МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Костромской государственный университет»

(КГУ)


УТВЕРЖДЕНО:

На заседании кафедры защиты информации

Протокол заседания № 10 от 15 мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

# МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Направленность/специализация: Организация и технология защиты информации

Квалификация выпускника: Бакалавр

**Кострома**
**2023**

Рабочая программа дисциплины «Математические основы криптологии» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность.
Приказ Минобрнауки России от 17.11.2020 № 1427.

Разработал: Чередникова Алла Викторовна, доцент кафедры защиты информации, к.ф.-м.н., доцент

Рецензенты: Виноградова Г.Л., доцент кафедры защиты информации КГУ, к.т.н., доцент

## 1. Цели и задачи освоения дисциплины

Цели дисциплины:

− обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность»;
− изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи дисциплины:

дать основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; принципов синтеза и анализа шифров; математических методов, используемых на практике.

## 2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

освоить компетенцию:

**ОПК-9** (способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности).

Код и содержание индикаторов компетенции:

Знать:

− принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
− принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах;

Уметь:

− устанавливать, настраивать и обслуживать программно-аппаратные средства защиты информации;
− применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищённости компьютерных систем;

Владеть:

− научно-технической терминологией;
− методами и средствами выявления угроз безопасности автоматизированным системам;
− методами организации проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации.

## 3. Место дисциплины в структуре ОП ВО

Дисциплина относится к обязательной части учебного плана. Изучается в пятом семестре обучения.

Изучение дисциплины основывается на ранее освоенных дисциплинах/практиках: «Основы информационной безопасности», «Дискретная математика», «Теория информации и кодирования», «Теория вероятностей и математическая статистика», «Линейная алгебра», «Математический анализ», «Дополнительные главы высшей математики», «Математические основы криптологии». Базируются на изучении данной дисциплины «Комплексные система зашиты информации на предприятии», «Организация и управление службой защиты информации на предприятии».

## 4. Объем дисциплины

### 4.1. Объем дисциплины в зачетных единицах с указанием академических часов и виды учебной работы

| Виды учебной работы, | Очная форма |
|---|---|
| Общая трудоемкость в зачетных единицах | 5 |
| Общая трудоемкость в часах | 180 |
| Аудиторные занятия в часах, в том числе: | 68 |
| Лекции | 34 |
| Практические занятия | – |
| Лабораторные занятия | 34 |
| Практическая подготовка | – |
| ИКР | 5,35 |
| Самостоятельная работа в часах | 70,65 |
| Форма промежуточной аттестации | Экзамен 36 |

### 4.2. Объем контактной работы на 1 обучающегося

| Виды учебных занятий | Очная форма |
|---|---|
| Лекции | 34 |
| Практические занятия | – |
| Лабораторные занятий | 34 |
| Консультации | 2 |
| Зачет/зачеты | – |
| Экзамен/экзамены | 0,35 |
| Курсовые работы | 3 |
| Курсовые проекты | – |
| Практическая подготовка | – |
| **Всего** | 73,35 |

## 5. Содержание дисциплины, структурированное по темам (разделам), с указанием количества часов и видов занятий

## 5.1 Тематический план учебной дисциплины

| № | Название раздела, темы | Всего з.е./час | Аудиторные занятия | | Самост. работа |
|---|---|---|---|---|---|
| | | | Лекц. | Лаб. | |
| 1 | **Раздел 1.** История криптографии. Классические шифры | **20,65** | **4** | **6** | **10,65** |
| 1.1 | Основные понятия и определения криптографии. Шифры замены и перестановки. Классические шифры перестановки. Блочные и потоковые шифры. Шифры простой замены. Шифры сложной замены | 13,65 | 2 | 6 | 5,65 |
| 1.2 | Шифры гаммирования и колонной замены. Шифровальные машины | 7 | 2 | – | 5 |
| 2 | **Раздел 2.** Современные системы симметричной криптографии | **60** | **10** | **10** | **40** |
| 2.1 | Основы теории Шеннона и её развитие | 6 | 2 | – | 4 |
| 2.2 | Композиции шифров | 8 | 2 | 2 | 4 |
| 2.3 | Алгоритм шифрования DES. Режимы работы блочных шифров | 10 | 2 | 2 | 6 |
| 2.4 | Алгоритм ГОСТ 28147-89 и шифр «Магма» (ГОСТ Р 34.12-2015). Вычислительная стойкость алгоритмов. Атаки на алгоритмы шифрования. Методы криптоанализа блочных шифров. Требования, предъявляемые к современным блочным алгоритмам шифрования | 14 | 2 | 2 | 10 |
| 2.10 | Шифр AES | 8 | 2 | 2 | 4 |
| 2.11 | Шифр «Кузнечик» (ГОСТ Р 34.12-2015) и режимы работы блочных шифров (ГОСТ Р 34.13-2015). Имитостойкость и помехоустойчивость шифров. Управление криптографическими ключами. Построение сетей засекреченной связи | 14 | – | 2 | 12 |
| 3 | **Раздел 3.** Криптография с открытым ключом | **42** | **16** | **16** | **10** |
| 3.1 | Симметричные и асимметричные шифры. Криптосистема Диффи-Хеллмана. Шифр Шамира. | 8 | 2 | 2 | 2 |
| 3.4 | Шифр Эль-Гамаля | 4 | 2 | 2 | – |
| 3.5 | Шифр RSA | 4 | 2 | 2 | – |
| 3.6 | Вероятностное шифрование. Система Блюма-Гольдвассер | 4 | 2 | 2 | – |
| 3.7 | Функции хеширования | 6 | 2 | 2 | 2 |
| 3.8 | Цифровая подпись | 6 | 2 | 4 | – |
| 3.9 | Криптографические протоколы | 4 | 2 | – | 2 |
| 3.10 | Создание скрытого канала. Практическое применение систем | 6 | 2 | – | 4 |
| 4 | **Раздел 4.** Перспективные направления криптографии | **18** | **4** | **4** | **10** |
| 4.1 | Криптография на эллиптических кривых | 11 | 2 | 4 | 5 |
| 5 | Квантовая криптография | **7** | 2 | – | 5 |
| | ИКР | 5,25 | – | – | – |
| | Итого: | **5/180** | **34** | **34** | **70,65** |

## 5.2. Содержание:

**Раздел 1. История криптографии. Классические шифры.** Основные понятия и определения криптографии. Шифры замены и перестановки. Классические шифры перестановки. Блочные и потоковые шифры. Шифры простой замены. Шифры сложной замены. Шифры гаммирования и колонной замены. Шифровальные машины.

**Раздел 2. Современные системы симметричной криптографии.** Основы теории Шеннона и её развитие. Композиции шифров. Алгоритм шифрования DES. Режимы работы блочных шифров. Алгоритм ГОСТ 28147-89 и шифр «Магма» (ГОСТ Р 34.12-2015). Вычислительная стойкость алгоритмов. Атаки на алгоритмы шифрования. Методы криптоанализа блочных шифров. Требования, предъявляемые к современным блочным алгоритмам шифрования. Шифр AES. Шифр «Кузнечик» (ГОСТ Р 34.12-2015) и режимы работы блочных шифров (ГОСТ Р 34.13-2015). Имитостойкость и помехоустойчивость шифров. Управление криптографическими ключами. Построение сетей засекреченной связи.

**Раздел 3. Криптография с открытым ключом.** Симметричные и асимметричные шифры. Криптосистема Диффи-Хеллмана. Шифр Шамира. Шифр Эль-Гамаля. Шифр RSA. Вероятностное шифрование. Система Блюма-Гольдвассер. Функции хеширования. Цифровая подпись. Криптографические протоколы. Создание скрытого канала. Практическое применение систем.

**Раздел 4. Перспективные направления криптографии.** Криптография на эллиптических кривых. Квантовая криптография.

# 6. Методические материалы для обучающихся по освоению дисциплины

## 6.1. Самостоятельная работа обучающихся по дисциплине (модулю)

| № п/п | Раздел (тема) дисциплины | Задание | Часы | Методические рекомендации по выполнению задания *(Литература)* | Форма контроля |
|---|---|---|---|---|---|
| 1. | Раздел 1. История криптографии. Классические шифры | Изучение теоретического материала лекций и лабораторных работ. Выполнение заданий к лабораторным работам | 10,65 | Лекционный материал, [1–3] | Тестирование по разделу в СДО<br>Проверка выполнения заданий к лабораторным работам и защита<br>Экзамен |
| 2. | Раздел 2. Современные системы симметричной криптографии | Изучение теоретического материала лекций и лабораторных работ. Выполнение заданий к лабораторным работам | 40 | Лекционный материал, [1–3] | Тестирование по разделу в СДО<br>Проверка выполнения заданий к лабораторным работам и |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | защита<br>Экзамен |
| 3. | Раздел 3. Криптография с открытым ключом | Изучение теоретического материала лекций и лабораторных работ. Выполнение заданий к лабораторным работам | 10 | Лекционный материал, [1–3] | Тестирование по разделу в СДО<br>Проверка выполнения заданий к лабораторным работам и защита<br>Экзамен |
| 4. | Раздел 4. Перспективные направления криптографии | Изучение теоретического материала лекций и лабораторных работ. Выполнение заданий к лабораторным работам | 10 | Лекционный материал, [1–3] | Тестирование по разделу в СДО<br>Проверка выполнения заданий к лабораторным работам и защита<br>Экзамен |

## 6.2. Тематика и задания для практических занятий

*Практические занятия не предусмотрены.*

## 6.3. Тематика лабораторных занятий

1. Изучение классических шифров замены.
2. Криптоанализ шифров табличной перестановки.
3. Генерация псевдослучайных чисел.
4. Схема Фейстеля.
5. Алгоритм шифрования DES.
6. Слайдовая атака.
7. Алгоритм шифрования AES.
8. Криптосистема Диффи-Хеллмана. Шифр Шамира.
9. Криптосистема Эль-Гамаля.
10. Изучение криптосистемы RSA.
11. Вероятностное шифрование. Система Блюма-Гольдвассер.
12. Функции хеширования.
13. Цифровая подпись.
14. Выполнение операций с точками на эллиптической кривой.
15. Изучение криптосистем на эллиптических кривых.

По каждой лабораторной работе студентам выдаются задания для самостоятельной работы, которые затем проверяются преподавателем и защищаются студентами в форме устного

собеседования. Формой промежуточной аттестации по данной дисциплине является экзамен. Необходимые условия допуска к экзамену:

- прохождение тестов по всем разделам с положительным результатом;
- сдача всех лабораторных работ с положительным результатом.

## 6.4. Тематика курсовых работ

1. Криптоанализ шифра Виженера.
2. Шифр Хилла. Криптоанализ шифра.
3. Аффинные криптосистемы. Криптоанализ аффинных криптосистем.
4. Шифрующие матрицы. Криптоанализ аффинных матричных криптосистем.
5. Задача дискретного логарифмирования. Нахождение дискретного логарифма методами перебора и согласования.
6. Вероятностные тесты простоты. Тесты Соловея-Штрассена и Миллера-Рабина.
7. Алгоритм быстрого возведения в степень. Метод Монтгомери.
8. Генерация больших простых чисел.
9. Современные методы факторизации. Метод Полларда-Флойда. (P – 1)-метод Полларда.
10. Факторизация натуральных чисел методом Лежандра.
11. Факторизация натуральных чисел методом цепных дробей Бриллхарта-Моррисона.
12. Факторизация натуральных чисел методом квадратичного решета.
13. Электронная цифровая подпись DSA.
14. Криптосистема Рабина. Электронная цифровая подпись Рабина с извлечением сообщения.
15. Рюкзачная схема шифрования Меркле-Хеллмана.
16. Рюкзачная схема шифрования Хора-Ривеста.
17. Вероятностная схема шифрования Голдвассер-Микали.
18. Электронная цифровая подпись Фейге-Фиат-Шамира.
19. Электронная цифровая подпись GQ.
20. Алгоритмы хеширования SHA-2.

## 7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

| № п/п | Литература | Кол-во книг |
|---|---|---|
| | *Основная* | |
| 1 | Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с.: ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429092 | ЭБ |
| 2 | Криптографические методы защиты информации. Том 3: Учебно-методическое по-собие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с.: 60x88 1/8. - (Высшее образование: Бакалавриат). (обложка) ISBN 978-5-369-01304-5, 200 экз. http://znanium.com/catalog.php?bookinfo=432654 | ЭБ |

| | | |
|---|---|---|
| 3 | Кнауб, Л.В. Теоретико-численные методы в криптографии : учебное пособие / Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов ; Министерство образования и науки Рос-сийской Федерации, Сибирский Федеральный университет. - Красноярск : Сибир-ский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=229582 | ЭБ |
| *Дополнительная* | | |
| 4 | Моделирование системы защиты информации. Практикум: учеб. пособие / Е.К. Баранова, А.В. Бабаш. — 2-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2018. — 224 с. + Доп. материалы [Электронный ресурс; Режим доступа http: //www.znanium.com]. — (Высшее образование: Бакалавриат). — DOI: https://doi.org/10.12737/18877 http://znanium.com/catalog.php?bookinfo=916068 | ЭБ |
| 5 | Поддержка принятия решений при проектировании систем защиты информации: монография / В.В. Бухтояров, М.Н. Жукова, В.В. Золотарев [и др.]. — М.: ИН-ФРА-М, 2018. – 311 с. – (Научная мысль) http://znanium.com/catalog.php?bookinfo=947806 | ЭБ |
| 6 | Актуальные вопросы защиты информации: монография / А.В. Бабаш, Е.К. Барано-ва. — М.: РИОР: ИНФРА-М, 2017. — 111 с. — (Научная мысль). — http://znanium.com/catalog.php?bookinfo=854634 | ЭБ |
| 7 | Криптографические методы защиты информации : лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет» ; авт.-сост. И.А. Калмыков, Д.О. Науменко и др. - Ставрополь : СКФУ, 2015. - 109 с.: ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458059 | ЭБ |
| 8 | Разработка моделей криптографической защиты информации: монография / В.Г. Шубович, В.В. Капитанчук, Н.С. Знаенко, Ю.И. Титаренко ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Ульяновский государственный педагогический университет имени И.Н. Ульянова». - Ульяновск: Ул-ГПУ, 2013. - 128 с.: схем. - Библиогр.: с. 108-112. - ISBN 978-5-86045-640-2; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=278070 | ЭБ |
| 9 | Ниссенбаум, О. В. Теоретико-числовые методы в криптографии. Сборник заданий (часть III): учебно-методическое пособие / О. В. Ниссенбаум. — Тюмень: ТюмГУ, 2014. — 40 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/110138 (дата обращения: 16.06.2021). — Режим доступа: для авториз. пользователей. | ЭБ |

## 8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Информация о курсе дисциплины в СДО:
Элемент «Лекции»*;*
Элемент «Лабораторные занятия»*;*

Элемент «Самостоятельная работа»;
Элемент «Тест»;
Элемент «Список рекомендуемой литературы»;
Элемент «Промежуточная аттестация».
Используются следующие элементы и ресурсы СДО: форум «Объявления»; «Страница»; «Задание»; «Лекция»; «Тест»; «Гиперссылка»; «Пояснение»; «Папка»; «Файл»; блоки «Последние объявления», «Календарь», «Проверь меня!», «Пользователи на сайте», «Статистика».

*Электронные библиотечные системы:*

1. ЭБС Университетская библиотека онлайн – http://biblioclub.ru
2. ЭБС «Лань» – https://e.lanbook.com
3. ЭБС «Znanium» – https://znanium.com

## 9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия проводятся в аудиториях с требуемым числом посадочных мест, оборудованные мультимедиа.

Лабораторные занятия проводятся в компьютерных классах с выходом в интернет.

Лицензионное программное обеспечение:

MS Excel

Свободно распространяемое программное обеспечение:

Cryptool 2 https://www.cryptool.org/en/

Офисный пакет