

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
«МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ»
практико-ориентированная дисциплина

Направление подготовки:	01.03.02 Прикладная математика и информатика
Профиль подготовки:	Прикладная математика и информатика
Образовательная программа:	<u>Бакалавриат</u>
Квалификация:	Академический бакалавр
Форма обучения:	<u>очная</u>

Донецк 2021

УТВЕРЖДАЮ:


Декан факультета математики
и информационных технологий
И. А. Моисеенко



Рабочая программа учебной дисциплины **«Математические основы защиты информации»** составлена на основании Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 01.03.02 Прикладная математика и информатика, утвержденного приказом Министерства образования и науки Российской Федерации от «10» января 2018г. № 9; Государственного образовательного стандарта высшего образования (ГОС ВО) Донецкой Народной Республики (ДНР) (проекта) по направлению подготовки 01.03.02 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 01.03.02 Прикладная математика и информатика, профиля: «Прикладная математика и информатика», разработанных в ГОУ ВПО «Донецкий национальный университет».

Разработчик:

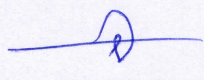
*старший преподаватель кафедры
теории упругости и вычислительной математики
имени академика А.С. Космодамианского*

 М. Н. Пачева

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

Протокол № 15 от «12» апреля 2021 г.

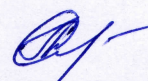
Заведующий кафедрой

 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 «Математические основы защиты информации» является практико-ориентированной дисциплиной и относится к вариативной части образовательной программы. Для изучения данной учебной дисциплины необходимы знания и умения, формируемые *предшествующими дисциплинами* – Б1.Б.8 Математический анализ, Б1.Б.9 Алгебра и геометрия, Б1.Б.10 Дискретная математика, Б1.Б.11 Языки и методы программирования. Знания и умения, полученные в ходе изучения дисциплины «Математические основы защиты информации» являются основой для изучения *последующих* дисциплин: Б1.В.ОД.1 Современные методы криптографии; используются при написании выпускной квалификационной работы.

2. СТРУКТУРА ДИСЦИПЛИНЫ

Характеристика учебной дисциплины	Форма обучения	
	Очная	Заочная
Направление подготовки	01.03.02 Прикладная математика и информатика	
Профиль	Прикладная математика и информатика	
Образовательная программа	Бакалавриат	
Квалификация	Академический бакалавр	
Количество содержательных модулей и тем	1 (6)	
Дисциплина базовой / вариативной части образовательной программы	Вариативной части	
Формы контроля	1 модульный контроль, зачет в 6-м семестре	
Год подготовки	3	
Семестр	6	
Количество зачетных единиц	3	
Количество часов всего	108	
в т.ч.:		
- лекционных	17	
- практических или семинарских	×	
- лабораторных	34	
- самостоятельной работы	57	
в т.ч. индивидуальное задание	×	
Недельное количество часов	6,35	
в т. ч.: - аудиторных	3	
- самостоятельной работы студента	3,35	

3. ОПИСАНИЕ ДИСЦИПЛИНЫ

Цель изучения дисциплины «Математические основы защиты информации» – изучение криптографических методов защиты информации, сравнительный анализ этих методов, их надежности и эффективности с помощью традиционных способов криптографии, классической математики, методов формализованного описания систем, процессов.

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 ФГОС ВО РФ, ГОС ВО ДНР (проект) по направлению подготовки 01.03.02 Прикладная математика и информатика и основной профессиональной образовательной программы высшего образования направления подготовки 01.03.02 Прикладная математика и информатика, профиля: «Прикладная математика и информатика»:

Универсальные компетенции (УК):	
Наименование категории (группы) универсальных компетенций: «Системное и критическое мышление»	
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
Наименование категории (группы) универсальных компетенций: «Разработка и реализация проектов»	
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
Общепрофессиональные компетенции (ОПК):	
Наименование категории (группы) общепрофессиональных компетенций: «Теоретические и практические основы профессиональной деятельности»	
ОПК-1	Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности
ОПК-2	Способен использовать и адаптировать существующие математические методы и системы программирования для разработки и реализации алгоритмов решения прикладных задач
Профессиональные компетенции (ПК):¹	
Тип задач профессиональной деятельности: научно-исследовательский	
ПК-1	Способен выполнять научно-исследовательские работы в соответствии с техническим заданием в составе научного коллектива по отдельным разделам темы
ПК-2	Способен проводить обработку и анализ научной информации и результатов исследований
ПК-3	Способен публично представлять собственные и известные научные результаты
Тип задач профессиональной деятельности: производственно-технологический	
ПК-4	Способен к выбору варианта архитектуры программного средства, разработке и верификации программного обеспечения для решения технических и научно-исследовательских задач
Тип задач профессиональной деятельности: Организационно-управленческий	

¹ Если ПК взята из профессионального стандарта – можно указать название профстандарта, кем и когда утвержден, регистрационный номер профстандарта

ПК-7	Способен составлять и контролировать план выполняемой работы, планировать необходимые для ее выполнения ресурсы, оценивать результаты собственной работы
------	--

Индикаторы достижения компетенций и результаты обучения². 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 поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.И-1. Применяет методы системного подхода для решения поставленных задач	Знает методику математического исследования прикладных задач
			Умеет оценивать полученные результаты и обосновывать их.
Разработка и реализация проектов	УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-1.И-1. Проводит анализ поставленной цели и определяет совокупность задач, обеспечивающих ее достижение	Знает методику математического исследования прикладных задач
			Умеет при решении задач выбирать и использовать стандартные алгоритмы в зависимости от поставленных задач

Общепрофессиональные компетенции	Индикаторы	Результаты обучения
ОПК-1. Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности	ОПК-1.И-1. Решает стандартные математические задачи и применяет их решения в профессиональной деятельности	Знает специфику современного математического аппарата и сферы его использования
		Знает основные понятия и методы защиты информации
		Умеет применять фундаментальные математические знания, алгоритмы и методы при решении научно-исследовательских и прикладных задач
		Умеет при решении задач выбирать и использовать стандартные алгоритмы в зависимости от поставленных задач

² Количество индикаторов по каждой компетенции может варьироваться (от одного и более).

ОПК-2. Способен использовать и адаптировать существующие математические методы и системы программирования для разработки и реализации алгоритмов решения прикладных задач	ОПК-2.И-1. Использует и адаптирует существующие математические методы для разработки алгоритмов решения прикладных задач	Знает современные математические методы, использующиеся при решении прикладных задач
		Умеет использовать и адаптировать существующие математические методы для разработки алгоритмов решения прикладных задач
	ОПК-2.И-2. Использует современные системы программирования для реализации алгоритмов решения прикладных задач	Знает современные системы программирования, использующиеся при решении прикладных задач
		Умеет использовать современные системы программирования

Профессиональные компетенции	Индикаторы	Результаты обучения
ПК-1. Способен выполнять научно-исследовательские работы в соответствии с техническим заданием в составе научного коллектива по отдельным разделам темы	ПК-1.И-1. Осуществляет критический анализ отдельных результатов использования стандартных методов и алгоритмов компьютерно-математического моделирования	Знает методы анализа результатов использования стандартных методов
		Умеет анализировать техническое задание
		Умеет оценивать точность полученных численными методами результатов и обосновывать их.
ПК-2. Способен проводить обработку и анализ научной информации и результатов исследований	ПК-2.И-1. Оформляет результаты научно-исследовательских работ и вычислительных экспериментов в соответствии с актуальными стандартами	Знает порядок формирования и оформления отчета по результатам проведенной работы
		Умеет работать с основными информационными источниками по теме исследования
		Умеет правильно оформлять результаты вычислительных экспериментов
ПК-3. Способен публично представлять собственные и известные научные результаты	ПК-3.И-1. Публично представляет результаты научно-исследовательской работы, выполненной индивидуально и в составе научного коллектива	Знает требования, предъявляемые к оформлению отчета по результатам исследования
		Умеет представлять результаты проделанной работы в виде доклада
ПК-4. Способен к выбору варианта архитектуры программного средства, разработке и верификации	ПК-4.И-1. Разрабатывает процедуры и осуществляет интеграцию программных мо	Знает основные принципы процесса разработки программного обеспечения
		Знает методы и способы идентификации сбоев и ошибок при интеграции приложений

программного обеспечения для решения технических и научно-исследовательских задач	дулей и компонент	Умеет осуществлять разработку кода программного модуля на современных языках программирования
		Умеет выполнять отладку и тестирование программы на уровне модуля
ПК-7. Способен составлять и контролировать план выполняемой работы, планировать необходимые для ее выполнения ресурсы, оценивать результаты собственной работы	ПК-7.И-1. Планирует этапы работы по разработке программного обеспечения, информационно-коммуникационных технологий, их техническое описание	Знает методы и способы выполнения профессиональных задач
		Умеет планировать деятельность по решению задачи в рамках заданных технологий
		Умеет анализировать потребности в ресурсах и планировать ресурсы в соответствии с заданным способом решения задачи

4. ФОРМЫ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Дисциплина «Математические основы защиты информации» предусматривает следующие формы организации учебного процесса: лекции, лабораторные занятия, самостоятельную работу студентов.

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

В учебном процессе применяются активные и интерактивные формы проведения занятий, 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, самостоятельная работа; контрольные работы.

Самостоятельная работа студентов предусматривает выполнение домашних заданий, подготовку к лабораторным занятиям, изучение учебно-методической литературы, составление конспектов, подготовку презентаций и докладов.

Текущий контроль осуществляется путем написания самостоятельных и контрольных работ по решению практических заданий, модульных контрольных работ по проверке знаний теоретических положений (определений, теорем и их доказательств).

Тематический план «Математические основы защиты информации»

Темы	Вопросы темы
Содержательный модуль 1.	
1. Введение в теорию защиты информации	1.1. Основные понятия информационной безопасности. 1.2. Сервисы и методы информационной безопасности. 1.3. Понятие угрозы. 1.4. Классификация криптографических методов защиты информации. 1.5. Краткий исторический обзор развития методов защиты информации.

2. Симметричные криптосистемы и их свойства*	2.1. Шифры замены. 2.2. Шифры перестановки. 2.3. Поточные криптосистемы. 2.4. Блочные криптосистемы.
3. Математические модели информационной безопасности*	3.1. Формальные модели шифров. 3.2. Математические модели открытого текста. 3.3. Критерии распознавания открытого текста.
4. Арифметика остатков*	4.1. Введение в теорию чисел. 4.2. Вычеты и их свойства. 4.3. Алгоритм Эвклида и расширенный алгоритм Эвклида. 4.4. Взаимно обратные числа в классе вычетов.
5. Методы криптоанализа симметричных криптосистем*	5.1. Задачи и принципы криптоанализа. 5.2. Метод полного перебора. 5.3. Методы криптоанализа с использованием теории статистических решений
6. Теория стойкости криптосистем*	6.1. Совершенно стойкие криптосистемы. 6.2. Идеально стойкие криптосистемы. 6.3. Практическая стойкость криптосистем. 6.4. Имитостойкость и помехоустойчивость криптосистем.

* – практико-ориентированные темы.

Структура дисциплины «Математические основы защиты информации» 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.										
1. Введение в теорию защиты информации	10	2		4	4					
2. Симметричные криптосистемы и их свойства	26	4		12	10					
3. Математические модели информационной безопасности	14	2		2	10					
4. Арифметика остатков	20	4		6	10					
5. Методы криптоанализа симметричных криптосистем	18	2		6	10					
6. Теория стойкости криптосистем	20	3		4	13					
Итого по содержательному модулю 1	108	17		34	57					
Всего часов	108	17		34	57					

5. ТЕМАТИКА ЛЕКЦИОННЫХ, ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Темы лекционных занятий

№ п/п	Название темы	Количество часов	
		Очная форма	Заочная форма
1	Введение в теорию защиты информации	2	
2	Симметричные криптосистемы и их свойства	4	
3	Математические модели информационной безопасности	2	
4	Арифметика остатков	4	
5	Методы криптоанализа симметричных криптосистем	2	
6	Теория стойкости криптосистем	3	
Всего		18	

Тексты лекций приведены в: дистанционном курсе на платформе Moodle <http://dl-test.donnu-support.ru/course/view.php?id=516>

Темы лабораторных работ

№ п/п	Название темы	Количество часов	
		Очная форма	Заочная форма
1	Введение в теорию защиты информации	4	
2	Симметричные криптосистемы и их свойства	12	
3	Математические модели информационной безопасности	2	
4	Арифметика остатков	6	
5	Методы криптоанализа симметричных криптосистем	6	
6	Теория стойкости криптосистем	4	
Всего			

Содержание лабораторных работ и методические рекомендации к их выполнению приведены в: дистанционном курсе на платформе Moodle <http://dl-test.donnu-support.ru/course/view.php?id=516>

6. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

№ п/п	Название темы	Количество часов	
		Очная форма	Заочная форма
1	Введение в теорию защиты информации	4	
2	Симметричные криптосистемы и их свойства	10	
3	Математические модели информационной безопасности	10	
4	Арифметика остатков	10	
5	Методы криптоанализа симметричных криптосистем	10	
6	Теория стойкости криптосистем	13	
Всего			

Содержание самостоятельной (в т.ч. индивидуальной) работы по темам и методические рекомендации по ее выполнению приведены в: дистанционном курсе на платформе Moodle <http://dl-test.donnu-support.ru/course/view.php?id=516>

7. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Содержательный модуль 1.

1. Методы информационной безопасности.
2. Классификация криптографических методов защиты информации.
3. Наивная криптография. Шифр Цезаря и частокола.
4. Классические шифры Плейфейера, Виженера.
5. Общий шифр перестановок.
6. Матричный шифр обхода.
7. Математическая модель шифра.
8. Математическая модель открытого текста.
9. Алгоритм Эвклида и его следствие.
10. Конгруэнции и их свойства. Кольцо остатков.
11. Кольцо матриц. Нахождение обратной матрицы в качестве дешифрующего ключа.
12. Аффинный шифр 1-го порядка. Пример.
13. Аффинный шифр 2-го порядка. Пример.
14. Задачи и принципы криптоанализа.
15. Метод полного перебора.
16. Частотный анализ, его применение ко взлому шифра.
17. Криптографическая стойкость криптосистем
18. Методы оценки стойкости криптосистем

8. ОБРАЗЕЦ ЗАДАНИЯ МОДУЛЬНОГО КОНТРОЛЯ

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Образовательная программа: бакалавриат

Направление подготовки: 01.03.02 Прикладная математика и информатика

Профиль: Прикладная математика и информатика

Очная форма обучения. Семестр: 6

Учебная дисциплина: Математические основы защиты информации

Модульная контрольная работа

Вариант № n

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

Преподаватель

В.И.Сторожев

М.Н.Пачева

9. КРИТЕРИИ ОЦЕНИВАНИЯ ЗАДАНИЯ МОДУЛЬНОГО КОНТРОЛЯ

Номер задания	Количество баллов
1	20
2	15
Всего	35

10. ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Экзамен не предусмотрен учебным планом

11. КРИТЕРИИ ОЦЕНИВАНИЯ ЭКЗАМЕНАЦИОННОГО ЗАДАНИЯ

Экзамен не предусмотрен учебным планом

12. КРИТЕРИИ ОЦЕНИВАНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Самостоятельная работа оценивается в 60 баллов. В разрезе отдельных тем оценивание осуществляется следующим образом.

Оценивание СРС и ИРС по дисциплине «Математические основы защиты информации»

Названия содержательных модулей и тем	СРС	ИРС
Содержательный модуль 1.		
1. Введение в теорию защиты информации	5	
2. Симметричные криптосистемы и их свойства	15	
3. Математические модели информационной безопасности	5	
4. Арифметика остатков	10	
5. Методы криптоанализа симметричных криптосистем	15	
6. Теория стойкости криптосистем	10	
Итого по 1-му содержательному модулю	60	
Всего баллов	60	

13. ИНДИВИДУАЛЬНОЕ ТВОРЧЕСКОЕ ЗАДАНИЕ

Не предусмотрено

14. КРИТЕРИИ ОЦЕНИВАНИЯ ИНДИВИДУАЛЬНОГО ТВОРЧЕСКОГО ЗАДАНИЯ

Не предусмотрено

15. 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 лабораторных занятий (вопросы лектору по теме лекционного материала, участие в обсуждении пройденного материала, решение задач и ситуаций у доски и т.п.).

Содержательные модули	Вид работы	Баллы
Содержательный модуль 1	Организационно-учебная работа студента в аудитории	5
	Самостоятельная работа	60
	Модульная контрольная работа	35
	Итого	100
Общий итог		100

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

16. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в главном (83001, г. Донецк, пр. Гурова, 6) учебном корпусе университета. Для проведения лекционных и лабораторных 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-методических кабинетах главного (ауд.604) учебного корпуса, материально-техническую базу учебной лаборатории «Сетевых компьютерных технологий» (ауд. 606) и учебной лаборатории «Интегрированных сред программирования» (ауд. 610) кафедры теории упругости и вычислительной математики имени академика А.С. Космодамианского. В процессе обучения студенты имеют возможность использовать учебные материалы по дисциплине «Математические основы защиты информации», размещенные на платформе Moodle Центра дистанционного образования ГОУ ВПО «ДонНУ».

17. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонНУ	Наличие электронной версии в ЭБС
Основная литература			
1.	Бородин А.И. Теория чисел: учеб. пособие для ун-тов по спец. "Математика" / А.И.Бородин. - Киев: Выща шк., 1992. - 288 с.	25	-
2.	Вербицкий О.В. Вступ до криптології. Видавн. наук.-техн. літератури. Львів. – 1998. – 247 с.	1	-
3.	Калоеров С.А. Программирование на C++: учеб. пособие / С.А.Калоеров; Донецкий нац. ун-т. – Изд. 3-е. – Донецк: Уго-Восток, 2009. – 298 с.	101	-

4.	Методические указания к лабораторным работам по криптографии / [сост.: Л. Н. Шкодина, М. Н. Пачева, А. И. Занько] ; ГОУ ВПО "Донецкий национальный университет". - Донецк : ГОУ ВПО "ДонНУ", 2018. - 42 с.	6	+
5.	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	-
6.	Практический курс по современным методам криптографии [Электронный ресурс] : учебно-методическое пособие / ГОУ ВПО "Донецкий национальный университет" ; сост.: Л. Н. Шкодина, А. И. Занько. - 2-е изд. - Донецк : ДонНУ, 2019.		+
7.	Рублинецкий В.И. Введение в компьютерную криптологию / Харьк. гуманит. ин-т "Нар. укр. акад.". - Харьков: ОКО, 1997. - 128 с.	1	-
8.	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	-
9.	Скобелев В.Г. Введение в криптологию: учеб. пособие / В.Г. Скобелев; Донецкий нац. ун-т. - Донецк: Юго-Восток, 2008. - 175 с.	15	-
10.	Современные методы криптографии [Электронный ресурс] : учебное пособие / ГОУ ВПО "Донецкий национальный университет" ; сост.: Л. Н. Шкодина, А. И. Занько. - Донецк : ДонНУ, 2019.		+
11.	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	-
12.	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	-
13.	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	-
14.	Шкодина, Л. Н. Современные методы криптографии [Электронный ресурс] : учебное пособие / Л. Н. Шкодина. А. И. Занько. - Донецк : ДонНУ, 2020.		+
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	-

18. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Криптографические методы защиты информации <https://www.classcentral.com/course/edx-kriptograficheskie-metody-zashchity-informacii-17269>

19. 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 для свободного программного обеспечения: Антивирус Касперского, Libre Office, Adobe Acrobat Reader, xPDF, Paint.NET.