

Министерство науки и высшего образования
Российской Федерации

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

Факультет математики и информационных технологий
Кафедра прикладной механики и компьютерных технологий



УТВЕРЖДАЮ
проректор

«29» марта 2024 г.

МП

П.А. Машаров

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

КРИПТОГРАФИЯ

Укрупненная группа направлений
подготовки
Программа высшего образования
Направление подготовки
Профиль подготовки
Квалификация
Форма обучения

09.00.00 Информатика и вычислительная
техника
Программа бакалавриата
09.03.04 Программная инженерия
Программная инженерия
Бакалавр
Очная

Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины **«Криптография»** для обучающихся по направлению подготовки 09.03.04 Программная инженерия (Профиль: Программная инженерия), составлена на основании Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 09.03.04 Программная инженерия, утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 920 (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:

доц. кафедры прикладной механики
и компьютерных технологий,
к. техн. наук

А.-В.В. Мельник

Рабочая программа одобрена на заседании кафедры прикладной механики и компьютерных технологий
Протокол от 26.03.2024 г. № 14

Заведующий кафедрой

А.С. Гольцев

СОГЛАСОВАНО:

Декан факультета математики и
информационных технологий
28.03.2024 г.

И.А. Моисеенко

Учебно-методическая комиссия факультета математики и информационных технологий.
Протокол от 27.03.2024 г. № 3.
Председатель

Л. И. Селякова

Руководитель основной профессиональной
образовательной программы,
д-р физ.-мат. наук, проф.
26.03.2024 г.

А.С. Гольцев

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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

дисциплины программы бакалавриата: Алгебра и геометрия, Теория вероятности и математическая статистика, Объектно-ориентированное программирование, Математическая логика и теория алгоритмов, Алгоритмы и структуры данных, Программирование.

1.2. Дисциплины, курсовые работы и практики, для которых освоение данной дисциплины необходимо как предшествующее:

используются при написании выпускной квалификационной работы

2. ОПИСАНИЕ ДИСЦИПЛИНЫ

2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	09.03.04 Программная инженерия (Профиль: Программная инженерия)
Шифр и название в соответствии с учебным планом	Б1.В.ДВ.2.2 Криптография
Часть образовательной программы	Вариативная часть: выбор обучающегося
Количество зачетных единиц / всего часов	4 / 144

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	4	7	34	34	0	76	144	зачет

3. ЦЕЛИ 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, а также развитие у студентов логического обоснования выбранного метода шифрования, его математического обоснования и умения реализовать криптографический метод.

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

4.1. Компетенции

ПК-1. Способен использовать методы и инструментальные средства исследования объектов профессиональной деятельности.

4.2. Индикаторы компетенций

ПК-1.4. Умеет применять средства криптоанализа для исследования соответствия криптологического протокола современным требованиями к безопасности.

4.3. Результаты обучения

ПК-1.4.1. Знает особенности современных симметричных и асимметричных криптографических алгоритмов.

ПК-1.4.2. Владеет навыками разработки криптографических протоколов для различных практических задач (взаимная идентификация, электронная подпись, электронные деньги и т.п.).

ПК-1.4.3. Умеет разрабатывать эффективные с точки зрения вычислений алгоритмы расчета вспомогательных величин при работе с длинной арифметикой.

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
Тема 1. Введение в криптографию	Основные термины, определения и задачи криптографии. История криптографии. Криптографические методы защиты информации. Особенности симметричного и асимметричного шифрования.
Тема 2. Элементарные шифры	Шифр простой замены. Полибианский квадрат. Система шифрования Цезаря. Шифрующие таблицы Трисемуса. Биграммный шифр Плейфейра. Шифры перестановки. Шифрующие таблицы. Применение магических квадратов. Математические основы шифра одноалфавитной замены. Аффинная система подстановок Цезаря. Криптосистема Хилла. Шифр многоалфавитной замены. Шифрование гаммированием. Шифр «двойной квадрат».
Тема 3. Асимметричные шифры	Основные идеи. Система Диффи-Хеллмана. Элементы теории чисел. Алгоритм Евклида. Шифр Шамира. Шифр Эль-Гамала. Односторонняя функция с «лазейкой» и шифр RSA.
Тема 4. Электронная подпись	Цифровая подпись RSA. Электронная подпись на базе шифра Эль-Гамала. Стандарты на электронную подпись.
Тема 5. Взлом шифров	Метод «шаг младенца, шаг великана». Алгоритм исчисления порядка.
Тема 6 Криптографические протоколы	Понятие криптографического протокола. Ментальный покер. Электронные деньги. Взаимная идентификация с установлением ключа.
Тема 7. Эллиптические кривые	Математические основы. Операции над точками кривой. Выбор параметров кривой. Построение криптосистем на базе эллиптических кривых. Цифровая подпись по ГОСТ Р 34.10-2001. Определение количества точек на кривой.
Тема 8. Современные криптосистемы	Современные шифры с секретным ключом. Блочные шифры. Шифр ГОСТ 28147-89.

	Шифр Rijndael (AES). Сквозное шифрование. Особенности обеспечения безопасности данных в интернет. Сертификаты. Виды сертификатов.
--	---

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6.1. Форма обучения – очная, курс – 4, семестр – 7

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС	Всего
Тема 1. Введение в криптографию	4	4		6	14
Тема 2. Элементарные шифры	4	4		10	18
Тема 3. Асимметричные шифры	4	4		10	18
Тема 4. Электронная подпись	4	4		10	18
Тема 5. Взлом шифров	4	4		10	18
Тема 6 Криптографические протоколы	4	4		10	18
Тема 7. Эллиптические кривые	6	6		10	22
Тема 8. Современные криптосистемы	4	4		10	18
ПО КОМПОНЕНТУ ОПОП	34	34		76	144

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

7.1. Контрольные вопросы

1. Разновидности шифров перестановки.
2. Одноалфавитные и многоалфавитные замены.
3. Шифрование гаммированием.
4. Современные симметричные криптосистемы на примере AES
5. Криптосистема Диффи-Хеллмана
6. Шифр Шамира с обоснованием
7. Шифр Эль-Гамала с обоснованием
8. Шифр RSA с обоснованием
9. Метод «Шаг младенца – шаг великана» с обоснованием
10. Алгоритм исчисления порядка с обоснованием.
11. Подпись на основе RSA с обоснованием
12. Подпись на основе Эль-Гамала с обоснованием
13. ГОСТ на электронную подпись
14. Электронные деньги с обоснованием
15. Ментальный покер с обоснованием
16. Основы построения вычислений с помощью эллиптических кривых
17. Выбор параметров эллиптической кривой
18. Определение количества точек на кривой
19. Шифр Эль-Гамала на эллиптической кривой с обоснованием
20. Современные системы шифрования.

7.2. Пример индивидуального задания (тип задания)

Задание 1.1. Осуществить подпись сообщения со своей фамилией и именем в соответствии со следующими параметрами. Метод создания подписи определяется как $(p_1 \bmod 3)+1$, где p_1 – номер в списке, а список методов следующий:

1. RSA
2. Эль-Гамаль

3. ГОСТ на основе Эль-Гамала

В зависимости от вида подписи, взять параметры P – простое число, ближайшее к числу $(2 \cdot n) + 10$, а для Q – аналогичное определенное число $3 \cdot n + 5$. Индивидуальные параметры для подписи двух пользователей следует вычислить по формуле: $((i+1) \cdot n) \bmod 50 + 10$, где i – номер пользователя, n – номер варианта. Проверить, будет ли подтверждена подпись при изменении автора сообщения без изменения подписи.

Задание 1.2. Промоделировать расчет между собой 3х лиц в следующем порядке: первый человек снимает в банке сумму K в купюрах, указанных в таблице; после чего передает сумму L_1 первому пользователю, и L_2 второму пользователю, после чего те передают деньги в банк. Показать процедуру расчета и изменение состояния счетов в банке, если пользователь 2 принесет деньги раньше, чем пользователь 3. В качестве типа идентификации купюры использовать «слепую» подпись для купюр, где первая цифра соответствует номинации купюры. При этом в качестве параметров банка использовать P – простое число, ближайшее к числу $(2 \cdot n) + 10$, а для Q – аналогичное определенное число $3 \cdot n + 5$. Вариант определить по формуле $(m \bmod 10) + 1$, где m – номер в списке группы.

Задание 1.3. Осуществить проверку возможности использования эллиптической кривой с заданными параметрами. Определить точки эллиптической кривой путем перебора. Осуществить шифрование с помощью заданной эллиптической кривой, предварительно сформировав все необходимые данные для сети из 2х человек. Зашифровать и дешифровать инициалы (предварительно перевести их в число от 0 до $p-1$).

Задание 1.4. Дополнительное задание

Осуществить расчет количества точек эллиптической кривой.

Задание 2.1. Разработать алгоритмы, интерфейс и реализовать программное обеспечение, осуществляющее дешифрование текста путем взлома шифротекста, если заданы открытые параметры ключей. Замечание: где возможно, использовать ускоренные алгоритмы для получения необходимых остатков при умножении.

Задание 2.2. Реализовать механизм расчета с помощью «электронных денег». Требования: возможность заведения счета для пользователей и учета движения денег (т.е. хранится группа пользователей с параметрами и счетом наличных); для расчета используются купюры 2х номиналов (т.е. необходимо отдельно хранить данные о номерах купюр, где это необходимо). Предусмотреть возможности расчета с другими пользователями в качестве получателей.

7.3. Темы письменных работ (типы задач)

Контрольные работы по практике:

- простейшие алгоритмы с отображением всех шагов: алгоритм Евклида для НОД, обобщенный алгоритм Евклида для обратных величин, возведение в степень по ускоренному алгоритму;
- простейшие манипуляции на эллиптических кривых;
- простейшие симметричные/асимметричные шифры;
- криптографические протоколы.

Контрольная работа по проверке теоретических знаний – по всем темам, с использованием указанных выше контрольных вопросов.

8. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Общая оценка знаний обучающихся по дисциплине проводится по 100-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.), выполнение индивидуальных заданий.

8.1. Семестр 1

Номера разделов	Виды работ	Максимальное количество баллов
1	Организационно-учебная работа в аудитории	10
	Индивидуальные задания	60
	Модульный контроль	30
ИТОГО		100
Общий итог за семестр		100

Соответствие баллов оценке

Количество баллов из 100	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 Главном корпусе ДонГУ (г. Донецк, пр. Гурова, 6) и двенадцатом (г. Донецк, ул. Университетская, 24-а, УПВЦ). 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.505).

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. Вельшенбах, М. Криптография на Си и C++ в действии : [Учеб. пособие / М. Вельшенбах. - М. : Триумф, 2004. - 461 с. + 1 электрон. опт. диск (CD-ROM).
2. Осипян В. О. Криптография в задачах и упражнениях / В. О. Осипян, К. В. Осипян. - М. : Гелиос АРВ, 2004. - 144 с.
3. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: учебное пособие. – М.: Горячая линия – Телеком, 2005. – 229 с.

11.2. Дополнительная литература

4. 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 (1 файл).

12. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. **Национальная электронная библиотека (НЭБ):** федеральная государственная информационная система / Министерство Культуры РФ; Российская государственная библиотека. – Москва, 2019- . – URL: <https://rusneb.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный, подписка. Необходима установка программного обеспечения. – Текст: электронный.
2. **eLIBRARY.RU:** научная электронная библиотека: сайт. – Москва, 2000- . – URL: <https://elibrary.ru> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.
3. Научная электронная библиотека **«КиберЛенинка»:** сайт / Ассоциация «Открытая наука». – Москва, 2014- . – URL: <https://cyberleninka.ru/>. – Режим доступа: свободный. – Текст: электронный.
4. Электронно-библиотечная система **«Лань»:** [сайт]. – URL: <https://e.lanbook.com> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.
5. **ЭБС Юрайт:** электронная библиотечная система: сайт. – Москва, 2013. – URL: <https://biblio-online.ru> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.
6. **Электронно-библиотечная система ДонГУ:** сайт / ФГБОУ ВО «ДонГУ». – Донецк, 2016- . – URL: <http://library.donnu.ru/> (дата обращения: 01.09.2023). – 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: 01.09.2023). – 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: 01.09.2023). – Режим доступа: свободный.

13. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДОННУ № 46484614);
2. Microsoft Office (корпоративная лицензия ДОННУ лицензия № 46472919);
3. Microsoft Visual Studio (лицензия программы DreamSpark для высших учебных заведений);