

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра прикладной математики и теории систем управления

УТВЕРЖДАЮ:



Проректор по научно-методической  
и учебной работе

Е.И. Скафа

«22» апреля 2020 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**  
**«МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ И**  
**ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

Направление подготовки:	02.04.02 Фундаментальная информатика и информационные технологии
Магистерская программа:	Фундаментальная информатика и информационные технологии
Программа подготовки:	Академическая магистратура
Квалификация:	Магистр
Форма обучения:	<u>очная</u> , очно-заочная, заочная нужное подчеркнуть

Донецк 2020

**УТВЕРЖДАЮ:**

Декан факультета математики  
и информационных технологий

И. А. Моисеенко

«16» апреля 2020 г.

МП



Программа учебной дисциплины «Математические основы защиты информации и информационной безопасности» составлена с учетом Федерального государственного образовательного стандарта высшего образования направления подготовки 02.04.02 Фундаментальная информатика и информационные технологии, утвержденного приказом Министерства образования и науки Российской Федерации от «23» августа 2017 г. № 811; основной образовательной программы и учебного плана направления подготовки 02.04.02 Фундаментальная информатика и информационные технологии, разработанных в ГОУ ВПО «Донецкий национальный университет».

Разработчик:

Доцент кафедры прикладной математики и  
теории систем управления

Л.А. Рыбалко

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

Протокол № 12 от « 9 » 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 Б1.Б.6 «Математические основы защиты информации и информационной безопасности» относится к базовой части профессионального блока дисциплин подготовки студентов по направлению подготовки 02.04.02 «Фундаментальная информатика и информационные технологии».

Изучение данной дисциплины основывается на базе дисциплин: «Дискретная математика», «Основы программирования», «Введение в объектно-ориентированное программирование», «Языки программирования», «Прикладные информационные технологии 1-8», «Математические модели в информационных технологиях 1-8».

Является основой для научно-исследовательской работы над магистерской диссертацией.

## 2. СТРУКТУРА ДИСЦИПЛИНЫ

<i>Характеристика учебной дисциплины</i>		
Направление подготовки	02.04.02 Фундаментальная информатика и информационные технологии	
Магистерская программа	Фундаментальная информатика и информационные технологии	
Образовательная программа	академическая магистратура	
Квалификация	магистр	
Количество содержательных модулей	2	
Дисциплина базовой / вариативной части образовательной программы	Базовая часть	
Формы контроля (МК, экзамен, зачет)	1 модульный контроль, 1 экзамен в 3 семестре	
Показатели	очная форма обучения	заочная форма обучения
Количество зачетных единиц (кредитов)	6	
Год подготовки	2	
Семестр	3	
Количество часов	216	
- лекционных	18	
- практических, семинарских	–	
- лабораторных	54	
- самостоятельной работы	144	
в т.ч. индивидуальное задание	–	
Недельное количество часов,	12	
в т.ч. аудиторных	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, 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 асимметричных криптографических систем;
- сформировать навыки компьютерной реализации алгоритмов защиты информации;
- развивать умение использовать математические методы и программирование в исследовательской и практической деятельности.

**Требования к результатам освоения дисциплины.** Процесс изучения дисциплины «Математические основы защиты информации и информационной безопасности» направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО РФ направления подготовки 02.04.02 – «Фундаментальная информатика и информационные технологии» и основной образовательной программы высшего профессионального образования направления подготовки 02.04.02 – «Фундаментальная информатика и информационные технологии» (магистерская программа: Фундаментальная информатика и информационные технологии):

***а) универсальные компетенции (УК):***

способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (УК-1);

способен управлять проектом на всех этапах его жизненного цикла (УК-2);

способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия (УК-4);

способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия (УК-5);

способен определять и реализовывать приоритеты собственной деятельности и способы её совершенствования на основе самооценки (УК-6);

***б) общепрофессиональные компетенции (ОПК):***

способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий (ОПК-1);

способен применять компьютерные/суперкомпьютерные методы, современное программное обеспечение (в том числе отечественного производства) для решения задач профессиональной деятельности (ОПК-2);

способен проводить анализ математических моделей, создавать инновационные методы решения прикладных задач профессиональной деятельности в области информатики и математического моделирования (ОПК-3);

способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учётом требований информационной безопасности (ОПК-4);

способен устанавливать и сопровождать программное обеспечение информационных систем, осуществлять эффективное управление разработкой программных средств и проектов (ОПК-5);

***в) профессиональные компетенции (ПК):***

способен формализовать и алгоритмизировать поставленные задачи (ПК-3); способен написать программный код с использованием языков программирования, определять и манипулировать данными (ПК-4); способен определять входные-выходные данные каждого компонента и программного средства в целом (ПК-5); способен испытывать создаваемое программное средство и его компоненты (ПК-6); способен разрабатывать тестовые документы, включая план тестирования (ПК-7); способен устанавливать и настраивать программное обеспечение (ПО) для обеспечения работы пользователей с БД (ПК-8); способен осуществлять сбор данных для выявления требований к типовой ИС в соответствии с трудовым заданием (ПК-10); способен кодировать на языках программирования в

соответствии с трудовым заданием (ПК-12); способен оформлять технические документы в соответствии с заданным стандартом (ПК-13); способен разрабатывать эксплуатационные документы, адресованные конечному пользователю компьютерной системы (ПК-14); способен формализовать и документировать требования к функциям системы (ПК-15); способен формализовать и документировать требования к системе и подсистеме (ПК-16).

**В результате изучения учебной дисциплины студент должен**

**Знать:**

- ✓ основные математические проблемы, на которых базируется криптографическая защита информации;
- ✓ основные алгоритмы работы с большими числами;
- ✓ общие положения асимметричных криптосистем.

**Уметь:**

- ✓ применять программные методы защиты информации.

**Владеть:**

- ✓ навыками компьютерной реализации алгоритмов защиты информации.

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

Порядковый номер и тема	Краткое содержание темы
<b>Содержательный модуль 1</b>	
Тема 1. Введение в информационную безопасность	Основные понятия, методы, сервисы и угрозы информационной безопасности. Классификация криптографических методов защиты информации.
Тема 2. Системы шифрования с открытым ключом. Метод RSA	Особенности систем с открытым ключом. Модулярная арифметика. Функция Эйлера $\phi(n)$ . Алгоритм RSA. Расширенный алгоритм Евклида. Алгоритм быстрого возведения в степень по модулю. Генерация простых чисел. Решето Эратосфена. Метод пробных делений. Решето Аткина. Тест Поклингтона. Генерация простых чисел. Символ Лежандра. Тест простоты Миллера–Рабина.
Тема 3. Криптостойкость RSA. Алгоритмы факторизации	Метод Ферма. $(p - 1)$ –метод Полларда. $(p + 1)$ –метод Вильямса. $p$ –метод Полларда. $p$ –метод Полларда для вычисления дискретного логарифма.
<b>Содержательный модуль 2</b>	
Тема 4. Криптографические методы, основанные на задаче дискретного логарифмирования в конечном поле	Протокол Диффи-Хеллмана. Электронная цифровая подпись и ее свойства. Односторонние функции. Хеш-функции. Алгоритм создания электронной цифровой подписи. Алгоритм построения ЭЦП Эль-Гамала.
Тема 5. Эллиптические кривые и их приложения в криптографии	Определение эллиптической кривой. Эллиптические кривые в проективных координатах. Эллиптические кривые в якобиановых проективных координатах. Число точек эллиптической кривой. Алгоритм факторизации Ленстры ECF. Рекордные разложения метода ECFM. "Скрученные" кривые и метод Монтгомери. Кривые Эдвардса.

## Тематический план

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	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа
Содержательный модуль 1												
Тема 1. Введение в информационную безопасность	12	2		2	8							
Тема 2. Системы шифрования с открытым ключом. Метод RSA	46	4		12	30							
Тема 3. Криптостойкость RSA. Алгоритмы факторизации	54	4		14	36							
Итого по содержательному модулю 1	112	10		28	74							
Содержательный модуль 2												
Тема 4. Криптографические методы, основанные на задаче дискретного логарифмирования в конечном поле	41	3		10	28							
Тема 5. Эллиптические кривые и их приложения в криптографии	63	5		16	42							
Итого по содержательному модулю 2	104	8		26	70							
Всего по дисциплине	216	18		54	144							

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

## Темы лекционных занятий

№ п/п	Название темы	Количество часов
1	Тема 1. Введение в информационную безопасность	2
2	Тема 2. Системы шифрования с открытым ключом. Метод RSA	4
3	Тема 3. Криптостойкость RSA. Алгоритмы факторизации	4
4	Тема 4. Криптографические методы, основанные на задаче дискретного логарифмирования в конечном поле	3

5	Тема 5. Эллиптические кривые и их приложения в криптографии	5
	<b>ВСЕГО</b>	<b>18</b>

#### Темы лабораторных занятий

<i>№ п/п</i>	<i>Название темы</i>	<i>Количество часов</i>
1	Тема 1. Основные понятия, методы, сервисы и угрозы информационной безопасности. Классификация криптографических методов защиты информации.	2
2	Тема 2. Особенности систем с открытым ключом. Модулярная арифметика. Функция Эйлера $\varphi(n)$ . Алгоритм RSA.	4
3	Тема 3. Расширенный алгоритм Евклида. Алгоритм быстрого возведения в степень по модулю. Генерация простых чисел. Решето Эратосфена. Метод пробных делений.	6
4	Тема 4. Тест Поклингтона. Тест простоты Миллера–Рабина.	2
5	Тема 5. Метод Ферма. $(p - 1)$ –метод Полларда.	2
6	Тема 6. $(p + 1)$ –метод Вильямса. $p$ –метод Полларда.	2
7	Тема 7. $p$ –метод Полларда для вычисления дискретного логарифма.	2
8	Тема 8. Протокол Диффи-Хеллмана. Электронная цифровая подпись и ее свойства. Односторонние функции. Хеш-функции.	4
9	Тема 9. Алгоритм создания электронной цифровой подписи. Алгоритм построения ЭЦП Эль-Гамала.	4
10	Тема 10. Определение эллиптической кривой. Эллиптические кривые в проективных координатах.	4
11	Тема 11. Число точек эллиптической кривой.	2
12	Тема 12. Алгоритм факторизации Ленстры ECF.	2
13	Тема 13. "Скрученные" кривые и метод Монтгомери.	4
14	Тема 14. Криптографические протоколы на эллиптических кривых	4
15	Тема 15. Модульный контроль.	2
16	Тема 16. Защита индивидуальных заданий.	8
	<b>ВСЕГО</b>	<b>54</b>

## 6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

### Организация самостоятельной работы студентов

<i>№ п/п</i>	<i>Название темы</i>	<i>Количество часов</i>
1	Тема 1. Введение в информационную безопасность	8
2	Тема 2. Системы шифрования с открытым ключом. Метод RSA	30
3	Тема 3. Криптостойкость RSA. Алгоритмы факторизации	36
4	Тема 4. Криптографические методы, основанные на задаче дискретного логарифмирования в конечном поле	28
5	Тема 5. Эллиптические кривые и их приложения в криптографии	42
	<b>ВСЕГО</b>	<b>144</b>

## 7. ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ

### Цель:

Формирование и развитие профессиональных знаний и умений в области защиты информации; изучение соответствующей терминологии; анализ существующих подходов и алгоритмов в области защиты информации; формирование базового уровня подготовки для последующего анализа и решения проблем шифрования, передачи и хранения информации; формирование навыков компьютерной реализации современных алгоритмов защиты информации; развитие умений 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; получать практические навыки самостоятельной работы с учебной, методической и научной литературой.

Каждое индивидуальное задание состоит из 2х частей: реферативной, в которой должен быть приведен соответствующий теоретический материал по математическим основам защиты информации, и Windows-приложения, реализующего рассмотренные в первой части алгоритмы.

### Задания:

#### Пример индивидуального задания №1

##### Элементы теории чисел.

- a) Модулярная арифметика.
- b) Алгоритм Евклида для нахождения наибольшего общего делителя.
- c) Вычисление обратных величин.
- d) Расширенный алгоритм Евклида.
- e) Китайская теорема об остатках.
- f) Квадратичные вычеты.
- g) Программная реализация операций модулярной арифметики и вычисления обратных величин с помощью расширенного алгоритма Евклида; решение линейных систем сравнений.

#### Пример индивидуального задания №2

##### Криптосистемы на эллиптических кривых.

- a) Математические основы.
- b) Выбор параметров кривой.
- c) Построение криптосистем. Алгоритмы эффективной реализации операций.
- d) Программная реализация.

## 8. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1. Основные понятия, методы, сервисы и угрозы информационной безопасности.
2. Классификация криптографических методов защиты информации.
3. Особенности систем с открытым ключом. Модулярная арифметика. Функция Эйлера  $\varphi(n)$ .
4. Алгоритм RSA.
5. Простые числа. Теорема о бесконечном множестве простых чисел. Оценка распределения простых чисел на множестве натуральных чисел.
6. Тесты Ферма и Соловея-Штрассена простоты чисел.
7. Тест Миллера-Рабина простоты чисел.
8. Алгоритм Евклида для нахождения наибольшего общего делителя. Расширенный алгоритм Евклида.
9. Бинарные алгоритмы вычисления степени большого числа.



10. Генерация простых чисел. Решето Эратосфена. Метод пробных делений.
11. Китайская теорема об остатках.
12. Квадратичные вычеты.
13. Алгоритмы разложения большого числа на множители. Эвристики Флойда и Брента.
14. Метод Ферма.  $(p - 1)$ -метод Полларда.
15.  $(p + 1)$ -метод Вильямса.  $p$ -метод Полларда.
16. Определение дискретного логарифма.
17. Алгоритмы вычисления квадратного корня.
18. Математические основы криптосистем на эллиптических кривых.
19. Выбор параметров эллиптической кривой.
20. Определение эллиптической кривой. Эллиптические кривые в проективных координатах.
21.  $p$ -метод Полларда для вычисления дискретного логарифма.
22. Протокол Диффи-Хеллмана. Электронная цифровая подпись и ее свойства.
23. Односторонние функции. Хеш-функции.
24. Алгоритм создания электронной цифровой подписи. Алгоритм построения ЭЦП Эль-Гамала.
25. Число точек эллиптической кривой.
26. Алгоритм факторизации Ленстры ECF.
27. «Скрученные» кривые и метод Монтгомери.
28. Криптографические протоколы на эллиптических кривых

## 9. ОБРАЗЕЦ МОДУЛЬНОГО КОНТРОЛЯ

### ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Факультет математики и информационных технологий

Направление подготовки:	<b>02.04.02 Фундаментальная информатика и информационные технологии</b>
Магистерская программа:	<b>Фундаментальная информатика и информационные технологии</b>
Программа подготовки:	<b>Академическая магистратура</b>
Семестр	<b>3</b>
Учебная дисциплина	<b>Математические основы защиты информации и информационной безопасности</b>

### МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА

#### ВАРИАНТ №1

1. Классификация криптографических методов защиты информации.
2. Генерация простых чисел. Решето Эратосфена. Метод пробных делений.

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

<i>Номер задания</i>	<i>Количество баллов</i>
1	10
2	10
<b>Всего</b>	<b>20</b>

## 10. ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

#### Теоретические вопросы к экзамену

1. Основные понятия, методы, сервисы и угрозы информационной безопасности.
2. Классификация криптографических методов защиты информации.
3. Особенности систем с открытым ключом. Модулярная арифметика. Функция Эйлера  $\varphi(n)$ .
4. Алгоритм RSA.
5. Простые числа. Теорема о бесконечном множестве простых чисел. Оценка распределения простых чисел на множестве натуральных чисел.
6. Тесты Ферма и Соловея-Штрассена простоты чисел.
7. Тест Миллера-Рабина простоты чисел.
8. Алгоритм Евклида для нахождения наибольшего общего делителя. Расширенный алгоритм Евклида.
9. Бинарные алгоритмы вычисления степени большого числа.
10. Генерация простых чисел. Решето Эратосфена. Метод пробных делений.
11. Китайская теорема об остатках.
12. Квадратичные вычеты.

13. Алгоритмы разложения большого числа на множители. Эвристики Флойда и Брента.
14. Метод Ферма.  $(p - 1)$ –метод Полларда.
15.  $(p + 1)$ –метод Вильямса.  $p$ –метод Полларда.
16. Определение дискретного логарифма.
17. Алгоритмы вычисления квадратного корня.
18. Математические основы криптосистем на эллиптических кривых.
19. Выбор параметров эллиптической кривой.
20. Определение эллиптической кривой. Эллиптические кривые в проективных координатах.
21.  $p$ –метод Полларда для вычисления дискретного логарифма.
22. Протокол Диффи-Хеллмана. Электронная цифровая подпись и ее свойства.
23. Односторонние функции. Хеш-функции.
24. Алгоритм создания электронной цифровой подписи. Алгоритм построения ЭЦП Эль-Гамала.
25. Число точек эллиптической кривой.
26. Алгоритм факторизации Ленстры ECF.
27. "Скрученные" кривые и метод Монтгомери.
28. Криптографические протоколы на эллиптических кривых

### ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Факультет математики и информационных технологий

Направление подготовки: **02.04.02 Фундаментальная информатика и информационные технологии**

Магистерская программа: **Фундаментальная информатика и информационные технологии**

Программа подготовки: **Академическая магистратура**

Семестр: **3**

Учебная дисциплина: **Математические основы защиты информации и информационной безопасности**

#### БИЛЕТ №1

1. Классификация криптографических методов защиты информации.
2. Дискретный логарифм.  $p$ –метод Полларда для вычисления дискретного логарифма.
3. Вычислить  $2^{-1} \bmod 41$ .

Утверждено на заседании кафедры прикладной математики и ТСУ,  
протокол № \_\_\_\_ от « \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

Заведующий кафедрой  
Экзаменатор

Шевцов Д.В.  
Рыбалко Л.А.

#### Критерии оценивания экзамена

Номер задания	Количество баллов
1	5
2	5
3	10
<b>Всего</b>	<b>20</b>

## 11. ОБРАЗЕЦ ТЕСТОВОГО ЗАДАНИЯ

Не предусмотрено.

## 12. КРИТЕРИИ ОЦЕНИВАНИЯ

В течение семестра студент может получить до 80 баллов на лабораторных занятиях за выполнение двух индивидуальных заданий по подготовке и защите рефератов (до 40 баллов) и созданию программных приложений (до 40 баллов) и до 20 баллов за модульный контроль

При оценивании задания учитываются:

- полнота освещения теоретических вопросов (до 8 баллов),
- уровень владения материалом (до 8 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).

Таким образом, количество набранных баллов  $K_z \leq 100$ . По желанию студента эта оценка **перед началом экзамена** может быть принята как экзаменационная:  $K_э = K_z$ .

Студент **имеет право** сдавать экзамен для улучшения оценки  $K_z$ , или **обязан** сдавать экзамен, если  $K_z < 60$ . В этом случае он берет билет, содержащий два теоретических вопроса и практическое задание. Ответ на каждый теоретический пункт оценивается от нуля до 5 баллов:

- правильный ответ, потребовавший не более одного уточнения – 5 баллов;
- в целом правильный ответ, потребовавший 2-3 уточнения – 4 балла;
- удовлетворительный ответ с 1-2 ошибками, которые не смог исправить экзаменуемый – 3 балла;
- ответ неудовлетворительный, но содержащий элементы, соответствующие сути поставленных вопросов – 1 – 2 балла;
- ответ отсутствует – 0 баллов.

Ответ на практический пункт оценивается от нуля до 10 баллов:

- правильный ответ – 10 баллов;
- в целом правильный ответ, потребовавший 1-3 уточнения – 7 - 9 баллов;
- удовлетворительное решение с 1-3 ошибками, которые не смог исправить экзаменуемый – 4 - 6 баллов;
- ответ неудовлетворительный, но содержащий элементы, соответствующие сути решения задачи – 1 – 3 балла;
- ответ отсутствует – 0 баллов.

Экзаменационная оценка рассчитывается по формуле  $K_э = L + T_1 + T_2 + P_3$ , где  $T_1, T_2$  - баллы, полученные за ответы на теоретические вопросы,  $P_3$  - баллы, полученные за практическое задание,  $L$  - баллы, полученные за выполнение индивидуальных заданий.

**Шкала соответствия баллов национальной шкале**

Оценка по шкале ECTS	Оценка по 100-балльной шкале	Оценка по государственной шкале (экзамен, дифференцированный зачет)
<b>A</b>	90-100	5 (отлично)
<b>B</b>	80-89	4 (хорошо)
<b>C</b>	75-79	4 (хорошо)
<b>D</b>	70-74	3 (удовлетворительно)
<b>E</b>	60-69	3 (удовлетворительно)
<b>FX</b>	35-59	2 (неудовлетворительно) с возможностью повторной сдачи
<b>F</b>	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.

Для проведения лабораторных занятий требуется дисплейный класс ПК с установленной ОС **Windows**

**14. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА**

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонНУ	Наличие электронной версии в ЭБС
<b>Основная литература</b>			
1.	Бабаш А.В., Криптографические методы защиты информации : учебник / А.В. Бабаш, Е.К. Баранова. — М. : КНОРУС, 2016. — 190 с. — (Бакалавриат и магистратура).	0	+
2.	Лось А.Б., Нестеренко А.Ю., Рожков М.И., Криптографические методы защиты информации: учебник для академического бакалавриата - М.: Юрайт, 2016	0	+
3.	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	20	+
<b>Дополнительная литература</b>			
1.	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	+
2.	Коноплева, И. А. Информационные технологии : учебное пособие / И. А. Коноплева, О. А. Хохлова, А. В. Денисов. - 2-е изд. - Москва : Проспект, 2014. - 327	0	+

	с.		
3.	Воронков Б.Н. Криптографические методы защиты информации: Учебное пособие для вузов - Издательско-полиграфический центр Воронежского государственного университета, 2008.	0	+
4.	Основы криптографии : (письменная справка) / [сост. Н. А. Фесенко] ; ДонНУ. Науч. б-ка. Справ.-библиогр. отд. - Донецк : ДонНУ, 2015. - 16 с. (1 экз.)	3	+
5.	Ишмухаметов Ш.Т., Рубцова Р.Г.. Математические основы защиты информации. Электронное учебное пособие для студентов института вычислительной математики и информационных технологий: Казань 2012. – 139 с.	0	+
6.	Романец Ю.В. и др., Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001.	1	+

## 15. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Поиск в электронных каталогах НБ ДонНУ. Режим доступа к ресурсу: <http://library.donnu-support.ru/catalog/>

2. Блоги по программированию и не только от Microsoft (TechNet Blogs) [Электронный ресурс]. Режим доступа к ресурсу: <http://blogs.technet.com>

3. Материал из Википедии — свободной энциклопедии [Электронный ресурс]. Режим доступа к ресурсу: <http://ru.wikipedia.org>

4. Единое окно доступа к образовательным ресурсам / Федеральный портал / Федеральный центр ЭОР / Единая коллекция ЦОР. Режим доступа к ресурсу: <http://window.edu.ru/resource/848/23848>

5. Единое окно доступа к образовательным ресурсам / Федеральный портал / Федеральный центр ЭОР / Единая коллекция ЦОР. Режим доступа к ресурсу: <http://window.edu.ru/resource/128/78128>

## 16. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Визуальные среды программирования.

Рабочая программа рассмотрена и переутверждена на заседании кафедры прикладной математики и ТСУ с изменениями (без изменений) на 20\_\_\_\_\_ год.

Протокол № \_\_\_\_ от «\_\_\_\_» \_\_\_\_\_ 20\_\_\_\_ г.

Заведующий. кафедрой

**Д.В. Шевцов**

Рабочая программа рассмотрена и переутверждена на заседании кафедры прикладной математики и ТСУ с изменениями (без изменений) на 20\_\_\_\_\_ год.

Протокол № \_\_\_\_ от «\_\_\_\_» \_\_\_\_\_ 20\_\_\_\_ г.

Заведующий. кафедрой

**Д.В. Шевцов**