

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра прикладной математики и ТСУ



УТВЕРЖДАЮ:

проректор по научно-методической
и учебной работе

Е.И. Скафа

22 апреля 2020 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
«ПРИКЛАДНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ 7»**

Направление подготовки:	02.03.02 Фундаментальная информатика и информационные технологии
Образовательная программа:	Бакалавриат
Квалификация:	Академический бакалавр
Форма обучения:	<u>очная</u> , 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 «Прикладные информационные технологии 7» составлена на основании Государственного образовательного стандарта высшего профессионального образования (ГОС ВПО) Донецкой Народной Республики (ДНР) по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии, утвержденного приказом Министерства образования и науки ДНР от 04 апреля 2016 г. № 283;

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 02.03.02 Фундаментальная информатика и информационные технологии, разработанных в ГОУ ВПО «Донецкий национальный университет».

Разработчик:

Доцент кафедры прикладной математики и ТСУ



Л.А. Рыбалко

Программа учебной дисциплины утверждена на заседании кафедры прикладной математики и теории систем управления

Протокол № 12 от «09» апреля 2020 г.

Заведующий кафедрой



Д.В. Шевцов

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 ПБ.ВС.7 «Прикладные информационные технологии 7» является дисциплиной по выбору студента профессионального блока дисциплин подготовки студентов по направлению подготовки 02.03.02 «Фундаментальная информатика и информационные технологии».

Изучение данной дисциплины основывается на базе дисциплин: «Дискретная математика», «Алгоритмы и анализ сложности», «Основы программирования», «Введение в объектно-ориентированное программирование».

Является основой для изучения дисциплины «Математические основы защиты информации и информационной безопасности» магистратуры и для научно-исследовательской работы над выпускным квалификационным дипломом бакалавра.

2. СТРУКТУРА ДИСЦИПЛИНЫ

<i>Характеристика учебной дисциплины</i>				
Направление подготовки	02.03.02 «Фундаментальная информатика и информационные технологии»			
Профиль	Общий			
Образовательная программа	бакалавриат			
Квалификация	Академический бакалавр			
Количество содержательных модулей	1			
Дисциплина базовой / вариативной части образовательной программы	Вариативная часть профессионального блока			
Формы контроля (МК, экзамен, зачет)	1 модульный контроль, 1 экзамен в 8/6 семестре			
Показатели	очная форма обучения		заочная форма обучения	
	нормат. срок	ускор. срок	нормат. срок	ускор. срок
Количество зачетных единиц (кредитов)	2	2		
Год подготовки	4	3		
Семестр	8	6		
Количество часов	72	72		
- лекционных	20	20		
- практических, семинарских				
- лабораторных	20	20		
- самостоятельной работы	32	32		
в т.ч. индивидуальное задание	-	-		
Недельное количество часов,	7,2	7,2		
в т.ч. аудиторных	4	4		

3. ОПИСАНИЕ ДИСЦИПЛИНЫ

Цели и задачи

Цель - формирование представлений о роли и месте математики и вычислительной техники в современной цивилизации и в мировой культуре, умений логически мыслить, составлять несложные информационно-математические модели, оперировать с абстрактными объектами и быть корректным в употреблении математических понятий и символов для выражения количественных и качественных отношений, воспитание высокой математической культуры.

Задачи:

- изучить соответствующую терминологию в области криптографии, основные классы симметричных криптографических систем;
- сформировать навыки компьютерной реализации простых алгоритмов защиты информации;
- развивать умение использовать математические методы и программирование в исследовательской и практической деятельности.

Требования к результатам освоения дисциплины: Процесс изучения дисциплины «Прикладные информационные технологии 7» направлен на формирование элементов следующих компетенций в соответствии с ГОС ВПО ДНР по направлению подготовки 02.03.02 «Фундаментальная информатика и информационные технологии» и основной образовательной программы высшего профессионального образования направления подготовки 02.03.02 «Фундаментальная информатика и информационные технологии» (профиль: Общий):

а) общекультурных (ОК):

способность работать в команде, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия (ОК - 6);

способность к самоорганизации самообразованию (ОК-7);

б) общепрофессиональных (ОПК):

способность использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с фундаментальной информатикой и информационными технологиями (ОПК-1);

способность применять в профессиональной деятельности современные языки программирования и языки баз данных, методологии системной инженерии, системы автоматизации проектирования, электронные библиотеки и коллекции, сетевые технологии, библиотеки и пакеты программ, современные профессиональные стандарты информационных технологий (ОПК-2);

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):**научно-исследовательская деятельность:**

способность собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям (ПК-1);

способность понимать, совершенствовать и применять современный математический аппарат, фундаментальные концепции и системные методологии, международные и профессиональные стандарты в области информационных технологий (ПК-2);

способность использовать современные инструментальные и вычислительные средства (ПК-3);

способность решать задачи профессиональной деятельности в составе научно-исследовательского и производственного коллектива (ПК-4);

способность критически переосмысливать накопленный опыт, изменять при необходимости вид и характер своей профессиональной деятельности (ПК-5);

проектная и производственно-технологическая деятельность:

способность эффективно применять базовые математические знания и информационные технологии при решении проектно-технических и прикладных задач,

связанных с развитием и использованием информационных технологий (ПК-6);

способность разрабатывать и реализовывать процессы жизненного цикла информационных систем, программного обеспечения, сервисов систем информационных технологий, а также методы и механизмы оценки и анализа функционирования средств и систем информационных технологий (ПК-7);

способность применять на практике международные и профессиональные стандарты информационных технологий, современные парадигмы и методологии, инструментальные и вычислительные средства (ПК-8);

В результате изучения учебной дисциплины студент должен

Знать:

- ✓ основные табличные шифры перестановок и замен;
- ✓ основные классы симметричных криптографических систем;
- ✓ общие положения асимметричных криптосистем.

Уметь:

- ✓ применять программные методы защиты информации.

Владеть:

- ✓ навыками компьютерной реализации простых алгоритмов защиты информации.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И ФОРМЫ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА

Порядковый номер и тема	Краткое содержание темы
Содержательный модуль 1	
Тема 1. Информационная безопасность компьютерных систем	Основные понятия и определения. Основные угрозы безопасности АСОИ. Задачи информационной безопасности. Криптографические системы и требования к ним.
Тема 2. Классические криптосистемы	Основные понятия и определения. Табличные шифры перестановок. Табличные шифры замен: системы шифрования Цезаря, Гронсфельда, шифрующие таблицы Трисемуса, биграммный шифр Плейфейра, криптосистема Хилла, система шифрования Вижинера, шифр «двойной квадрат» Уитсона.
Тема 3. Современные симметричные криптосистемы	Основные классы симметричных криптографических систем. Модель сети Фейстела. Система блочного шифрования DES. Основные режимы работы алгоритма DES. Система блочного шифрования ГОСТ 28147-89. Режимы работы алгоритма ГОСТ 28147-89. Системы блочного шифрования RC6, SAFER+. Поточковые шифры RC4, WAKE.
Тема 4. Асимметричные криптосистемы	Общие положения асимметричных криптосистем. Однонаправленные функции. Системы шифрования Эль-Гамала и RSA.

Тематический план

[illegible]

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

Темы лекционных занятий

№ n/n	Название темы	Количество часов
1	<i>Тема 1. Информационная безопасность компьютерных систем</i>	2
2	<i>Тема 2. Классические криптосистемы</i>	6
3	<i>Тема 3. Современные симметричные криптосистемы</i>	8
4	<i>Тема 4. Асимметричные криптосистемы</i>	4
	ВСЕГО	20

Темы лабораторных занятий

№ n/n	Название темы	Количество часов
1	<i>Тема 1. Информационная безопасность компьютерных систем</i>	2
2	<i>Тема 2. Классические криптосистемы</i>	6
3	<i>Тема 3. Современные симметричные криптосистемы</i>	8
4	<i>Тема 4. Асимметричные криптосистемы</i>	4
	ВСЕГО	20

6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Организация самостоятельной работы студентов (соответственно данным в таблице тематического плана)

№ n/n	Название темы	Количество часов
1	<i>Тема 1. Информационная безопасность компьютерных систем</i>	2
2	<i>Тема 2. Классические криптосистемы</i>	10
3	<i>Тема 3. Современные симметричные криптосистемы</i>	12
4	<i>Тема 4. Асимметричные криптосистемы</i>	8
	ВСЕГО	32

7. ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ

Цель:

Формирование и развитие профессиональных умений в области криптографии: изучить соответствующую терминологию, основные классы симметричных и асимметричных криптографических систем; сформировать навыки компьютерной реализации простых алгоритмов защиты информации, развивать умение использовать математические методы и программирование в исследовательской и практической деятельности; представлять и записывать решение задачи с использованием объектно-ориентированного подхода; реализовывать разработанный алгоритм в визуальной среде программирования, отлаживать, тестировать программу; оформлять результаты работы в

форме отчета; получить практические навыки самостоятельной работы с учебной, методической и научной литературой.

Пример индивидуального задания 1

1) Информационная безопасность компьютерных систем

- a) Основные понятия и определения информационной безопасности. (5 баллов)
- b) Основные угрозы безопасности АСОИ. (5 баллов)
- c) Табличные шифры перестановок. (5 баллов)
- d) Программная реализация шифрующих таблиц. (20 баллов)

Пример индивидуального задания 2

2) Современные симметричные криптосистемы

- a) Основные классы симметричных криптографических систем. (5 баллов)
- b) Система блочного шифрования DES. (5 баллов)
- c) Основные режимы работы алгоритма DES. (5 баллов)
- d) Программная реализация алгоритма DES. (20 баллов)

8. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1. Табличные шифры перестановок.
2. Табличные шифры замен: системы шифрования Цезаря.
3. Шифрующие таблицы Трисемуса.
4. Биграммный шифр Плейфейра.
5. Система шифрования Вижинера.
6. Шифр «двойной квадрат» Уитсона.
7. Система блочного шифрования DES.
8. Система блочного шифрования ГОСТ 28147-89.
9. Система блочного шифрования RC6.
10. Система блочного шифрования SAFER+.
11. Основные режимы работы блочных шифров.
12. Поточковый шифр RC4.
13. Поточковый шифр WAKE.
14. Общие положения асимметричных криптосистем.
15. Однонаправленные функции.
16. Система шифрования Эль-Гамала.
17. Система шифрования RSA.

9. ОБРАЗЕЦ МОДУЛЬНОГО КОНТРОЛЯ

(образец варианта и критерии оценивания)

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»
Факультет МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Направление подготовки: **02.03.02 Фундаментальная информатика и информационные технологии**

Профиль: **общий**
Программа подготовки: **бакалавриат**

Семестр **8**

Учебная дисциплина **Прикладные информационные технологии 7**

МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА ВАРИАНТ №1

1. Набор из 30 тестовых вопросов

.....

Утверждено на заседании кафедры прикладной математики и ТСУ,
протокол № ____ от «__» _____ 20__ г.

Заведующий кафедрой
Преподаватель

Шевцов Д.В.
Рыбалко Л.А.

Критерии оценивания модульного контроля

Количество набранных баллов равно количеству правильных ответов.

10. ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

(теоретические вопросы к экзамену, образец билета и критерии оценивания)

Теоретические вопросы к экзамену

1. Основные понятия и определения информационной безопасности.
2. Основные угрозы безопасности АСОИ.
3. Задачи информационной безопасности.
4. Криптографические системы и требования к ним.
5. Основные понятия и определения криптологии.
6. Табличные шифры перестановок.
7. Табличные шифры замен: системы шифрования Цезаря.
8. Система шифрования Цезаря с ключевым словом.
9. Афинная система шифрования Цезаря.
10. Шифрующие таблицы Трисемуса.
11. Биграммный шифр Плейфейра.
12. Криптосистема Хилла
13. Система шифрования Вижинера.
14. Шифр «двойной квадрат» Уитсона.
15. Основные классы симметричных криптографических систем.
16. Модель сети Фейстела.
17. Система блочного шифрования DES.
18. Основные режимы работы алгоритма DES .
19. Система блочного шифрования ГОСТ 28147-89.
20. Режимы работы алгоритма ГОСТ 28147-89.
21. Система блочного шифрования RC6.
22. Система блочного шифрования SAFER+.
23. Поточковый шифр RC4.
24. Поточковый шифр WAKE.
25. Общие положения асимметричных криптосистем.
26. Однонаправленные функции.
27. Система шифрования Эль-Гамала.
28. Система шифрования RSA.

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»
Факультет МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Направление подготовки: **02.03.02 Фундаментальная информатика и информационные технологии**

Профиль: **общий**

Программа подготовки: **бакалавриат**

Семестр **8**

Учебная дисциплина **Прикладные информационные технологии 7**

БИЛЕТ № 1

1. Криптографические системы и требования к ним.
2. Асимметричная система шифрования RSA.

Утверждено на заседании кафедры прикладной математики и ТСУ

Протокол № 1 от 31.08.19

Заведующий кафедрой

Экзаменатор

Шевцов Д.В.

Рыбалко Л.А.

Критерии оценивания экзамена

<i>Номер задания</i>	<i>Количество баллов</i>
1	15
2	15
Всего	30 баллов

11. ОБРАЗЕЦ ТЕСТОВОГО ЗАДАНИЯ

- 1) Система шифрования Цезаря относится к :
 - а) шифрам перестановки;
 - б) шифрам сложной замены;
 - в) шифрам простой замены;
 - г) шифрованию методом гаммирования;
- 2) Система шифрования с применением магических квадратов относится к :
 - а) шифрам простой замены;
 - б) шифрам перестановки;
 - в) шифрам сложной замены;
 - г) шифрованию методом гаммирования;
- 3) Система шифрования Гронсфелда относится к :
 - а) шифрам сложной замены;
 - б) шифрам простой замены;
 - в) шифрам перестановки;
 - г) шифрованию методом гаммирования;
- 4) Система шифрования с применением таблиц Трисемуса относится к :
 - а) шифрам простой замены;
 - б) шифрам перестановки;
 - в) шифрам сложной замены;
 - г) шифрованию методом гаммирования;
- 5) Алгоритм шифрования RC6 является :
 - а) блочным алгоритмом с длиной блока 128 бит и длиной ключа 256 бит;
 - б) асимметричным алгоритмом, надежность которой основана на трудности вычисления дискретных логарифмов;
 - в) параметризованным алгоритмом с длиной блока в битах, кратной четырем, и произвольной длиной ключа в байтах;
 - г) асимметричным алгоритмом, надежность которой основана на трудности разложения большого числа на множители;
- 6) Алгоритм шифрования SAFER+ является :

- а) блочным алгоритмом с длиной блока 64 бита и длиной ключа 256 бит;
 - б) асимметричным алгоритмом, надежность которой основана на трудности вычисления дискретных логарифмов;
 - в) блочным алгоритмом с длиной блока 128 бит и длиной ключа 128, 192 или 256 бит;
 - г) асимметричным алгоритмом, надежность которой основана на трудности разложения большого числа на множители;
- 7) Криптосистема ГОСТ 28147-89 является :
- а) симметричной криптосистемой с длиной блока 128 бит и длиной ключа 64 бита;
 - б) асимметричной криптосистемой, надежность которой основана на трудности вычисления дискретных логарифмов;
 - в) симметричной криптосистемой с длиной блока 64 бита и длиной ключа 256 бит;
 - г) асимметричной криптосистемой, надежность которой основана на трудности разложения большого числа на множители;
- 8) Какой из алгоритмов блочного шифрования не использует структуру сети Фейстела?
- а) SAFER+;
 - б) DES;
 - в) ГОСТ 28147-89;
 - г) RC6;
- 9) Криптосистема DES является :
- а) симметричной криптосистемой с длиной блока 128 бит и длиной ключа 128 бит;
 - б) асимметричной криптосистемой, надежность которой основана на трудности вычисления дискретных логарифмов;
 - в) асимметричной криптосистемой, надежность которой основана на трудности разложения большого числа на множители;
 - г) симметричной криптосистемой с длиной блока 64 бита и длиной ключа 56 бит;
- 10) Что из ниже перечисленного не является режимом работы алгоритма шифрования ГОСТ 28147-89?
- а) режим простой замены;
 - б) режим обратной замены;
 - в) режим гаммирования;
 - г) режим гаммирования с обратной связью;
- 11) Какой из ниже приведенных алгоритмов шифрования является потоковым?
- а) RC4;
 - б) DES;
 - в) ГОСТ 28147-89;
 - г) RC6;
- 12) Криптосистема RSA (Ривеста-Шамира-Адлемана) является :
- а) симметричной криптосистемой с длиной блока 128 бит и длиной ключа 64 бита;
 - б) асимметричной криптосистемой, надежность которой основана на трудности разложения большого числа на множители;
 - в) асимметричной криптосистемой, надежность которой основана на трудности вычисления дискретных логарифмов;
 - г) симметричной криптосистемой с длиной блока 64 бита и длиной ключа 256 бит;
- 13) В каком режиме шифрования алгоритмом DES каждый блок исходного текста шифруется независимо от других блоков?
- а) в режиме электронной кодовой книги ECB (Electronic Code Book);
 - б) в режиме сцепления блоков шифрованного текста CBC (Cipher Block Chaining);
 - в) в режиме обратной связи по шифротексту CFB (Cipher Feed Back);
 - г) в режиме обратной связи по выходу OFB (Output Feed Back);
- 14) Криптосистема Эль-Гамала является :
- а) симметричной криптосистемой с длиной блока 128 бит и длиной ключа 64 бита;
 - б) асимметричной криптосистемой, надежность которой основана на трудности вычисления дискретных логарифмов;
 - в) асимметричной криптосистемой, надежность которой основана на трудности разложения большого числа на множители;
 - г) симметричной криптосистемой с длиной блока 64 бита и длиной ключа 256 бит;

- 15) Какой алгоритм цифровой подписи используется в стандарте цифровой подписи DSS (Digital Signature Standard)?
- а) RSA (Rivest, Shamir, Adleman);
 - б) EGSA (El Gamal Signature Algorithm);
 - в) ГОСТ Р 34.10-94;
 - г) DSA (Digital Signature Algorithm);
- 16) Какой алгоритм хэширования используется в стандарте безопасного хэширования SHS (Secure Hash Standard)?
- а) MD5;
 - б) SHA;
 - в) ГОСТ Р 34.10-94;
 - г) иной;
- 17) Два ключа используются в системах шифрования
- а) асимметричных
 - б) симметричных
 - в) потоковых
 - г) других
- 18) В каком из приведенных алгоритмов происходит шифрование блоками длиной 64 бит?
- а) DES, ГОСТ 28147-89
 - б) DES
 - в) ГОСТ 28147-89
 - г) SAFER+
- 19) В каком из приведенных алгоритмов происходит шифрование блоками длиной 128 бит?
- а) SAFER+
 - б) DES, ГОСТ 28147-89
 - в) DES
 - г) ГОСТ 28147-89
- 20) В каком из приведенных алгоритмов используется ключ длиной 56 бит?
- а) DES
 - б) DES, ГОСТ 28147-89
 - в) ГОСТ 28147-89
 - г) SAFER+
- 21) В каком из приведенных алгоритмов используется ключ длиной 256 бит?
- а) ГОСТ 28147-89
 - б) DES
 - в) DES, ГОСТ 28147-89
 - г) SAFER+
- 22) В каком из приведенных алгоритмов используется ключ длиной 128, 192 або 256 бит?
- а) SAFER+
 - б) DES, ГОСТ 28147-89
 - в) DES
 - г) ГОСТ 28147-89
- 23) В каком из приведенных алгоритмов в сети Фейстела происходит расширение полублока в полтора раза?
- а) DES
 - б) RC6
 - в) ГОСТ 28147-89
 - г) SAFER+
- 24) Сколько итераций осуществляется в сети Фейстела криптосистемы DES?
- а) 16
 - б) 24
 - в) 32
 - г) 48
- 25) Сколько итераций осуществляется в сети Фейстела криптосистемы ГОСТ 28147-89?
- а) 32
 - б) 24

- в) 16
 - г) 8
- 26) В каком из приведенных алгоритмов используется расширенная сеть Фейстела?
- а) RC6
 - б) DES
 - в) ГОСТ 28147-89
 - г) SAFER+
- 27) В каком из приведенных алгоритмов используется функция Эйлера?
- а) RSA
 - б) Эль-Гамаль
 - в) RC4
 - г) WAKE
- 28) В алгоритме RSA открытый ключ
- а) выбирают
 - б) вычисляют как обратный к тайному ключу по некоторому модулю
 - в) вычисляют как степень с показателем – тайным ключем по некоторому модулю
 - г) не существует
- 29) В алгоритме RSA закрытый ключ
- а) вычисляют как обратный к открытому ключу по некоторому модулю
 - б) вычисляют как степень с показателем – открытым ключем по некоторому модулю
 - в) выбирают
 - г) не связан с открытым ключем какой-либо зависимостью.
- 30) В алгоритме Эль-Гамала открытый ключ
- а) вычисляют как степень с показателем – тайным ключем по некоторому модулю
 - б) выбирают
 - в) вычисляют как обратный к тайному ключу по некоторому модулю
 - г) не существует

12. КРИТЕРИИ ОЦЕНИВАНИЯ

В течение семестра студент может получить до 70 баллов ($L1 + L2$) на лабораторных занятиях за выполнение двух индивидуальных заданий по написанию и защите рефератов и созданию программных приложений и до 30 баллов (M) за контрольную работу по тестам.

При оценивании индивидуального задания (до 35 баллов) учитываются:

- полнота освещения теоретических вопросов (до 6 баллов),
- уровень владения материалом (до 5 баллов),
- ориентация в смежных вопросах (до 2 баллов),
- качество оформления реферата (до 2 баллов),
- правильная работа разработанных программных приложений (до 12 баллов),
- удобство интерфейса для пользователя (до 4 баллов),
- возможность модернизации приложений в направлении расширения их функциональности (до 2 баллов),
- применение современных приемов и сред разработки приложений (до 2 баллов).

Студенту может быть добавлено до 10 баллов (D) за активную аудиторную работу, своевременную сдачу индивидуальных заданий, отсутствие пропусков занятий без уважительной причины. Таким образом, количество набранных баллов $K_z = \min\{(L1 + L2 + M + D); 100\}$.

Студент может сдавать экзамен для улучшения оценки K_z , или **обязан** сдавать экзамен, если $K_z < 60$. В этом случае ему предлагаются два теоретических вопроса. Правильный ответ на каждый теоретический вопрос оценивается от нуля до 15 баллов:

- правильный исчерпывающий ответ – 15 баллов;
- правильный ответ, потребовавший 1-2 уточнения – 13 - 14 баллов;
- в целом правильный ответ, потребовавший исправлений 1-2 ошибок – 10 – 12

баллов;

- удовлетворительный ответ с 1-2 ошибками, которые не смог исправить экзаменуемый – 7 – 9 баллов;
- ответ неудовлетворительный, но содержащий элементы, соответствующие сути поставленных вопросов – 1 – 6 баллов;
- ответ отсутствует – 0 баллов.

Оценка рассчитывается по формуле $K_э = L1 + L2 + T_1 + T_2$, где T_1, T_2 - баллы, полученные за ответы на теоретические вопросы.

Шкала соответствия баллов национальной шкале

Оценка по шкале ECTS	Оценка по 100-балльной шкале	Оценка по государственной шкале (экзамен, дифференцированный зачет)
A	90-100	5 (отлично)
B	80-89	4 (хорошо)
C	75-79	4 (хорошо)
D	70-74	3 (удовлетворительно)
E	60-69	3 (удовлетворительно)
FX	35-59	2 (неудовлетворительно) с возможностью повторной сдачи
F	0-34	2 (неудовлетворительно) с возможностью повторной сдачи при условии обязательного набора дополнительных баллов

13. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

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

Лабораторные занятия проводятся в компьютерном классе, оборудованном компьютерами с лицензионным программным обеспечением, доступом к сети Интернет, столами, доской.

14. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонНУ	Наличие электронной версии в ЭБС
<i>Основная литература</i>			
1.	Бабаш А.В., Криптографические методы защиты информации : учебник / А.В. Бабаш, Е.К. Баранова. — М. : КНОРУС, 2016. — 190 с. — (Бакалавриат и магистратура).		+
2.	Лось А.Б., Нестеренко А.Ю., Рожков М.И., Криптографические методы защиты информации: учебник для академического бакалавриата - М.: Юрайт, 2016		+
3.	Романец Ю.В. и др., Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001.	20	+

<i>Дополнительная литература</i>			
4.	Мельников В.В., Защита информации в компьютерных системах – М.: Финансы и статистика, 1997. – 368 с.	3	+
5.	Домарев В.В., Защита информации и безопасность компьютерных систем – К.: DiaSoft, 1999. – 476 с.	3	+
6.	Баричев С.Г. и др., Основы современной криптографии. – М.: «Горячая линия – Телеком», 2001.		+
7.	Хорев П.Б., Методы и средства защиты информации в компьютерных системах. – М.: Издательский центр «Академия», 2005.		+
8.	Новиков Е.А., Шитов Ю.А., Криптографические методы защиты информации - Учебное пособие. – Красноярск: Сибирский федеральный университет, 2008		+
9.	Куприянов А.И., Сахаров А.В., Шевцов В.А., Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений – М.: Издательский центр «Академия», 2006.		+
10.	Шнайер Брюс, Прикладная криптография, 2-е издание, Протоколы, алгоритмы и исходные тексты на языке С.		+
11.	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.	10	

15. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Библиотека Института вычислительного моделирования СО РАН. Режим доступа к ресурсу: http://library.krasn.ru/trudy/2008/Novikov_kript_metod_posobie.pdf
2. Поиск в электронных каталогах НБ ДонНУ. Режим доступа к ресурсу: <http://library.donnu-support.ru/catalog/>
3. Электронная библиотека СПбПУ. Режим доступа к ресурсу: <http://elib.spbstu.ru/dl/2889.pdf>
4. Единое окно доступа к образовательным ресурсам / Федеральный портал / Федеральный центр ЭОР / Единая коллекция ЦОР. Режим доступа к ресурсу: <http://window.edu.ru/catalog/>

16. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Визуальная среда программирования.

Рабочая программа рассмотрена и переутверждена на заседании кафедры прикладной математики и ТСУ с изменениями (без изменений) на 201_ год.

Протокол заседания кафедры № ____ от _____ 20____ г. .

Зав.кафедрой
прикладной математики и ТСУ _____

Рабочая программа рассмотрена и переутверждена на заседании кафедры прикладной математики и ТСУ с изменениями (без изменений) на 201_ год.

Протокол заседания кафедры № ____ от _____ 20____ г. .

Зав.кафедрой
прикладной математики и ТСУ _____

Рабочая программа рассмотрена и переутверждена на заседании кафедры прикладной математики и ТСУ с изменениями (без изменений) на 201_ год.

Протокол заседания кафедры № ____ от _____ 20____ г. .

Зав.кафедрой
прикладной математики и ТСУ _____

Рабочая программа рассмотрена и переутверждена на заседании кафедры прикладной математики и ТСУ с изменениями (без изменений) на 201_ год.

Протокол заседания кафедры № ____ от _____ 20____ г. .

Зав.кафедрой
прикладной математики и ТСУ _____

Рабочая программа рассмотрена и переутверждена на заседании кафедры прикладной математики и ТСУ с изменениями (без изменений) на 201_ год.

Протокол заседания кафедры № ____ от _____ 20____ г. .

Зав.кафедрой
прикладной математики и ТСУ _____

Рабочая программа рассмотрена и переутверждена на заседании кафедры прикладной математики и ТСУ с изменениями (без изменений) на 201_ год.

Протокол заседания кафедры № ____ от _____ 20____ г. .

Зав.кафедрой
прикладной математики и ТСУ _____