

Министерство науки и высшего образования  
Российской Федерации

Федеральное государственное бюджетное  
образовательное учреждение высшего образования  
«Донецкий государственный университет»

Факультет дополнительного и профессионального образования  
Кафедра инженерной и компьютерной педагогики



П.А. Машаров

« 29 » марта 2024 г.

МП

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ  
«КРИПТОГРАФИЯ И СТЕГАНОГРАФИЯ»**

Укрупненная группа направлений подготовки	44.00.00 - Образование и педагогические науки
Программа высшего образования	Программа бакалавриата
Направление подготовки	44.03.04 - Профессиональное обучение (по отраслям)
Профиль подготовки	Информатика и вычислительная техника
Квалификация	Бакалавр
Форма обучения	Очная, заочная

Рабочая программа адаптирована для лиц  
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины «Криптография и стеганография» для обучающихся по направлению подготовки 44.03.04 Профессиональное обучение (по отраслям) (Профиль подготовки: Информатика и вычислительная техника), составлена на основании Федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 44.03.04 Профессиональное обучение (по отраслям), утвержденного приказом Министерства образования и науки Российской Федерации от 10 января 2018 г. № 8 (с изм. и доп.), Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06 апреля 2021 г. № 245 (с изм. и доп.), в соответствии с учебным планом, утвержденным Ученым советом ФГБОУ ВО «ДонГУ» для набора 2024 года.

Разработчик:

ст. преподаватель кафедры инженерной и  
компьютерной педагогики



В.В. Бочаров

Рабочая программа одобрена на заседании кафедры инженерной и  
компьютерной педагогики

Протокол от 26 . 03 .2024 г. № 10\_\_



Заведующий кафедрой д-р пед. наук,  
проф.

М.Г. Коляда

СОГЛАСОВАНО:

И.о. декана факультета дополнительного  
и профессионального образования

28 . 03 .2024 г.



М.П. Загорный

Учебно-методическая комиссия факультета дополнительного и  
профессионального образования.

Протокол от 27 . 03 .2024 г. № 7\_\_.

Председатель



В.А. Тарасенко

Руководитель основной

профессиональной

образовательной программы,

д-р пед. наук, проф., зав. кафедрой ИКП

26 . 03 .2024 г.



М.Г. Коляда

## 1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Требования к предварительной подготовке обучающихся, предшествующие и сопутствующие дисциплины, на которых основывается изучение данной:

- базовая подготовка по математике в объеме программы средней школы

1.2. Дисциплины, курсовые работы и практики, для которых освоение данной дисциплины необходимо как предшествующее: Информационная безопасность, Правовые аспекты информационных технологий.

## 2. ОПИСАНИЕ ДИСЦИПЛИНЫ / ПРАКТИКИ / КУРСОВОЙ РАБОТЫ / ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

### 2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	44.03.04 Профессиональное обучение (Профиль: Информатика и вычислительная техника)
Шифр и название в соответствии с учебным планом	Б1.В.ДВ.3.2. Криптография и стеганография
Часть образовательной программы	Вариативная часть: дисциплины по выбору
Количество зачетных единиц / всего часов	2/72

### 2.2. Распределение часов по формам и периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы + контроль	всего	
Очная	2	3	12	–	24	36	72	зачет
Заочная	2	3	2	–	4	66	72	зачет

## 3. ЦЕЛИ ДИСЦИПЛИНЫ

Формирование у студентов понимания основ информационных технологий, знания компонентов ПК и периферического оборудования.

## 4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ КОМПОНЕНТА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, ИХ ИНДИКАТОРЫ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

### 4.1. Компетенции

ПК-3. Способен осуществлять техническую поддержку создания, модификации и сопровождения информационных систем.

ПК-4. Способен выполнять работы по созданию, модификации и сопровождению информационных систем

### 4.2. Индикаторы компетенций

ПК-3.И-1. Осуществляет криптографическую защиту информации в соответствии с требованиями инструкций и пожеланиями пользователей.

ПК-4.И-1. Осуществляет проектирование, модификацию и сопровождение систем и методик криптографической защиты информации соответствии с требованиями инструкций и пожеланиями пользователей

#### 4.3.Результаты обучения

ПК-3.И-1.1. Знает предназначение и функции методов криптографической защиты информации.

ПК-3.И-1.2. Умеет осуществлять выбор методов криптографической защиты информации.

ПК-3.И-1.3. Имеет навыки использования методов криптографической защиты информации.

ПК-4.И-1.1. Знает критерии методов криптографической защиты информации.

ПК-4.И-1.2. Умеет осуществлять выбор методов криптографической защиты информации, основываясь на требованиях пользователя, ПО и инструкциях.

ПК-4.И-1.3. Имеет навыки выбора и комплексного использования методов криптографической защиты информации.

Компетенции	Индикаторы	Результаты обучения
ПК-3. Способен осуществлять техническую поддержку создания, модификации и сопровождения информационных систем.	ПК-3.И-1. Осуществляет техническую поддержку пользователей в соответствии с требованиями инструкций и пожеланиями пользователей.	ПК-3.И-1.1. Знает предназначение и функции методов криптографической защиты информации. ПК-3.И-1.2. Умеет осуществлять выбор методов криптографической защиты информации. ПК-3.И-1.3. Имеет навыки использования методов криптографической защиты информации..
ПК-4. Способен выполнять работы по созданию, модификации и сопровождению информационных систем	ПК-4.И-1. Осуществляет проектирование, модификацию и сопровождение конфигурации рабочего места пользователя в соответствии с требованиями инструкций и пожеланиями пользователей	ПК-4.И-1.1. Знает критерии методов криптографической защиты информации. ПК-4.И-1.2. Умеет осуществлять выбор методов криптографической защиты информации, основываясь на требованиях пользователя, ПО и инструкциях. ПК-4.И-1.3. Имеет навыки выбора и комплексного использования методов криптографической защиты информации.

## 5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
<b>Раздел 1. Криптография и стеганография</b>	
1. Краткая история развития криптографии и стеганографии.	1.1.Диск Энея. 1.2.Квадрат Полибия. 1.3.Шифр Цезаря. 1.4.Развитие криптографии от Средних веков до Нового времени. 1.5.Тайнопись: восковые дощечки, татуировка, сообщение внутри варёных яиц,

	музыкальные ноты, газетный код, невидимые чернила, микроточки.
2. Стеганография	2.1.Стеганография изображений. 2.2.Текстовая стеганография. 2.3.Видеостеганография. 2.4.Аудиостеганография 2.5.Сетевая стеганографии.
3. Идеи и методы криптографии	3.1.Краткие сведения из теории чисел, применяемой в криптографии 3.2.Модели шифрования/дешифрования дискретных сообщений 3.3.Понятие стойкости криптосистемы
4. Способы формирования криптограмм	4.1.Блочное шифрование: симметричные блочные шифры; схемы образования блочных шифров с помощью сетей; многократное шифрование блоков. 4.2.Потоковые шифры: аддитивные потоковые шифры; применение линейных рекуррентных регистров для потокового шифрования
5. Асимметричные криптосистемы	5.1.Особенности асимметричных криптосистем 5.2.Основы построения асимметричных систем 5.3.Гибридная система шифрования.
6. Применения криптографии	6.1. Электронная цифровая подпись. 6.2. Хэширование. 6.3. Обеспечение безопасности электронных платежей.

## 6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 6.1.Форма обучения – очная, курс – 2, семестр – 3

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС	Всего
Раздел 1. Криптография и стеганография	12		24	36	72
1. Краткая история развития криптографии и стеганографии.			2	6	8
2. Стеганография	1		4	4	9
3. Идеи и методы криптографии	3		4	6	13
4. Способы формирования криптограмм	2		4	6	12
5. Асимметричные криптосистемы	3		5	7	15
6. Применения криптографии	3		5	7	15
ИТОГО ЗА КУРС	12		24	36	72

### 6.2.Форма обучения – заочная, курс – 2, семестр – 3)

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС	Всего
Раздел 1. Криптография и стеганография	2	4		66	72

1. Краткая история развития криптографии и стеганографии.		0,5		7,5	8
2. Стеганография		0,5		8,5	9
3. Идеи и методы криптографии	0,5	1		11,5	13
4. Способы формирования криптограмм	0,5	1		10,5	12
5. Асимметричные криптосистемы	0,5	0,5		14	15
6. Применения криптографии	0,5	0,5		14	15
ИТОГО ЗА КУРС	2	4		66	72

## 7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

### 7.1. Контрольные вопросы

#### Раздел 1

1. Предмет и задачи криптографии. История криптографии
2. Квадрат Полибия, шифр Цезаря, диск Энея
3. Предмет и задачи Стеганографии. Стеганографии.
4. Виды стеганографии
5. Математические основы криптографии
6. Делимость чисел. Признаки делимости. Простые и составные числа.
7. Нахождение НОД
8. Наибольший общий делитель. Взаимно простые числа.
9. Алгоритм Евклида для нахождения НОД.
10. Разложение числа на множители.
11. Методы симметричного шифрования
12. Методы перестановки.
13. Основные принципы поточного шифрования
14. Представление информации в двоичном коде
15. Шифры Виженера и Вернама.
16. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4
17. Криптосистемы с открытым ключом.
18. Структурная схема шифрования с открытым ключом.
19. Алгоритм RSA.
20. Алгоритмы хэширования
21. Аутентификация данных. Общие понятия. ЭП. MAC.
22. Деление методов шифрования на симметричные и асимметричные.
23. Симметричные методы
24. Центры сертификации в компьютерных сетях.
25. Сертификаты. Сертификат как файл и как понятие.
26. Сертификаты по типу выдачи и типу валидации
27. Явление коллизии в шифрах MD5.
28. Свойства сертификатов.
29. Отличие ЭЦП от цифровой подписи и электронной подписи.
30. Криптостойкость
31. Хэш-функции и дайджесты. Основная информация о них.
32. Алгоритмы SHA.
33. Отличие поточного и блочного методов шифрования.
34. Абсолютно стойкие шифры. Оценка надежности.
35. Криптографические методы защиты информации.
36. Три основных функции ЦС.
37. Алфавит в криптографии.
38. Логическая операция «исключающее или».

## 8. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Общая оценка знаний обучающихся по дисциплине проводится по -балльной шкале исходя из максимума, приведенного в таблице ниже. Организационно-учебная работа в аудитории оценивается на основе таких критериев как посещаемость занятий, своевременное и качественное выполнение домашних заданий, активность во время проведения лекционных и практических занятий (участие в обсуждении текущего и пройденного материала, решение задач и т.п.).

### 8.1.Семестр 4

Номера разделов	Виды работ	Максимальное количество баллов
-	Организационно-учебная работа в аудитории	10
	Самостоятельная работа	20
	Контрольные работы по практике	10
	Контрольная работа по теоретическому материалу	10
ИТОГО		50
Зачет		50
Общий итог за семестр		100

### Соответствие баллов оценке

Количество баллов из	ECTS	Оценка по пятибалльной шкале	
		Экзамен, дифференцированный зачет	Зачет
90-100	A	отлично	зачтено
80-89	B	хорошо	зачтено
75-79	C		зачтено
70-74	D	удовлетворительно	зачтено
60-69	E		зачтено
35-59	FX	неудовлетворительно	не зачтено
0-34	F		не зачтено

## 9. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- 1) для слепых и слабовидящих:
  - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
  - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
  - письменные задания оформляются увеличенным шрифтом.
- 2) для глухих и слабослышащих:
  - лекции оформляются в виде электронного документа;

- письменные задания выполняются на компьютере в письменной форме;
- экзамен проводится в письменной форме на компьютере; возможно проведение в форме тестирования.

3) для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- 1) для слепых и слабовидящих:
  - в печатной форме увеличенным шрифтом;
  - в форме электронного документа;
- 2) для глухих и слабослышащих:
  - в печатной форме;
  - в форме электронного документа.
- 3) для обучающихся с нарушениями опорно-двигательного аппарата:
  - в печатной форме;
  - в форме электронного документа.

## 10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в 3-м корпусе ДонГУ (г. Донецк, ул. Щорса). Для проведения 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-методическом кабинете Главного корпуса (ауд.).

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные на платформе Moodle Центра дистанционного образования ФГБОУ ВО «ДонГУ». При изучении дисциплины применяются электронное обучение и дистанционные образовательные технологии.

С использованием ресурсов платформы дистанционного образования осуществляется текущий контроль знаний обучающихся на основе тестирования и проверки результатов самостоятельной работы.

## 11. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

### 11.1. Основная литература

1. Васильева И. Н. Криптографические методы защиты информации. / И.Н. Романькова. - М.: Юрайт. 2024. -- 350 с.

2. Лось А. Б., Нестеренко А. Ю., Рожков М. И. Криптографические методы защиты информации для изучающих компьютерную безопасность. / А.Б. Лось, А.Ю. Нестеренко, М.И. Рожков. -- М.: Юрайт. 2024. -- 474 с.
  3. Романьков В. А. Введение в криптографию. Курс лекций. / В.А. Романьков. -- М.: Форум. 2023. -- 240 с.
- 11.2. Дополнительная литература
4. Рубин Фрэнк. Криптография с секретным ключом. Шифры. / Ф. Рубин. -- М.: ДМК Пресс. 2022. -- 386 с.
  5. Фомичев В. М. Криптографические методы защиты информации. Курс лекций. / В.М. Фомичев. -- М.: Прометей. 2023. -- 340 с.

## 12. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. **Национальная электронная библиотека (НЭБ):** федеральная государственная информационная система / Министерство Культуры РФ; Российская государственная библиотека. – Москва, - . – URL: <https://rusneb.ru/> (дата обращения: ..). – Режим доступа: свободный, подписка. Необходима установка программного обеспечения. – Текст: электронный.
2. **eLIBRARY.RU:** научная электронная библиотека: сайт. – Москва, - . – URL: <https://elibrary.ru> (дата обращения: ..). – Режим доступа: для авторизов. пользователей. – Текст: электронный.
3. Научная электронная библиотека **«КиберЛенинка»:** сайт / Ассоциация «Открытая наука». – Москва, - . – URL: <https://cyberleninka.ru/>. – Режим доступа: свободный. – Текст: электронный.
4. Электронно-библиотечная система **«Лань»:** [сайт]. – URL: <https://e.lanbook.com> (дата обращения: ..). – Режим доступа: для авторизов. пользователей. – Текст: электронный.
5. **ЭБС Юрайт:** электронная библиотечная система: сайт. – Москва, . – URL: <https://biblio-online.ru> (дата обращения: ..). – Режим доступа: для авторизов. пользователей. – Текст: электронный.
6. **Электронно-библиотечная система ДонГУ:** сайт / ФГБОУ ВО «ДонГУ». – Донецк, - . – URL: <http://library.donnu.ru/> (дата обращения: ..). – Режим доступа: свободный. – Текст: электронный.
7. **Электронный каталог** Научной библиотеки ДонГУ: раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://library.donnu.ru/catalog/> (дата обращения: ..). – Режим доступа: поиск свободный, электронные документы – для пользователей ДонГУ.
8. **Электронный архив ДонГУ:** раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://repo.donnu.ru/> (дата обращения: ..). – Режим доступа: свободный.

## 13. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows PRO (корпоративная лицензия ДонГУ № )
2. Microsoft Office (корпоративная лицензия ДонГУ № )
3. Антивирус Касперского, Adobe Acrobat Reader, xPDF (лицензии GPL, Apache, BSD для свободного программного обеспечения).