применение ко взлому шифра.
4. Общий шифр перестановок.
5. Матричный шифр обхода.
6. Алгоритм Эвклида и его следствие.
7. Конгруэнции и их свойства. Кольцо остатков.
8. Кольцо матриц. Нахождение обратной матрицы в качестве дешифрующего ключа.
8. Аффинный шифр 1-го порядка. Пример.
9. Аффинный шифр 2-го порядка. Пример.

9. ОБРАЗЕЦ МОДУЛЬНОГО КОНТРОЛЯ

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»
Факультет математики и информационных технологий

Направление подготовки: ***01.03.02 Прикладная математика и информатика***
Магистерская программа: ***прикладная математика и информатика***
Программа подготовки: ***бакалавриат***
Семестр *6*
Учебная дисциплина ***Математические основы защиты информации.***

МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА
ВАРИАНТ №1

1. Полиалфавитные шифры замены. Шифр Виженера, подход к криптоанализу в алгоритме.
2. Зашифровать слово «математика» аффинным шифром 1-го порядка с ключами $a=5$, $s=3$, $n=33$.

Утверждено на заседании кафедры теории упругости и вычислительной математики имени академика А.С. Космодамианского, протокол № ___ от «___» _____ 20___ г.

Заведующий кафедрой _____ В.И. Сторожев
Преподаватель _____ Л.Н. Шкодина

Критерии оценивания модульного контроля

Номер задания	***Количество баллов***
Теория	40
Задача	60
Всего	***100***

10. ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Теоретические вопросы к экзамену

1. Наивная криптография. Шифр Цезаря и частокола.
2. Классические шифры Плейфейера, Виженера.
3. Частотный анализ, его применение ко взлому шифра.
4. Общий шифр перестановок.
5. Матричный шифр обхода.
6. Алгоритм Эвклида и его следствие.
7. Конгруэнции и их свойства. Кольцо остатков.
8. Кольцо матриц. Нахождение обратной матрицы в качестве дешифрующего ключа.
8. Аффинный шифр 1-го порядка.
9. Аффинный шифр 2-го порядка.

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»
Факультет математики и информационных технологий

Направление подготовки: ***01.03.02 Прикладная математика и информатика***
Программа подготовки: ***бакалавриат***
Семестр ***6***
Учебная дисциплина ***Математические основы защиты информации***

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Шифр матричного обхода.
2. Для числа 5 найти, с помощью алгоритма Евклида, мультипликативное обратное по модулю n=34.

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

Заведующий кафедрой _____ В.И. Сторожев
Преподаватель _____ Л.Н. Шкодина

Критерии оценивания экзамена

Номер задания	***Количество баллов***
Теория	40
Задача	60
Всего	**100 баллов**

11. КРИТЕРИИ ОЦЕНИВАНИЯ

В течение семестра обучающийся может заработать балы за следующие виды деятельности: индивидуальное задание (домашние работы), самостоятельные и контрольные работы по практике, модульные контрольные работы по теории и практике (в общей сложности максимум 100 баллов), активность на занятиях, индивидуальные творческие задания (бонусные баллы). Экзаменационная работа оценивается после защиты максимум в 100 баллов. Оценка за семестр вычисляется как максимальная из полученных за семестр и на экзамене и выставляется согласно шкале, принятой в ДонНУ. Более подробные критерии разрабатываются исходя из контингента и доводятся до ведома студентов в первый месяц обучения.

Оценка знаний студентов проводится по 100-балльной шкале согласно следующим критериям:

Распределение баллов, которые могут получить студенты в процессе изучения дисциплины

СРС			**Всего**
Индивидуальная работа	**Контрольная работа №1**	**Контрольная работа №2**	
max 60 баллов	max 20 баллов	max 20 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

12. ОБРАЗЕЦ ТЕСТОВОГО ЗАДАНИЯ – не предусмотрено программой

13. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Лекционные занятия проводятся в аудитории, оснащенной компьютерной техникой и доской. Лабораторные занятия проводятся в компьютерном классе, оборудованном компьютерами с лицензионным программным обеспечением, доступом к сети Интернет, столами, доской.

Для проведения лекционных занятий требуется аудитория на группу, оборудованная меловой или интерактивной доской.

14. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонНУ	Наличие электронной версии в ЭБС
	Основная литература		
1.	Вербицький О.В. Вступ до криптології. Видавн. наук.-техн. літератури. Львів. – 1998. – 247 с.	1	-
2.	Скобелев В.Г. Введение в криптологию: учеб. пособие / В.Г. Скобелев; Донецкий нац. ун-т. - Донецк: Юго-Восток, 2008. - 175 с.	15	-
3.	Бородин А.И. Теория чисел: учеб. пособие для ун-тов по спец. "Математика" / А.И.Бородин. - Киев: Выща шк., 1992. - 288 с.	25	-
4.	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	-
5.	Рублинецкий В.И. Введение в компьютерную криптологию / Харьк. гуманит. ин-т "Нар. укр. акад.". - Харьков: ОКО, 1997. - 128 с.	1	-
6.	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.	1	-
7.	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	-
8.	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	-

9.	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	-
10.	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	-
Дополнительная литература			
1.	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	-

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

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

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