

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

«22» апреля 2020 г. Е.И. Скафа

МП

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
«КРИПТОГРАФИЯ»

| | |
|----------------------------|---|
| Направление подготовки: | 09.03.04 Программная инженерия |
| Образовательная программа: | бакалавриат |
| Квалификация: | Академический бакалавр |
| Форма обучения: | <u>очная, очно-заочная, заочная, в том</u> <u>числе с ускоренным сроком обучения</u> |

Донецк 2020

УТВЕРЖДАЮ:

Декан факультета математики
и информационных технологий

И. А. Моисеенко

«16» апреля 2020
МП

Программа учебной дисциплины «Криптография» составлена на основании Государственного образовательного стандарта высшего профессионального образования (ГОС ВПО) Донецкой Народной Республики (ДНР) по направлению подготовки 09.03.04 Программная инженерия, утвержденного приказом Министерства образования и науки ДНР от «21» января 2016 г. № 33;

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 09.03.04 Программная инженерия, разработанных в ГОУ ВПО «Донецкий национальный университет».

Разработчик:

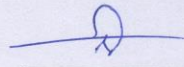
Старший преподаватель кафедры теории упругости и
вычислительной математики имени
академика А.С. Космодамианского



А. И. Занько

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

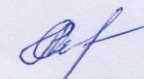
Протокол № 11 от «9» апреля 2020 г.
Заведующий кафедрой



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 «Криптография» относится к вариативной части профессионального блока и относится к циклу дисциплин по выбору студента.

Содержание дисциплины основывается на базе дисциплин:

- «Математический анализ»;
- «Программирование»;
- «Алгебра и геометрия»;
- «Защита информации»

и является основой для изучения следующих дисциплин:

- «Функциональное и логическое программирование».

2. СТРУКТУРА ДИСЦИПЛИНЫ

| <i>Характеристика учебной дисциплины</i> | | | | |
|--|---------------------------------------|-------------|------------------------|-------------|
| Направление подготовки | 09.03.04 Программная инженерия | | | |
| Профиль | Общий | | | |
| Образовательная программа | бакалавриат | | | |
| Квалификация | Академический бакалавр | | | |
| Количество содержательных модулей | 4 | | | |
| Дисциплина базовой / вариативной части образовательной программы | Выбор студента. Профессиональный блок | | | |
| 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 | 4 | |
| Год подготовки | 4 | 4 | 4 | |
| Семестр | 8 | 8 | 8 | |
| Количество часов | 144 | 144 | 144 | |
| - лекционных | 40 | 40 | 10 | |
| - практических, семинарских | - | - | - | |
| - лабораторных | 40 | 40 | 10 | |
| - самостоятельной работы | 64 | 64 | 124 | |
| в т.ч. индивидуальное задание | 0 | 0 | 0 | |
| Недельное количество часов, | 14,4 | 14,4 | | |
| в т.ч. аудиторных | 8 | 8 | | |

3. ОПИСАНИЕ ДИСЦИПЛИНЫ

Цели и задачи

Цели учебной дисциплины.

- 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 учебной дисциплины.

- освоение студентами теоретических сведений (определения, теоремы, их доказательства, связи между ними и их использование в криптографии) и методов реализации крипто- графических систем на современных ЭВМ.

Требования к результатам освоения дисциплины. процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ГОС ВПО по данному направлению подготовки (профилю):

а) общекультурных (ОК): способность к самоорганизации самообразованию (ОК-7);

б) общепрофессиональных (ОПК): владением основными концепциями, принципами, теориями и фактами, связанными с информатикой (ОПК-1); способностью осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять её в требуемом формате с использованием информационных, компьютерных и сетевых технологий (ОПК-4);

в) профессиональных (ПК):

научно-исследовательская деятельность: способностью к формализации в своей предметной области с учётом ограничений используемых методов исследования (ПК-12); готовностью к использованию методов и инструментальных средств исследования объектов профессиональной деятельности (ПК-13);

аналитическая деятельность: способностью формализовать предметную область программного проекта и разработать спецификации для компонентов программного продукта (ПК-16).

В результате изучения учебной 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.

владеть:

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

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И ФОРМЫ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА

Курс дисциплины «Криптография» предусматривает следующие формы организации учебного процесса: лекции, лабораторные занятия, самостоятельная работа студента.

Материал излагается с использованием объяснительно-иллюстративных, эвристических и исследовательских методов преподавания. При проведении лекций для обсуждения материала используются раздаточные материалы, таблицы, тексты лекций в электронном варианте.

В учебном процессе применяются активные и интерактивные формы проведения занятий (разбор конкретных ситуаций, дискуссия, полемика), внеаудиторная самостоятельная работа, балльно-рейтинговая система оценки успеваемости, личностно-ориентированное обучение, проблемное обучение, блочно-модульное обучение.

Использование в учебном процессе интернет-ресурсов по данному курсу; рассмотрение задач, максимально приближенных к возникающим на практике ситуациям, с элементами дискуссии и полемикой в процессе поиска путей решения сформулированных проблем; контрольные работы.

Самостоятельная работа студентов предусматривает выполнение индивидуальных заданий, подготовку к лабораторным занятиям, изучение учебной литературы, составление конспектов, защиту индивидуальных заданий.

| 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 и задачи криптографии |
| Тема 2. Элементарные шифры. Частотный анализ. | Исторический обзор криптографических методов |
| | Содержательный модуль 2. «Классическая криптография» |
| Тема 3. Шифры Плейфейера, Виженера | Рассматриваются криптографические методы примерно 14 – 19 веков, их надежность, крипто стойкость. Шифры Плейфейера, 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. При- чины успешного криптоанализа | Изучается представление информации в цифровой форме, шифр ШОБ |
| | Содержательный модуль 3 «Математические основы |

| | |
|--|---|
| | <i>криптографических методов»</i> |
| 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. Взаимнообратные ключи в кольце остатков | Кольцо остатков, арифметические операции в нем, доказательство свойств |
| | <i>Содержательный модуль 4 «Аналитические шифры»</i> |
| 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 порядка. Аффинный шифр k-го порядка. | Использование в качестве ключей матриц k-го порядка. 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 | 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 | самостоятельна я работа | индивидуальна | | лекции | практические | лабораторные | самостоятельна я работа | | индивидуальна | лекции | практические | лабораторные | | самостоятельна я работа | индивидуальна | лекции | практические | самостоятельна я работа |
| | Содержательный модуль 1. «Элементарная криптография» | | | | | | | | | | | | | | | | | | | | |
| Тема 1. Криптография, ее понятия и терминология | 11 | 3 | | 3 | 5 | | 11 | 3 | | 3 | 5 | | 12 | 1 | | 1 | 10 | | | | |
| Тема 2. Элементарные шифры. Частотный анализ. | 11 | 3 | | 3 | 5 | | 11 | 3 | | 3 | 5 | | 12 | 1 | | 1 | 10 | | | | |
| Итого по содержательному модулю 1 | 22 | 6 | | 6 | 10 | | 22 | 6 | | 6 | 10 | | 24 | 2 | | 2 | 20 | | | | |
| | Содержательный модуль 2. «Классическая криптография» | | | | | | | | | | | | | | | | | | | | |
| Тема 3. Шифры Плейфейера, Виженера | 11 | 3 | | 3 | 5 | | 11 | 3 | | 3 | 5 | | 12 | 1 | | 1 | 10 | | | | |
| Тема 4. Шифры перестановок Матричный шифр обхода | 11 | 3 | | 3 | 5 | | 11 | 3 | | 3 | 5 | | 12 | 1 | | 1 | 10 | | | | |
| Тема 5. Подача материала в цифровой форме, шифр одноразового блока. При- чины успешного криптоанализа | 11 | 3 | | 3 | 5 | | 11 | 3 | | 3 | 5 | | 12 | 1 | | 1 | 10 | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|----------|--|----------|-----------|--|-----------|----------|--|----------|-----------|--|-----------|----------|--|----------|-----------|--|--|--|--|--|--|
| Итого по содержательному модулю 2 | 33 | 9 | | 9 | 15 | | 33 | 9 | | 9 | 15 | | 36 | 3 | | 3 | 30 | | | | | | |
| | Содержательный модуль 3 «Математические основы криптографических методов» | | | | | | | | | | | | | | | | | | | | | | |
| Тема 6. Общие характеристики ШОБ и криптосистемы DES. Структура системы DES. Система DES | 11 | 3 | | 3 | 5 | | 11 | 3 | | 3 | 5 | | 12 | 1 | | 1 | 10 | | | | | | |
| Тема 7. Математический подход к криптографическим алгоритмам и его следствие. Алгоритм Эвклида. Следствие теоремы Эвклида | 11 | 3 | | 3 | 5 | | 11 | 3 | | 3 | 5 | | 12 | 1 | | 1 | 10 | | | | | | |
| Тема 8. Конгруэнции, их свойства. Кольцо остатков. Взаимнообратные ключи в кольце остатков | 11 | 3 | | 3 | 5 | | 11 | 3 | | 3 | 5 | | 12 | 1 | | 1 | 10 | | | | | | |
| Итого по содержательному модулю 3 | 33 | 9 | | 9 | 15 | | 33 | 9 | | 9 | 15 | | 36 | 3 | | 3 | 30 | | | | | | |
| | Содержательный модуль 4 «Аналитические шифры» | | | | | | | | | | | | | | | | | | | | | | |
| Тема 9. Кольцо матриц. Обратная матрица как дешифрующий ключ | 14 | 4 | | 4 | 6 | | 14 | 4 | | 4 | 6 | | 13 | 1 | | 1 | 11 | | | | | | |
| Тема 10. Аффинные шифры 1-го порядка. Подходы к взлому шифров | 14 | 4 | | 4 | 6 | | 14 | 4 | | 4 | 6 | | 13 | 1 | | 1 | 11 | | | | | | |
| Тема 11. Линейный шифр k-го порядка. Аффинный | 14 | 4 | | 4 | 6 | | 14 | 4 | | 4 | 6 | | 11 | | | | 11 | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | |
|--|------------|-----------|--|-----------|-----------|--|------------|-----------|--|-----------|-----------|--|------------|-----------|--|-----------|------------|--|--|--|--|--|
| шифр k-го порядка. | | | | | | | | | | | | | | | | | | | | | | |
| Тема 12. Примеры шифрования с матричными ключами. | 14 | 4 | | 4 | 6 | | 14 | 4 | | 4 | 6 | | 11 | | | | 11 | | | | | |
| <i>Итого по содержательному модулю 4</i> | 56 | 16 | | 16 | 24 | | 56 | 16 | | 16 | 24 | | 48 | 2 | | 2 | 44 | | | | | |
| <i>Всего по дисциплине</i> | 144 | 40 | | 40 | 64 | | 144 | 40 | | 40 | 64 | | 144 | 10 | | 10 | 124 | | | | | |

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

Темы лекционных занятий

| <i>№ п/п</i> | <i>Название темы</i> | <i>Количество часов</i> |
|------------------|---|-----------------------------|
| 1. | Криптография, ее понятия и терминология | 3 |
| 2. | Элементарные шифры. Частотный анализ. | 3 |
| 3. | Шифры Плейфейера, Виженера | 3 |
| 4. | Шифры перестановок Матричный шифр обхода | 3 |
| 5. | Подача материала в цифровой форме, шифр одноразового блока. Причины успешного криптоанализа | 3 |
| 6. | Общие характеристики ШОБ и криптосистемы DES. Структура системы DES. Система DES | 3 |
| 7. | Математический подход к криптографическим алгоритмам и его следствие. Алгоритм Эвклида. Следствие теоремы Эвклида | 3 |
| 8. | Конгруэнции, их свойства. Кольцо остатков. Взаимнообратные ключи в кольце остатков | 3 |
| 9. | Кольцо матриц. Обратная матрица как дешифрующий ключ | 4 |
| 10. | Аффинные шифры 1-го порядка. Подходы к взлому шифров | 4 |
| 11. | Линейный шифр k-го порядка. Аффинный шифр k-го порядка. | 4 |
| 12. | Примеры шифрования с матричными ключами. Понятие о механике теории относительности | 4 |
| | ВСЕГО | 40 |

Темы лабораторных занятий

| <i>№ п/п</i> | <i>Название темы</i> | <i>Количество часов</i> |
|------------------|---|-----------------------------|
| 1 | Криптография, ее понятия и терминология | 3 |
| 2 | Элементарные шифры. Частотный анализ. | 3 |
| 3 | Шифры Плейфейера, Виженера | 3 |
| 4 | Шифры перестановок Матричный шифр обхода | 3 |
| 5 | Подача материала в цифровой форме, шифр одноразового блока. Причины успешного криптоанализа | 3 |
| 6 | Общие характеристики ШОБ и криптосистемы DES. Структура системы DES. Система DES | 3 |
| 7 | Математический подход к криптографическим алгоритмам и его следствие. Алгоритм Эвклида. Следствие теоремы Эвклида | 3 |
| 8 | Конгруэнции, их свойства. Кольцо остатков. Взаимнообратные ключи в кольце остатков | 3 |
| 9 | Кольцо матриц. Обратная матрица как дешифрующий ключ | 4 |
| 10 | Аффинные шифры 1-го порядка. Подходы к взлому шифров | 4 |
| 11 | Линейный шифр k-го порядка. Аффинный шифр k-го порядка. | 4 |

| | | |
|----|--|-----------|
| 12 | Примеры шифрования с матричными ключами. Понятие о механике теории относительности | 4 |
| | ВСЕГО | 40 |

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 | Криптография, ее понятия и терминология | 5 |
| 2 | Элементарные шифры. Частотный анализ. | 5 |
| 3 | Шифры Плейфейера, Виженера | 5 |
| 4 | Шифры перестановок Матричный шифр обхода | 5 |
| 5 | Подача материала в цифровой форме, шифр одноразового блока. Причины успешного криптоанализа | 5 |
| 6 | Общие характеристики ШОБ и криптосистемы DES. Структура системы DES. Система DES | 5 |
| 7 | Математический подход к криптографическим алгоритмам и его следствие. Алгоритм Эвклида. Следствие теоремы Эвклида | 5 |
| 8 | Конгруэнции, их свойства. Кольцо остатков. Взаимнообратные ключи в кольце остатков | 5 |
| 9 | Кольцо матриц. Обратная матрица как дешифрующий ключ | 6 |
| 10 | Аффинные шифры 1-го порядка. Подходы к взлому шифров | 6 |
| 11 | Линейный шифр k-го порядка. Аффинный шифр k-го порядка. | 6 |
| 12 | Примеры шифрования с матричными ключами. Понятие о механике теории относительности | 6 |
| | ВСЕГО | 64 |

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.

9. ОБРАЗЕЦ МОДУЛЬНОГО КОНТРОЛЯ

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Факультет математики и информационных технологий

Направление подготовки: **09.03.04 Программная инженерия**

Программа подготовки: **бакалавриат**

Семестр **8**

Учебная дисциплина **Криптография**

МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА ВАРИАНТ №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
Преподаватель

Сторожев В. И.
Занько А. И.

Критерии оценивания модульного контроля

| <i>Номер задания</i> | <i>Количество баллов</i> |
|----------------------|--------------------------|
| 1 | 10 |
| 2 | 10 |
| 3 | 20 |
| Всего баллов | 40 |

10. ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Теоретические вопросы к экзамену

1. Алгоритм Эвклида и его следствие.
2. Конгруэнции и их свойства. Кольцо остатков.
3. Кольцо матриц. Нахождение обратной матрицы в качестве дешифрующего ключа.
4. Аффинный шифр 1-го порядка. Пример.
5. Аффинный шифр 2-го порядка. Пример.

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Факультет математики и информационных технологий

Направление подготовки: **09.03.04 Программная инженерия**

Программа подготовки: **бакалавриат**

Семестр **8**

Учебная дисциплина **Криптография**

БИЛЕТ №1

1. Конгруэнции и их свойства. Кольцо остатков.
2. Аффинный шифр 1-го порядка. Пример.

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

Заведующий кафедрой
Экзаменатор

Сторожев В. И.
Занько А. И.

Критерии оценивания экзамена

| <i>Номер задания</i> | <i>Количество баллов</i> |
|----------------------|--------------------------|
| 1 | 10 |
| 2 | 10 |
| 3 | 20 |
| Всего баллов | 40 |

11. ОБРАЗЕЦ ТЕСТОВОГО ЗАДАНИЯ -не предусмотрено программой-**12. КРИТЕРИИ ОЦЕНИВАНИЯ**

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

**Распределение баллов, которые могут получить студенты
в процессе изучения дисциплины**

| Организационно-учебная работа студента | СРС | | | | Всего |
|---|---------------------------|--|--|--|--------------|
| | Модульный контроль | Индивидуальная творческая работа | | | |
| Мах 100 баллов | мах 40 баллов | мах 20 баллов | мах 20 баллов | мах 20 баллов | 100 баллов |
| | | разработка доклада и презентации по выбранной теме | разработка приложения по расчету прикладной задачи | Разработок тестов по материалам лекций | |

Шкала соответствия баллов национальной шкале

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

13. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Лекционные занятия проводятся в аудитории, оснащенной мультимедийной техникой и доской.

Лабораторные 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 |
|----------------------------------|--|---------------------------------------|----------------------------------|
| Основная литература | | | |
| 1. | Вельшенбах, М. Криптография на Си и C++ в действии : [Учеб. пособие / М. Вельшенбах. - М. : Триумф, 2004. - 461 с. + 1 электрон. опт. диск (CD-ROM). | 4 | + |
| 2. | Осипян В. О. Криптография в задачах и упражнениях / В. О. Осипян, К. В. Осипян. - М. : Гелиос АРВ, 2004. - 144 с. | 4 | - |
| Дополнительная литература | | | |
| 3. | Кораблев, А. А. Криптография романа М. А. Булгакова "Мастер и Маргарита" [Электронный ресурс] : учебно-методическое пособие соответствует программе учебного курса дисциплины "Принципы филологической криптологии" / А. А. Кораблев ; ГОУ ВПО "Донецкий национальный университет", Филологический факультет, Кафедра истории русской литературы и теории словесности. - Донецк : ГОУ ВПО "ДонНУ", 2019. - Электронные текстовые данные (1файл). | - | + |
| 4. | Основы криптографии : (письменная справка) / [сост. Н. А. Фесенко] ; ДонНУ. Науч. б-ка. Справ.-библиогр. отд. - Донецк : ДонНУ, 2015. - 16 с. | 1 | + |

15. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Основы программирования на языке C++: Учебное пособие
http://tk.ulstu.ru/lib/books/lang_c_1.pdf
2. Использование визуальных компонент в C++ Builder: методические указания к лабораторным работам по программированию
http://pnu.edu.ru/media/filer_public/2013/03/04/mu_builder.pdf
3. Структуры данных и алгоритмы: программирование на языке C++. Учеб, пособие в 2 ч. Часть 1 <https://studfiles.net/preview/6324253/>
4. Краткий справочник по языку программирования c++
<http://dspace.univer.kharkov.ua/bitstream/123456789/1356/2/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%A3%D0%BA%D0%B0%D0%B7%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%2B%D0%A4.pdf>
5. Вестник Донецкого национального университета. Серия А: Естественные науки
<http://donnu.ru/vestnikA/archive>

16. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДОННУ № 46484614);
2. Microsoft Office (корпоративная лицензия ДОННУ лицензия № 46472919);

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

Сторожев В. И.

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

Сторожев В. И.

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

Сторожев В. И.