

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ДонГТУ»)

Факультет информационных технологий и
автоматизации производственных процессов
Кафедра интеллектуальных систем и информационной безопасности



УТВЕРЖДАЮ
И.о. проректора
по учебной работе

Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Математика криптографии

(наименование дисциплины)

02.03.01 Математика и компьютерные науки

(код, наименование специальности)

Квалификация

бакалавр

(бакалавр/специалист/магистр)

Форма обучения

очная, очно-заочная

(очная, очно-заочная, заочная)

Алчевск, 2024

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целью изучения дисциплины «Математика криптографии» является получение базовых знаний математических основ криптографии и криптоанализа.

Задачи изучения дисциплины: формирование навыков использования методов криптографии в профессиональной деятельности для решения прикладных научно-технических задач; овладение знаниями о фундаментальных алгебро-геометрических основах построения криптосистем, о закономерностях создания, использования и анализа современных криптопротоколов, выработка умений применять полученные теоретические сведения для решения практических задач.

Дисциплина направлена на формирование общепрофессиональных (ОПК-1, ОПК-4) компетенций выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит в обязательную часть БЛОКА 1 «Дисциплины (модули)» подготовки студентов по специальности 02.03.01 «Математика и компьютерные науки».

Дисциплина реализуется кафедрой интеллектуальных систем и информационной безопасности. Основывается на базе дисциплин: «Высшая математика».

Является основой для изучения следующих дисциплин: «Научно-исследовательская работа».

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения общепрофессиональных задач деятельности, связанных с применением вычислительных систем в области информационной безопасности.

Курс является фундаментом для ориентации студентов в сфере разработки защищенных информационных систем.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 ак.ч. Программой дисциплины предусмотрены лекционные (18 ак.ч.), практические (36 ак.ч.) занятия, самостоятельная работа студента (54 ак.ч.).

Дисциплина изучается на 3 курсе в 5 семестре. Форма промежуточной аттестации – зачет.

3 Перечень результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины «Математика криптографии» направлен на формирование компетенции, представленной в таблице 1.

Таблица 1 – Компетенции, обязательные к освоению

Содержание компетенции	Код компетенции	Код и наименование индикатора достижения компетенции
Способен консультировать и использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в профессиональной деятельности	ОПК-1	ОПК-1.3 Имеет навыки выбора методов решения задач профессиональной деятельности на основе теоретических знаний
Способен находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем	ОПК-4	ОПК-4.2. Умеет использовать этот математический аппарат в профессиональной деятельности

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 3 зачётных единицы, 108 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к практическим занятиям, текущему контролю, выполнение индивидуального задания, самостоятельное изучение материала и подготовку к зачету.

При организации внеаудиторной самостоятельной работы по данной дисциплине используются формы и распределение бюджета времени на СРС для очной формы обучения в соответствии с таблицей 2.

Таблица 2 – Распределение бюджета времени на СРС

Вид учебной работы	Всего ак.ч.	Ак.ч. по семестрам
		5
Аудиторная работа, в том числе:	54	54
Лекции (Л)	18	18
Практические занятия (ПЗ)	36	36
Лабораторные работы (ЛР)	-	-
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	54	54
Подготовка к лекциям	4	4
Подготовка к лабораторным работам	-	-
Подготовка к практическим занятиям / семинарам	18	18
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	9	9
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	9	9
Работа в библиотеке	5	5
Подготовка к зачету	9	9
Промежуточная аттестация – зачет	3	3
Общая трудоемкость дисциплины		
ак.ч.	108	108
з.е.	3	3

5 Содержание дисциплины

С целью освоения компетенций, приведенных в п.3 дисциплина разбита на 3 темы:

- тема 1 (Линейные пространства над конечным полем);
- тема 2 (Применение простых чисел в криптографии);
- тема 3 (Дискретное логарифмирование и ПСП).

Виды занятий по дисциплине и распределение аудиторных часов для очной формы приведены в таблице 3.

Таблица 3 – Виды занятий по дисциплине и распределение аудиторных часов (очная форма обучения)

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудоемкость в ак.ч.	Темы практических занятий	Трудоемкость в ак.ч.	Тема лабораторных занятий	Трудоемкость в ак.ч.
1	2	3	4	5	6	7	8
1	Линейные пространства над конечным полем	Линейные пространства над конечным полем. Базис и размерность. Порождающая матрица. Расширенный алгоритм Евклида. Применение к многочленам над полем рациональных чисел и конечным полем. Конечные поля (поля Галуа). Расширение простого поля. Арифметика конечных полей. Нахождение обратного элемента поля.	6	Алгоритм Евклида, алгоритм Эратосфена Функция Эйлера. Подходящие дроби	6 6	—	—
2	Применение простых чисел в криптографии	Применение простых чисел в криптографии. Проверка чисел на простоту. Алгоритмы генерации простых чисел. Задача факторизации чисел. Алгоритмы факторизации.	6	Решение линейных сравнений первой степени Решение системы линейных сравнений 1 степени с помощью Китайской теоремы об остатках	6 6	—	—

Завершение таблицы 3

1	2	3	4	5	6	7	8
3	Дискретное логарифмирование и ПСП	Определение дискретного логарифма. Количество значений дискретного логарифма элемента поля. Алгоритмы дискретного логарифмирования. Определение ПСП. Методы генерации ПСП. Применение ПСП в криптографии.	6	Диофантовы уравнения Символ Якоби и Лежандра Решение квадратичных сравнений	4 4 4	—	—
Всего аудиторных часов		18		36		—	

6 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

6.1 Критерии оценивания

В соответствии с Положением о кредитно-модульной системе организации образовательного процесса ФГБОУ ВО «ДонГТУ» (https://www.dstu.education/images/structure/license_certificate/polog_kred_modul.pdf) при оценивании сформированности компетенций по дисциплине используется 100-балльная шкала.

Перечень работ по дисциплине и способы оценивания знаний приведены в таблице 4.

Таблица 4 – Перечень работ по дисциплине и способы оценивания знаний

Вид учебной работы	Способ оценивания	Количество баллов
Выполнение практических работ	Предоставление отчетов	48 - 80
Выполнение реферата	Предоставление отчета	12 - 20
Итого	—	60 - 100

Всего по текущей работе в семестре студент может набрать 100 баллов, в том числе:

- реферат – всего 20 баллов;
- практические работы – всего 80 баллов.

Оценка по зачету проставляется автоматически, если студент набрал в течении семестра не менее 60 баллов и отчитался за каждую контрольную точку. Минимальное количество баллов по каждому из видов текущей работы составляет 60% от максимального.

Зачет по дисциплине «Математика криптографии» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время сессии студент имеет право повысить итоговую оценку в форме устного собеседования по приведенным ниже вопросам.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 5.

Таблица 5 – Шкала оценивания знаний

Сумма баллов за все виды учебной деятельности	Оценка по национальной шкале зачёт/экзамен
0-59	Не зачтено/неудовлетворительно
60-73	Зачтено/удовлетворительно
74-89	Зачтено/хорошо
90-100	Зачтено/отлично

6.2 Домашнее задание

Домашнее задание не предусмотрено.

6.3 Темы для рефератов (презентаций) – индивидуальное задание

1. Теорема Кука
2. Основные NP-полные задачи
3. NP-полные задачи в теории кодирования
4. Задача об упаковке рюкзака
5. Методы вычисления дискретных логарифмов
6. Алгоритмы на эллиптических кривых
7. Простые числа и "основная" теорема арифметики.
8. Полная и приведенная системы вычетов.
9. Теорема Эйлера и теорема Ферма.
10. Алгоритм Евклида.
11. Бинарный алгоритм возведения в степень.
12. Китайская теорема об остатках.
13. Квадратичные вычеты
14. Метод пробных делений.
15. Критерий Вильсона.
16. Тест Лукаса.
17. Алгоритм Конягина-Померанса.
18. Детерминистические и вероятностные тесты на простоту.
19. Тест Соловея-Штрассена.
20. Тест Рабина-Миллера.
21. Построение больших простых чисел
22. Задача факторизации составного числа.
23. (P-1)-метод Полларда.
24. Ро-метод Полларда.
25. Факторизация чисел с помощью квадратичного решета.
26. Основные понятия теории сложности.
27. Детерминированные машины Тьюринга и класс задач P.

28. Недетерминированные алгоритмы и класс задач NP.
29. Полиномиальная сводимость и NP-полные задачи.
30. Методы теории сложности в криптографии.
31. Детерминистические тесты на простоту. Метод пробных делений.
Критерий Вильсона. Тест Лукаса. Алгоритм Конягина-Померанса.
32. Построение больших простых чисел
33. Бинарный алгоритм возведения в степень.
34. Китайская теорема об остатках.
35. Квадратичные вычеты
36. Основные требования к шифрам.
37. Совершенные шифры. Безусловно стойкие и практически стойкие шифры. Избыточность языка и расстояние единственности.
38. Переход от стандартного базиса конечного поля к нормальному.
39. Группа точек эллиптической кривой.
40. Тестирование неприводимости многочлена над конечным полем.
41. Алгоритмы умножения в конечном поле.
42. Быстрое возведение в степень в конечном поле.
43. Вероятностные алгоритмы проверки числа на простоту. Алгоритм Соловея - Штрассена. Алгоритм AKS (Агравала – Кайала – Сахены).
44. Построение алгоритмов проверки чисел на простоту.
45. Символы Лежандра. Алгоритм RSA. Символы Якоби. Закон взаимности.
46. Основы квантовой криптографии.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1 (Линейные пространства над конечным полем)

Базовые тесты (выбор одного из 4 вариантов)

1. Что такое конечное поле?
 - а) Множество всех действительных чисел.
 - б) Множество всех комплексных чисел.
 - с) Множество с конечным числом элементов, где определены операции сложения, вычитания, умножения и деления.
 - д) Множество всех целых чисел.
- Ответ: с)
2. Что такое базис линейного пространства?
 - а) Минимальное множество линейно независимых векторов, порождающих пространство.
 - б) Максимальное множество линейно зависимых векторов.

- с) Любое множество векторов.
- д) Множество всех векторов пространства.

Ответ: а)

3. Что такое порождающая матрица?

- а) Матрица, строки которой образуют базис линейного пространства.
- б) Матрица, столбцы которой образуют базис линейного пространства.
- с) Матрица, которая не имеет обратной.
- д) Матрица, состоящая из нулей.

Ответ: б)

4. Что делает расширенный алгоритм Евклида?

- а) Находит наибольший общий делитель двух чисел.
- б) Находит наименьшее общее кратное двух чисел.
- с) Решает системы линейных уравнений.
- д) Находит обратный элемент в поле.

Ответ: а)

Тесты повышенного уровня (вставить пропущенный термин)

1. Конечное поле F_q содержит $q = \underline{\hspace{2cm}}$ элементов.

Ответ: p^n , где p — простое число, n — натуральное число.

2. Базис линейного пространства — это минимальное множество $\underline{\hspace{2cm}}$ векторов, порождающих пространство.

Ответ: линейно независимых.

3. Расширенный алгоритм Евклида позволяет найти $\underline{\hspace{2cm}}$ двух чисел.

Ответ: наибольший общий делитель.

4. Для нахождения обратного элемента в поле F_p используется $\underline{\hspace{2cm}}$ алгоритм $\underline{\hspace{2cm}}$ Евклида.

Ответ: расширенный.

Тесты высокого уровня (написать формулу или определение)

1. Запишите формулу для нахождения обратного элемента a^{-1} в поле F_p с использованием расширенного алгоритма Евклида.

Ответ: $a * a^{-1} \equiv 1 \pmod{p}$.

2. Дайте определение линейного пространства над конечным полем.

Ответ: Линейное пространство над конечным полем F_q — это множество векторов, замкнутое относительно операций сложения и умножения на элементы поля, удовлетворяющее аксиомам линейного пространства.

3. Запишите формулу для нахождения НОД двух чисел a и b с использованием $\underline{\hspace{2cm}}$ алгоритма $\underline{\hspace{2cm}}$ Евклида.

Ответ: $\text{НОД}(a, b) = \text{НОД}(b, a \bmod b)$.

Запишите формулу для расширения простого поля F_p до поля F_{p^n} .

Ответ: $F_{p^n} = F_p[x] / (f(x))$, где $f(x)$ — неприводимый многочлен степени n над F_p .

Тема 2 (Применение простых чисел в криптографии)

Базовые тесты (выбор одного из 4 вариантов)

1. Какой алгоритм используется для проверки чисел на простоту?

- a) Алгоритм Евклида.
- b) Тест Миллера-Рабина.
- c) Алгоритм Флойда.
- d) Алгоритм Дейкстры.

Ответ: b)

2. Что такое задача факторизации?

- a) Нахождение наибольшего общего делителя двух чисел.
- b) Разложение числа на простые множители.
- c) Нахождение обратного элемента в поле.
- d) Решение системы линейных уравнений.

Ответ: b)

3. Какой алгоритм используется для генерации больших простых чисел?

- a) Алгоритм Евклида.
- b) Решето Эратосфена.
- c) Алгоритм Диффи-Хеллмана.
- d) Алгоритм RSA.

Ответ: b)

4. Что такое дискретный логарифм?

- a) Логарифм от действительного числа.
- b) Логарифм от комплексного числа.
- c) Логарифм в конечном поле или группе.
- d) Логарифм от матрицы.

Ответ: c)

Тесты повышенного уровня (вставить пропущенный термин)

1. Алгоритм _____ используется для проверки чисел на простоту.

Ответ: Миллера-Рабина.

2. Задача _____ заключается в разложении числа на простые множители.

Ответ: факторизации.

3. Дискретный логарифм элемента $g^x \equiv h \pmod{p}$ — это _____.

Ответ: x .

4. Алгоритм _____ используется для генерации больших простых чисел.

Ответ: решето Эратосфена.

Тесты высокого уровня (написать формулу или определение)

1. Запишите формулу для задачи дискретного логарифмирования в группе Z_p^* .

Ответ: $g^x \equiv h \pmod{p}$, где g — образующий элемент, h — элемент группы, x — искомый дискретный логарифм.

2. Дайте определение простого числа.

Ответ: Простое число — это натуральное число, большее 1, которое делится только на 1 и на само себя.

3. Запишите формулу для нахождения НОД двух чисел a и b с использованием алгоритма Евклида.

Ответ: $\text{НОД}(a, b) = \text{НОД}(b, a \bmod b)$.

Запишите формулу для расширения простого поля F_p до поля F_{p^n} .

Ответ: $F_{p^n} = F_p[x] / (f(x))$, где $f(x)$ — неприводимый многочлен степени n над F_p .

Тема 3 (Дискретное логарифмирование и ПСП)

Базовые тесты (выбор одного из 4 вариантов)

1. Что такое псевдослучайная последовательность (ПСП)?

а) Последовательность, которая полностью случайна.

б) Последовательность, которая выглядит случайной, но генерируется детерминированно.

с) Последовательность, которая всегда повторяется.

д) Последовательность, которая не используется в криптографии.

Ответ: б)

2. Какой алгоритм используется для генерации ПСП?

а) Алгоритм Евклида.

б) Линейный регистр сдвига (LFSR).

с) Алгоритм Диффи-Хеллмана.

д) Алгоритм RSA.

Ответ: б)

3. Что такое дискретный логарифм?

а) Логарифм от действительного числа.

б) Логарифм от комплексного числа.

с) Логарифм в конечном поле или группе.

д) Логарифм от матрицы.

Ответ: с)

4. Какой алгоритм используется для решения задачи дискретного логарифмирования?

- a) Алгоритм Евклида.
- b) Алгоритм "гигантских шагов — малых шагов".
- c) Алгоритм Флойда.
- d) Алгоритм Дейкстры.

Ответ: b)

Тесты повышенного уровня (вставить пропущенный термин)

1. Псевдослучайная последовательность генерируется с использованием _____ регистра сдвига.

Ответ: линейного.

2. Задача _____ заключается в нахождении показателя степени x в уравнении $g^x \equiv h \pmod{p}$.

Ответ: дискретного логарифмирования.

3. Алгоритм _____ используется для решения задачи дискретного логарифмирования.

Ответ: "гигантских шагов — малых шагов".

4. Псевдослучайные последовательности используются в _____ шифрах.

Ответ: потоковых.

Тесты высокого уровня (написать формулу или определение)

1. Запишите формулу для генерации псевдослучайной последовательности с использованием линейного регистра сдвига (LFSR).

Ответ: $s_n = c_1 * s_{n-1} + c_2 * s_{n-2} + \dots + c_k * s_{n-k}$, где c_i — коэффициенты, s_i — биты последовательности.

2. Дайте определение псевдослучайной последовательности.

Ответ: Псевдослучайная последовательность — это последовательность чисел, которая выглядит случайной, но генерируется детерминированным алгоритмом.

3. Запишите формулу для задачи дискретного логарифмирования в группе Z_p^* .

Ответ: $g^x \equiv h \pmod{p}$, где g — образующий элемент, h — элемент группы, x — искомый дискретный логарифм.

4. Запишите формулу для нахождения обратного элемента a^{-1} в поле F_p с использованием расширенного алгоритма Евклида.

Ответ: $a * a^{-1} \equiv 1 \pmod{p}$.

6.5 Вопросы для подготовки к зачету

- 1) Что такое определение линейного пространства (ЛП) над полем. Примеры линейных пространств?
- 2) Что такое определение линейной комбинации векторов ЛП. Линейно зависимые и линейно независимые системы векторов?
- 3) Что такое определение базиса и размерности ЛП. Разложение вектора по базису. Число базисных векторов и количество базисов в L_n ?
- 4) Что такое выражение результатов линейных операций над векторами в базисе?
- 5) Какие Вы знаете основные теоремы о базисе? Что такое канонический базис?
- 6) Что такое переход от одного базиса к другому? Что такое матрица перехода?
- 7) Как осуществляется нахождение базиса системы векторов?
- 8) Что такое определение линейного подпространства? Какова его размерность? Примеры линейных подпространств.
- 9) Что такое линейная оболочка системы векторов как подпространство? Каковы его базис и размерность?
- 10) Что такое изоморфизм линейных подпространств?
- 11) Как осуществляется решение системы линейных однородных уравнений? Что такое общее решение системы?
- 12) Что такое пространства со скалярным произведением? Какова геометрия пространства?
- 13) Что такое ортогональные и ортонормированные системы векторов?
- 14) Что такое ортогональный и ортонормированный базис?
- 15) Как осуществляется выражение скалярного произведения: в базисе; в ортонормированном базисе?
- 16) Что такое процесс ортогонализации Грамма-Шмидта?
- 17) Что такое ортогональное дополнение к линейному подпространству евклидова пространства?
- 18) Что такое Линейное пространство над конечным полем X . Что такое пространство $Q=X^n$; его размерность и мощность?
- 19) Подпространства пространства Q . Порождающая и проверочная матрицы. Их канонические формы?
- 20) Как осуществляется алгоритм быстрого возведения в степень?
- 21) Каковы определение и свойства функции Эйлера?
- 22) Что такое приведенная система вычетов?
- 23) Как формулируется теорема Ферма и Эйлера? Каково их применение?

24) Какие Вы знаете различные формы расширенного алгоритма Евклида в кольце целых чисел?

25) Что такое расширенный алгоритм Евклида в кольце $\mathbb{Z}_n$. Как осуществляется вычисление обратного элемента?

26) Что такое Расширенный алгоритм Евклида для многочленов: над полем рациональных чисел; над конечным полем $\mathbb{Z}_p$?

27) Каково общее определение конечного поля (поля Галуа). Что такое простые поля?

28) Каковы алгебраические свойства конечных полей?

29) Что такое определение примитивного элемента конечного поля? Какова теорема его существования?

30) Что такое характер конечного поля? Что такое числа поля? Что такое степень суммы элементов поля?

31) Какова основная теорема теории конечных полей? Что такое количество элементов поля?

32) Как осуществляется расширение полей с помощью неприводимого многочлена?

33) Что такое примитивный элемент и примитивный многочлен поля $\text{GF}(pm)$?

34) Что такое структура конечного поля?

35) Какова арифметика конечного поля? Как осуществляются операция умножения? Процедура x^{time} ?

36) Какова структура полей: $\text{GF}(p^2)$; $\text{GF}(pm)$?

37) Что такое количество простых чисел? Что такое неравенство Чебышева? Что такое числа Ферма? Что такое числа Мерсенны?

38) Что такое детерминированные и вероятностные тесты проверки чисел на простоту?

39) Как формулируется критерий Вильсона? Как формулируется полиномиальный тест?

40) Как формулируется тест Ферма? Что такое псевдопростые числа? Что такое числа Кармайкла?

41) Как осуществляется тест «испытание квадратным корнем»?

42) Каковы различные варианты теста Миллера-Рабина? Что такое алгоритмы генерации простых чисел с заданной разрядностью?

43) Что такое теорема Поклингтона и каково ее применение для генерации простых чисел?

44) Что такое алгоритм Маурера генерации простых чисел?

45) Что такое задача факторизации чисел? Что такое метод пробных делений?

- 46) Что такое алгоритм вычисления $[\square n]$?
- 47) Что такое метод Ферма факторизации чисел?
- 48) Что такое ρ -метод Полларда факторизации чисел?
- 49) Что такое $(\rho-1)$ – метод Полларда факторизации чисел?
- 50) Каково определение дискретного логарифма в циклической мультипликативной группе? Каково условие его существования? Случай неединственности?
- 51) Что такое ρ -метод Полларда вычисления дискретного логарифма?
- 52) Как осуществляется вычисление дискретного логарифма с помощью КТО (Метод Нечаева)?
- 53) Как осуществляется алгоритм «baby-step»?
- 54) Что такое шифр Вернама?
- 55) Что такое генераторы псевдослучайных чисел (ПСЧ)?
- 56) Что такое алгоритм RC4?
- 57) Что такое алгоритм RSA? Генератор ПСЧ на основе RSA?
- 58) Что такое датчики М-последовательностей?
- 59) Что такое тест «стопка книг»?

6.6 Тематика и содержание курсового проекта

Курсовой проект не предусмотрен.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Де́за Е. И. Введение в криптографию: Теоретико-числовые основы защиты информации. Учебное пособие. Изд. стереотип. — М.: ЛЕНАНД, 2022. — 376 с. — Режим доступа: <https://coollib.cc/b/616620-elena-ivanovna-deza-vvedenie-v-kriptografiyu-teoretiko-chislovyie-osnovyi-zaschityi-informatsii>. (Дата обращения 26.08.2024).
2. Мартынов Л. М. Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. — Санкт-Петербург : Лань, 2020. — 456 с. : ил. — Режим доступа: https://www.researchgate.net/profile/Leonid-Martynov/publication/343787756_Algebra_and_Number_Theory_for_Cryptography_in_Russian/links/61813c85a767a03c14e56287/Algebra-and-Number-Theory-for-Cryptography-in-Russian.pdf. (Дата обращения 26.08.2024).
3. Рацеев С.М. Математические методы защиты информации [Электронный ресурс]: Электронное учеб. пособие/ С.М. Рацеев. Ульяновск: УлГУ, 2018. 1 CD-R. № гос. регистрации – 0321901084. [Электронный ресурс] — Режим доступа: https://www.ulsu.ru/media/documents/Рацеев_С.М._Математические_методы_защиты_информации.pdf. (Дата обращения: 26.08.2024).

Дополнительная литература

1. Математические основы криптографии : тексты лекций для студентов специальности 1-98 01 03 «Программное обеспечение информационной безопасности мобильных систем» / авт.-сост. Е. И. Ловенецкая. — Минск: БГТУ, 2019. — 171 с. [Электронный ресурс]: Режим доступа: https://elib.belstu.by/bitstream/123456789/31285/1/Loveneckaja_matematicheskie_osnovy_kriptografii.pdf?ysclid=m7i2jvcq4d411197836. (Дата обращения: 26.08.2024).

Учебно-методические материалы и пособия

1. Закутный А.С. Математика криптографии: методические указания к лабораторно-практическим работам [Электронный ресурс] — URL: <https://3kl.dontu.ru/course/>. Режим доступа: для авториз. пользователей. — Текст: электронный. (Дата обращения 26.08.2024).

7.2 Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Научная библиотека ДонГТУ : официальный сайт.— Алчевск. —URL: library.dstu.education.— Текст : электронный.
2. Научно-техническая библиотека БГТУ им. Шухова : официальный сайт. — Белгород. — URL: <http://ntb.bstu.ru/jirbis2/> .— Текст : электронный.
3. Консультант студента : электронно-библиотечная система.— Москва. — URL: <http://www.studentlibrary.ru/cgi-bin/mb4x> .— Текст : электронный.
4. Университетская библиотека онлайн: электронно-библиотечная система. — URL: http://biblioclub.ru/index.php?page=main_ub_red .— Текст : электронный.
5. IPR BOOKS : электронно-библиотечная система.—Красногорск. — URL: <http://www.iprbookshop.ru/> . —Текст : электронный.
6. Сайт кафедры ИСИБ <http://scs.dstu.education> .

Материально-техническое обеспечение представлено в таблице 6.

Таблица 6 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: <i>Мультимедийная аудитория. (60 посадочных мест), оборудованная специализированной (учебной) мебелью (парта трехместная – 18 шт., парта двухместная – 6 шт, стол– 1 шт., доска аудиторная– 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран.</i> <i>Компьютерные классы (22 посадочных места), оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС:</i>	ауд. <u>207</u> корп. <u>4</u> ауд. <u>217</u> корп. <u>3</u> ауд. <u>211</u> корп. <u>4</u>

Лист согласования РПД

Разработал:

ст. преподаватель кафедры
интеллектуальных систем и
информационной безопасности
(должность)


(подпись)

А.С. Закутный
(Ф.И.О.)

И.о. заведующего кафедрой
интеллектуальных систем и
информационной безопасности
(наименование кафедры)


(подпись)

Е.Е. Бизянов
(Ф.И.О.)

Протокол № 1 заседания кафедрыот 27.08. 2024г.

И.о. декана факультета
(наименование факультета)


(подпись)

В.В. Дьячкова
(Ф.И.О.)

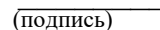
Согласовано

Председатель методической
комиссии по специальности
02.03.01 Математика и компьютерные
науки


(подпись)

Н.Н. Лепило
(Ф.И.О.)

Начальник учебно-методического центра


(подпись)

О.А. Коваленко
(Ф.И.О.)

Лист изменений и дополнений

Номер изменения, дата внесения изменения, номер страницы для внесения изменений	
ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:	ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:
Основание:	
Подпись лица, ответственного за внесение изменений	