МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению практических работ
по дисциплине
«МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»
для студентов направления подготовки 02.04.01 Математика и компьютерные науки
профиль «Искусственный интеллект в кибербезопасности»

Ставрополь
2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Методы и средства криптографической защиты информации» является формирование у будущего специалиста по направлению подготовки 02.04.01 Математика и компьютерные науки профиль «Искусственный интеллект в кибербезопасности» глубоких знаний о криптографических методах и средствах защиты информации.
Задачи дисциплины:

- Формирование понятий и методов криптографии: Ознакомление с историческими и современными криптосистемами, их принципами и математическими основами.
- Изучение криптоалгоритмов: Изучение симметричных и асимметричных шифров, криптографических функций хеширования и электронной цифровой подписи.
- Анализ криптостойкости: Изучение методов криптоанализа и оценка безопасности различных криптографических алгоритмов.
- Практические навыки: Развитие умения применять криптографические алгоритмы в компьютерных системах и реализовывать их на языках программирования.
- Системный подход: Формирование навыков выбора и применения криптографических методов для решения задач информационной безопасности.

Перечень осваиваемых компетенций:

Код	Формулировка
ОПК-3	Способен самостоятельно создавать прикладные программные средства на основе современных информационных технологий и сетевых ресурсов, в том числе отечественного производства

Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы высшего образования

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
ОПК-3 Способен самостоятельно создавать прикладные программные средства на основе современных информационных	**ИД-1** Самостоятельно создает прикладные программные продукты	Разрабатывает прикладные программные продукты с использованием современных информационных

технологий и сетевых ресурсов, в том числе отечественного производства		технологий и сетевых ресурсов, включая отечественные решения; применяет методы проектирования, тестирования и оптимизации программного обеспечения; использует инструменты автоматизации разработки и средства контроля версий для обеспечения качества и эффективности создаваемых программных решений.
	ИД-2 Знает и умеет находить современные информационные технологии, в том числе и отечественного производства, необходимые для создания прикладных программных продуктов	Осуществляет поиск и анализ современных информационных технологий и сетевых ресурсов, включая отечественные разработки, для создания прикладных программных продуктов; оценивает их применимость к поставленным задачам; использует эффективные методы интеграции и адаптации технологий в процессе разработки программного обеспечения.

СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Практическое занятие 1. Модели шифров.

Цель работы: освоить модели шифров и их реализацию на практике, а также оценить эффективность различных криптографических методов.

Задание 1: Математическая модель шифра замены

1. **Разработка модели шифра замены:**
   - Создайте простую модель шифра замены, где каждый символ открытого текста заменяется на другой символ по заданному правилу (например, сдвиг на 3 позиции в алфавите).
   - Напишите программу на Python для реализации шифрования и расшифрования текста с помощью этой модели.
2. **Анализ безопасности:**
   - Оцените безопасность шифра замены с ограниченным ключом. Какие атаки могут быть применены для взлома шифра?

Задание 2: Модель шифра перестановки

1. **Разработка модели шифра перестановки:**
   - Создайте модель шифра перестановки, где символы открытого текста переставляются по заданному шаблону (например, перестановка по столбцам).
   - Напишите программу на Python для реализации шифрования и расшифрования текста с помощью этой модели.
2. **Анализ безопасности:**
   - Оцените безопасность шифра перестановки. Какие методы могут быть использованы для взлома шифра?

Задание 3: Линейный криптоанализ

1. **Анализ S-блоков:**
   - Выберите простой криптографический алгоритм (например, DES) и проанализируйте его S-блоки.
   - Создайте таблицы линейных статистических аналогов для S-блоков.
2. **Эффективный линейный статистический аналог:**
   - Определите эффективный линейный статистический аналог для выбранного алгоритма.
   - Оцените вероятность успешной атаки с помощью этого аналога.

Задание 4: Реализация режима однократного гаммирования

1. **Разработка приложения:**
   - Создайте приложение для шифрования и расшифрования текста в режиме однократного гаммирования.
   - Позвольте пользователю просматривать и изменять ключ, шифруемый и зашифрованный тексты в двоичном, шестнадцатеричном и символьном виде.
2. **Исследование свойств скремблера:**
   - Исследуйте свойства генерируемой последовательности псевдослучайных чисел при различных начальных значениях скремблера.
   - Оцените равномерность, сбалансированность и корреляцию

последовательности.

Вопросы для обсуждения

- Какие преимущества и недостатки имеют различные модели шифров?
- Как можно улучшить безопасность шифров замены и перестановки?
- Какие методы линейного криптоанализа наиболее эффективны для взлома современных шифров?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 2. Алгоритм шифрования таблицей Виженера.

Цель: освоить принципы многоалфавитной замены, реализовать шифр Виженера программно, провести анализ его криптостойкости.

Задание 1. Теоретическое обоснование

1. Объясните математическую модель шифра:
   - Формула шифрования: ci=(mi+kj)mod Q$ci=(mi+kj)\mod Q$
   - Формула дешифрования: mi=(ci−kj)mod Q$mi=(ci-kj)\mod Q$
   - Где Q=33$Q=33$ (для русского алфавита), mimi – позиция символа открытого текста, kjkj – позиция символа ключа.
2. Постройте таблицу Виженера для русского алфавита (6х6 символов) и продемонстрируйте ручное шифрование фразы "КРИПТОГРАФИЯ" с ключом "ЗАЩИТА".

Задание 2. Программная реализация

Реализуйте на Python/C#:

1. Генератор повторяющегося ключа:

python

```
def generate_key(text,  keyword):
   return (keyword * (len(text)//len(keyword) + 1))[:len(text)]
```

2. Функции шифрования/дешифрования с обработкой:
    - Русского алфавита (33 буквы + "Ё")
    - Сохранения регистра и пробелов
3. Пример работы программы:

text
Ввод: "Атака на рассвете", ключ: "СЕКРЕТ"
Вывод: "СЯМРПЖ ЪЧ ДСУАЦХИ"

Задание 3. Криптоанализ

1. Проведите частотный анализ зашифрованного текста:
    - Сравните распределение символов с эталоном для русского языка
    - Определите длину ключа методом Казиски
2. Реализуйте атаку по известному открытому тексту:
    - Восстановите ключ по паре "исходный-зашифрованный текст"
    - Оцените минимальную длину ключа для обеспечения безопасности

Задание 4. Сравнительный анализ

Создайте таблицу сравнения:

Параметр	**Цезарь**	**Виженер**	**AES**
Тип шифра	Одноалфавитный	Многоалфавитный	Блочный
Криптостойкость	Низкая	Средняя	Высокая
Скорость работы	1x	1.2x	0.8x

Вопросы для защиты

1. Почему повторное использование ключа снижает безопасность?
2. Как влияет длина ключа на устойчивость к частотному анализу?
3. Какие модификации алгоритма могут повысить криптостойкость?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 3. Блочный шифр. Ключевая система.

Цель: изучить принципы работы блочных шифров, освоить методы генерации ключей и провести сравнительный анализ режимов шифрования.

Задание 1. Теоретические основы

1. **Сравнение типов шифров**
   Создайте таблицу различий между блочными и поточными шифрами:

Параметр	**Блочный шифр**	**Поточный шифр**
Обработка данных	Фиксированные блоки	Поток битов
Скорость	Медленнее	Быстрее
Примеры алгоритмов	AES, DES	RC4, ChaCha20

2. **Ключевое расписание**
   Изучите алгоритм генерации раундовых ключей в AES-256:
   - Напишите функцию на Python для преобразования 256-битного ключа в массив подключей (14 раундов).
   - Продемонстрируйте процесс расширения ключа для начальных 3 раундов.5

Задание 2. Реализация режимов шифрования

1. **Программная реализация ECB и CBC**
   Напишите на Python:
   - Шифрование блока AES-128 в режиме ECB
   - Реализацию CBC с использованием XOR для цепочки блоков

```
python
def cbc_encrypt(plain_blocks, key, iv):
    cipher = AES.new(key, AES.MODE_ECB)
    prev = iv
    cipher_blocks = []
    for block in plain_blocks:
        xored = xor_bytes(block, prev)
        encrypted = cipher.encrypt(xored)
        cipher_blocks.append(encrypted)
        prev = encrypted
    return cipher_blocks
```

2. **Анализ уязвимостей**
   Зашифруйте изображение в режиме ECB и CBC. Объясните, почему в ECB сохраняются видимые паттерны исходного изображения.

Задание 3. Криптоанализ ключевой системы

1. **Атака на слабый ключ**
   Для упрощенного блочного шифра (4-битные блоки):
   - Определите ключи, при которых E(E(m, k), k) = m
   - Рассчитайте вероятность нахождения таких ключей
2. **Эксперимент с повторным использованием ключа**
   Шифруйте два разных сообщения одним ключом в режиме CTR:
   - Покажите, как получить XOR оригинальных текстов из шифрограмм
   - Предложите метод восстановления сообщений при известной структуре данных

Задание 4. Оптимизация ключевой инфраструктуры

1. **Генерация производных ключей**
   Реализуйте схему HKDF для получения:
   - 3 сессионных ключей из мастер-ключа
   - Ключа аутентификации и ключа шифрования
2. **Оценка безопасности**
   Сравните стойкость следующих систем:
   - Статический ключ на 1 год
   - Ежедневная ротация ключей с мастер-ключом
   - Эфемерные ключи для каждой транзакции

Вопросы для защиты

1. Почему режим ECB запрещен в современных стандартах?
2. Как длина ключа влияет на устойчивость к brute-force атакам?
3. Какие угрозы возникают при ошибках в реализации ключевого расписания?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org

6. http://keirsey.com

Практическое занятие 4. Шифрование алгоритмом S-DES.

Цель: Освоить принципы работы упрощенного блочного шифра S-DES, реализовать алгоритм программно и провести анализ его криптостойкости.

Задание 1. Теоретическая часть

1. **Структура алгоритма**
   - Объясните схему работы S-DES с использованием 8-битных блоков и 10-битного ключа.
   - Нарисуйте блок-схему алгоритма, включая начальную/конечную перестановки, два раунда Фейстеля и функцию f(R, K).
2. **Функция шифрования f**
   - Опишите этапы работы функции:
     1. Расширение 4-битного блока до 8 бит (E-блок)
     2. XOR с подключом
     3. Преобразование через S-блоки (S0 и S1)
     4. Перестановка P-блока

Задание 2. Программная реализация

Реализуйте на Python:

1. **Генератор подключей**

```
python
def generate_subkeys(key):
    p10 = [3,5,2,7,4,10,1,9,8,6]
    p8 = [6,3,7,4,8,5,10,9]
    # Реализация преобразований P10 и P8
    return k1, k2
```

2. **Шифрование/дешифрование**

```
python
def s_des(block, key, mode='encrypt'):
    # Реализация начальной перестановки IP
    # Два раунда Фейстеля
    # Конечная перестановка IP⁻¹
    return cipher_block
```

3. **Пример работы:**

```
text
Вход: 0b01110010 (114 в ASCII - 'r')
Ключ: 0b1010000010
Шифротекст: 0b10110110 (182)
```

Задание 3. Криптоанализ

1. **Частотный анализ**
   - Зашифруйте текст на русском языке
   - Постройте гистограмму распределения битов в шифротексте
   - Сравните с распределением в открытом тексте
2. **Атака перебором**
   - Реализуйте брутфорс-атаку для 10-битного ключа
   - Рассчитайте теоретическое время взлома при скорости 1000 ключей/сек

Задание 4. Сравнение с DES

Создайте таблицу характеристик:

Параметр	S-DES	DES
Размер блока	8 бит	64 бит
Длина ключа	10 бит	56 бит
Число раундов	2	16
Тип S-блоков	2 (4x4)	8 (6x4)
Скорость (циклов/с)	1.2x	1x

Вопросы для защиты

1. Почему S-DES считается учебным алгоритмом?
2. Как влияет количество раундов на лавинный эффект?
3. Какие модификации могли бы повысить стойкость S-DES?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org

6. http://keirsey.com

Практическое занятие 5. Расшифрование алгоритмом S-DES.

Цель: освоить принципы расшифрования с помощью упрощенного блочного шифра S-DES, реализовать алгоритм программно и оценить его эффективность.

Задание 1. Теоретическая часть

1. **Обратимость S-DES**

- Объясните, почему S-DES является обратимым шифром.
- Опишите схему дешифрования, которая включает обратные операции по сравнению с шифрованием.

2. **Начальная и конечная перестановки**

- Покажите, как начальная перестановка IP и конечная перестановка IP^{-1} используются в процессе дешифрования.

Задание 2. Программная реализация

Реализуйте на Python:

1. **Генератор подключей**

```
python
def generate_subkeys(key):
    # Реализация генерации подключей K1 и K2
    return k1, k2
```

2. **Дешифрование**

```
python
def s_des_decrypt(cipher_block, key, mode='decrypt'):
    # Реализация обратных раундов Фейстеля
    # Применение конечной перестановки IP⁻¹
    return plain_block
```

3. **Пример работы:**

```
text
Вход: Зашифрованный блок 0b10110110
Ключ: 0b1010000010
Расшифрованный текст: 0b01110010
```

Задание 3. Анализ безопасности

1. **Атака на слабый ключ**

- Оцените вероятность успешной атаки на S-DES с помощью брутфорса.
- Рассчитайте время, необходимое для перебора всех возможных ключей при скорости 1000 ключей/сек.

2. **Частотный анализ**

- Расшифруйте текст, зашифрованный с помощью S-DES.
- Постройте гистограмму распределения битов в расшифрованном тексте и сравните с распределением в исходном тексте.

Задание 4. Сравнение с DES
Создайте таблицу сравнения:

Параметр	**S-DES**	**DES**
Размер блока	8 бит	64 бит
Длина ключа	10 бит	56 бит
Число раундов	2	16
Тип S-блоков	2 (4x4)	8 (6x4)
Скорость (циклов/с)	1.2x	1x

Вопросы для защиты
1. Как обратимость S-DES влияет на его криптостойкость?
2. Какие методы могут быть использованы для повышения безопасности S-DES?
3. Как сравнить эффективность S-DES и DES в реальных приложениях?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины
1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 6. Шифрование алгоритмом S-AES.

Цель: изучить принципы работы упрощенного алгоритма S-AES, реализовать его программно и оценить его криптостойкость.

Задание 1. Теоретическая часть
1. **Описание алгоритма S-AES**

- Объясните структуру S-AES: 16-битные блоки, 16-битный ключ, предварительный раунд и два раунда шифрования.
- Опишите функцию f и процесс расширения ключей для каждого раунда.

2. **Сравнение с AES**
   - Создайте таблицу сравнения S-AES и AES по размеру блока, длине ключа и числу раундов.

Задание 2. Программная реализация

Реализуйте на Python:

1. **Генератор ключей**

```
python
def generate_subkeys(key):
    # Реализация генерации подключей K0, K1, K2
    return k0, k1, k2
```

2. **Шифрование**

```
python
def s_aes_encrypt(block, key):
    # Реализация предварительного раунда
    # Два раунда шифрования
    return cipher_block
```

3. **Пример работы:**

```
text
Вход: Блок 0b11010101
Ключ: 0b10101010
Шифротекст: 0b11101110
```

Задание 3. Криптоанализ

1. **Атака на слабый ключ**
   - Оцените вероятность успешной атаки на S-AES с помощью брутфорса.
   - Рассчитайте время, необходимое для перебора всех возможных ключей при скорости 1000 ключей/сек.
2. **Квантово-усиленный криптоанализ**
   - Изучите возможность применения алгоритма Гровера для ускорения атаки на S-AES.
   - Оцените необходимое количество кубитов для реализации такой атаки.

Задание 4. Сравнение с другими алгоритмами

Создайте таблицу сравнения:

Параметр	**S-AES**	**AES**	**DES**
Размер блока	16 бит	128 бит	64 бит
Длина ключа	16 бит	128/192/256 бит	56 бит
Число раундов	2	10/12/14	16
Тип шифра	Не-Файстель	Не-Файстель	Файстель

Вопросы для защиты

1. Как S-AES используется для обучения криптографии?

2. Какие методы могут быть применены для повышения криптостойкости S-AES?
3. Как сравнить эффективность S-AES и AES в реальных приложениях?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 7. Расшифрованне алгоритмом S-AES.

Цель: освоить принципы расшифрования с помощью упрощенного алгоритма S-AES, реализовать его программно и оценить его эффективность.

Задание 1. Теоретическая часть

1. **Обратимость S-AES**
   - Объясните, почему S-AES является обратимым шифром.
   - Опишите схему дешифрования, которая включает обратные операции по сравнению с шифрованием.
2. **Ключевая система**
   - Опишите процесс генерации ключей для S-AES: ключ шифра на 16 бит, три ключа раунда (K0, K1, K2).

Задание 2. Программная реализация

Реализуйте на Python:

1. **Генератор ключей**

```
python
def generate_subkeys(key):
    # Реализация генерации подключей K0, K1, K2
    return k0, k1, k2
```

2. **Дешифрование**

```
python
def s_aes_decrypt(cipher_block, key, mode='decrypt'):
    # Реализация обратных раундов
    # Применение конечной перестановки
    return plain_block
```

3. **Пример работы:**

```
text
Вход: Зашифрованный блок 0b11101110
Ключ: 0b10101010
Расшифрованный текст: 0b11010101
```

Задание 3. Криптоанализ

1. **Атака на слабый ключ**
   - Оцените вероятность успешной атаки на S-AES с помощью брутфорса.
   - Рассчитайте время, необходимое для перебора всех возможных ключей при скорости 1000 ключей/сек.
2. **Частотный анализ**
   - Расшифруйте текст, зашифрованный с помощью S-AES.
   - Постройте гистограмму распределения битов в расшифрованном тексте и сравните с распределением в исходном тексте.

Задание 4. Сравнение с AES

Создайте таблицу сравнения:

Параметр	S-AES	AES
Размер блока	16 бит	128 бит
Длина ключа	16 бит	128/192/256 бит
Число раундов	2	10/12/14
Тип шифра	Не-Файстель	Не-Файстель
Скорость (циклов/с)	1.2x	1x

Вопросы для защиты

1. Как обратимость S-AES влияет на его криптостойкость?
2. Какие методы могут быть использованы для повышения безопасности S-AES?
3. Как сравнить эффективность S-AES и AES в реальных приложениях?

Перечень основной литературы

3. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
4. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

2. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

7. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
8. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
9. https://spravochnick.ru/psihologiya/ – Справочник по психологии
10. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
11. http://www.myersbriggs.org
12. http://keirsey.com

Практическое занятие 8. Шифрование и расшифрование алгоритмом S-Магма.

Цель: изучить принципы работы алгоритма Магма, реализовать его программно и оценить его криптостойкость.

Задание 1. Теоретическая часть

1. **Описание алгоритма Магма**
   - Объясните структуру алгоритма Магма: 64-битные блоки, 256-битный ключ, 32 раунда шифрования.
   - Опишите схему сети Фейстеля и функцию F*F*, которая включает сложение с ключом, замену в S-блоках и циклический сдвиг.
2. **Сравнение с другими алгоритмами**
   - Создайте таблицу сравнения Магма с AES и DES по размеру блока, длине ключа и числу раундов.

Задание 2. Программная реализация

Реализуйте на Python:

1. **Генератор раундовых ключей**

```
python
def generate_round_keys(key):
    # Разделение 256-битного ключа на 32 раундовых ключа
    return round_keys
```

2. **Шифрование и расшифрование**

```
python
def magma_encrypt(block, key):
    # Реализация 32 раундов шифрования
    return cipher_block

def magma_decrypt(cipher_block, key):
```

 # Реализация 32 раундов расшифрования с обратным порядком ключей
return plain_block

3. **Пример работы:**
   text
   Вход: Блок 0b11010101
   Ключ: 256-битный ключ
   Шифротекст: 0b11101110
   Расшифрованный текст: 0b11010101

Задание 3. Криптоанализ

1. **Атака на слабый ключ**
   - Оцените вероятность успешной атаки на Магму с помощью брутфорса.
   - Рассчитайте время, необходимое для перебора всех возможных ключей при скорости 1000 ключей/сек.
2. **Линейный криптоанализ**
   - Изучите возможность применения линейного криптоанализа к Магме.
   - Оцените эффективность этого метода для взлома шифра.

Задание 4. Сравнение с другими алгоритмами

Создайте таблицу сравнения:

Параметр	Магма	AES	DES
Размер блока	64 бит	128 бит	64 бит
Длина ключа	256 бит	128/192/256 бит	56 бит
Число раундов	32	10/12/14	16
Тип шифра	Фейстель	Не-Фейстель	Файстель
Скорость (циклов/с)	1x	1x	0.8x

Вопросы для защиты

1. Как фиксированные блоки замены влияют на криптостойкость Магмы?
2. Какие методы могут быть использованы для повышения безопасности Магмы?
3. Как сравнить эффективность Магмы и AES в реальных приложениях?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 9. Шифрование на основе генератора Фибоначчи.

Цель: изучить принципы генерации псевдослучайных чисел с помощью генератора Фибоначчи с запаздываниями и реализовать простой алгоритм шифрования на его основе.

Задание 1. Теоретическая часть

1. **Описание генератора Фибоначчи с запаздываниями**
   - Объясните принцип работы генератора: $x_n = x_{n-a} + x_{n-b}$ $x_n = x_{n-a} + x_{n-b}$, где a и b — константы запаздывания.
   - Опишите рекомендуемые значения для a и b, такие как (55, 24) или (17, 5).
2. **Применение в криптографии**
   - Обсудите роль генераторов псевдослучайных чисел в криптографии, особенно в поточных шифрах.
   - Опишите требования к генераторам ПСЧ для криптографических приложений.

Задание 2. Программная реализация

Реализуйте на Python:

1. **Генератор Фибоначчи с запаздываниями**

python
```
def lagged_fibonacci(a, b, seed, n):
    sequence = seed
    for i in range(n):
        sequence.append((sequence[-a] + sequence[-b]) % 2**32)
    return sequence
```

2. **Простой поточный шифр**

python
```
def encrypt(plaintext, key):
    # Генерация ключевой последовательности с помощью генератора Фибоначчи
    key_sequence = lagged_fibonacci(17, 5, [key], len(plaintext))
    # XOR с открытым текстом
```

```
    return [p ^ k for p, k in zip(plaintext, key_sequence)]
```

3. **Пример работы:**

text
Вход: "Привет"
Ключ: 12345
Шифротекст: "..."

Задание 3. Криптоанализ

1. **Атака на слабый ключ**
   - Оцените вероятность успешной атаки на шифр с помощью брутфорса.
   - Рассчитайте время, необходимое для перебора всех возможных ключей при скорости 1000 ключей/сек.
2. **Частотный анализ**
   - Расшифруйте текст, зашифрованный с помощью генератора Фибоначчи.
   - Постройте гистограмму распределения битов в расшифрованном тексте и сравните с распределением в исходном тексте.

Задание 4. Сравнение с другими алгоритмами

Создайте таблицу сравнения:

Параметр	**Генератор Фибоначчи**	**LFSR**	**RC4**
Тип генератора	Аддитивный	LFSR	LFSR
Применение	Криптография	Криптография	Криптография
Скорость	Высокая	Высокая	Высокая
Безопасность	Средняя	Низкая	Средняя

Вопросы для защиты

1. Как свойства генератора Фибоначчи с запаздываниями влияют на криптостойкость шифра?
2. Какие методы могут быть использованы для повышения безопасности шифра на основе генератора Фибоначчи?
3. Как сравнить эффективность генератора Фибоначчи с другими генераторами ПСЧ в криптографии?

Перечень основной литературы

1. Камнева, Е.В. Тренинг командообразования и групповой работы: учебник для магистратуры : [16+] / Е.В. Камнева, Н.С. Пряжников, М.В. Полевая ; Финансовый университет при Правительстве Российской Федерации. – Москва : Прометей, 2019. – 219 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576048 – Библиогр.: с. 123 - 131. – ISBN 978-5-907166-93-6. – Текст : электронный.
2. Управление проектами : учебник : [16+] / под ред. Н.М. Филимоновой, Н.В. Моргуновой, Н.В. Родионовой. – Москва : ИНФРА-М, 2018. – 347 с. : ил., табл. – (Высшее образование - бакалавриат). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=611356 – Библиогр.: с. 335-337. – ISBN 978-5-16-013197-9 (print). - ISBN 978-5-16-105962-3 (online). – Текст : электронный.

Перечень дополнительной литературы

1. Абельская, Р.Ш. Теория и практика делового общения для разработчиков программного обеспечения и IT-менеджеров : учебное пособие / Р.Ш. Абельская ; науч. ред. И. . Обабков ; Уральский федеральный университет им. первого Президента России Б. Н. Ельцина. – Екатеринбург : Издательство Уральского университета, 2018. – 113 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=275655 – Библиогр. в кн. – ISBN 978-5-7996-1215-3. – Текст : электронный.
2. Басманова, Н.И. Тренинг командообразования : учебное пособие : [16+] / Н.И. Басманова ; Технологический университет. – Москва ; Берлин : Директ-Медиа, 2019. – 60 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=572170 – Библиогр.: с. 33-34. – ISBN 978-5-4499-0549-9. – Текст : электронный.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование

Практическое занятие 10. Расшифрование на основе генератора Фибоначчи.

Цель: изучить принципы работы генератора Фибоначчи с запаздываниями, реализовать простой алгоритм расшифрования на его основе и оценить его эффективность.

Задание 1. Теоретическая часть

1. **Описание генератора Фибоначчи с запаздываниями**
   - Объясните принцип работы генератора: xn=xn−a+xn−b*xn=xn−a+xn−b*, где a*a* и b*b* — константы запаздывания.
   - Опишите рекомендуемые значения для a*a* и b*b*, такие как (55, 24) или (17, 5).
2. **Применение в криптографии**
   - Обсудите роль генераторов псевдослучайных чисел в криптографии, особенно в поточных шифрах.
   - Опишите требования к генераторам ПСЧ для криптографических приложений.

Задание 2. Программная реализация

Реализуйте на Python:

1. **Генератор Фибоначчи с запаздываниями**

python

```
def lagged_fibonacci(a, b, seed, n):
    sequence = seed
```

```
    for i in range(n):
        sequence.append((sequence[-a] + sequence[-b]) % 2**32)
    return sequence
```

2. **Расшифрование**

```
python
def decrypt(cipher_text, key):
    # Генерация ключевой последовательности с помощью генератора Фибоначчи
    key_sequence = lagged_fibonacci(17, 5, [key], len(cipher_text))
    # XOR с шифротекстом
    return [c ^ k for c, k in zip(cipher_text, key_sequence)]
```

3. **Пример работы:**

```
text
Вход: Зашифрованный текст "..."
Ключ: 12345
Расшифрованный текст: "..."
```

Задание 3. Криптоанализ

1. **Атака на слабый ключ**
   - Оцените вероятность успешной атаки на шифр с помощью брутфорса.
   - Рассчитайте время, необходимое для перебора всех возможных ключей при скорости 1000 ключей/сек.
2. **Частотный анализ**
   - Расшифруйте текст, зашифрованный с помощью генератора Фибоначчи.
   - Постройте гистограмму распределения битов в расшифрованном тексте и сравните с распределением в исходном тексте.

Задание 4. Сравнение с другими алгоритмами

Создайте таблицу сравнения:

Параметр	**Генератор Фибоначчи**	**LFSR**	**RC4**
Тип генератора	Аддитивный	LFSR	LFSR
Применение	Криптография	Криптография	Криптография
Скорость	Высокая	Высокая	Высокая
Безопасность	Средняя	Низкая	Средняя

Вопросы для защиты

1. Как свойства генератора Фибоначчи с запаздываниями влияют на криптостойкость шифра?
2. Какие методы могут быть использованы для повышения безопасности шифра на основе генератора Фибоначчи?
3. Как сравнить эффективность генератора Фибоначчи с другими генераторами ПСЧ в криптографии?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 11. Шифрование на основе генераторов многотактовых кодовых фильтров.

Цель: изучить принципы работы генераторов многотактовых кодовых фильтров, реализовать простой алгоритм шифрования на их основе и оценить его криптостойкость.

Задание 1. Теоретическая часть

1. **Описание генераторов многотактовых кодовых фильтров**
   - Объясните принцип работы генераторов, которые используют несколько регистров сдвига с линейной обратной связью (РСЛОС) и комбинирующие фильтры для повышения криптостойкости.
   - Опишите требования к генераторам ПСЧ для криптографических приложений.
2. **Применение в криптографии**
   - Обсудите роль генераторов псевдослучайных чисел в поточных шифрах.
   - Опишите преимущества использования многотактовых кодовых фильтров для повышения безопасности шифров.

Задание 2. Программная реализация

Реализуйте на Python:

1. **Генератор многотактового кодового фильтра**

python

```
def multi_tap_filter(r1, r2, taps, seed):
    # Инициализация регистров
    reg1 = seed[:len(r1)]
    reg2 = seed[len(r1):]
```

```
    output = []
    for _ in range(100):
        bit1 = sum([reg1[i] for i in taps[0]]) % 2
        bit2 = sum([reg2[i] for i in taps[1]]) % 2
        output.append(bit1 ^ bit2)
        reg1 = [bit1] + reg1[:-1]
        reg2 = [bit2] + reg2[:-1]
    return output
```

2. **Шифрование**

```
python
def encrypt(plaintext, key):
    # Генерация ключевой последовательности с помощью генератора многотактового кодового фильтра
    key_sequence = multi_tap_filter([8, 8], [8, 8], [[0, 3], [1, 4]], key)
    # XOR с открытым текстом
    return [p ^ k for p, k in zip(plaintext, key_sequence)]
```

3. **Пример работы:**

```
text
Вход: "Привет"
Ключ: [1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0]
Шифротекст: "..."
```

Задание 3. Криптоанализ

1. **Атака на слабый ключ**
   - Оцените вероятность успешной атаки на шифр с помощью брутфорса.
   - Рассчитайте время, необходимое для перебора всех возможных ключей при скорости 1000 ключей/сек.
2. **Корреляционный анализ**
   - Изучите возможность применения корреляционных атак для взлома шифра.
   - Оцените эффективность этого метода для восстановления ключа.

Задание 4. Сравнение с другими алгоритмами

Создайте таблицу сравнения:

Параметр	**Многотактовые кодовые фильтры**	**LFSR**	**RC4**
Тип генератора	Многотактовый	LFSR	LFSR
Применение	Криптография	Криптография	Криптография
Скорость	Высокая	Высокая	Высокая
Безопасность	Высокая	Низкая	Средняя

Вопросы для защиты

1. Как свойства многотактовых кодовых фильтров влияют на криптостойкость шифра?
2. Какие методы могут быть использованы для повышения безопасности шифра на основе многотактовых кодовых фильтров?
3. Как сравнить эффективность многотактовых кодовых фильтров с другими генераторами ПСЧ в криптографии?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 12. Расшифрование на основе генераторов многотактовых кодовых фильтров.

Цель: изучить принципы работы генераторов многотактовых кодовых фильтров, реализовать простой алгоритм расшифрования на их основе и оценить его эффективность.

Задание 1. Теоретическая часть

1. **Описание генераторов многотактовых кодовых фильтров**
   - Объясните принцип работы генераторов, которые используют несколько регистров сдвига с линейной обратной связью (РСЛОС) и комбинирующие фильтры для повышения криптостойкости.
   - Опишите требования к генераторам ПСЧ для криптографических приложений.
2. **Применение в криптографии**
   - Обсудите роль генераторов псевдослучайных чисел в поточных шифрах.
   - Опишите преимущества использования многотактовых кодовых фильтров для повышения безопасности шифров.

Задание 2. Программная реализация

Реализуйте на Python:

1. **Генератор многотактового кодового фильтра**

```
python
def multi_tap_filter(r1, r2, taps, seed):
    # Инициализация регистров
    reg1 = seed[:len(r1)]
    reg2 = seed[len(r1):]
    output = []
```

```
    for _ in range(100):
        bit1 = sum([reg1[i] for i in taps[0]]) % 2
        bit2 = sum([reg2[i] for i in taps[1]]) % 2
        output.append(bit1 ^ bit2)
        reg1 = [bit1] + reg1[:-1]
        reg2 = [bit2] + reg2[:-1]
    return output
```

2. **Расшифрование**

```
python
def decrypt(cipher_text, key):
    # Генерация ключевой последовательности с помощью генератора многотактового кодового фильтра
    key_sequence = multi_tap_filter([8, 8], [8, 8], [[0, 3], [1, 4]], key)
    # XOR с шифротекстом
    return [c ^ k for c, k in zip(cipher_text, key_sequence)]
```

3. **Пример работы:**

```
text
Вход: Зашифрованный текст "..."
Ключ: [1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0]
Расшифрованный текст: "..."
```

Задание 3. Криптоанализ

1. **Атака на слабый ключ**
   - Оцените вероятность успешной атаки на шифр с помощью брутфорса.
   - Рассчитайте время, необходимое для перебора всех возможных ключей при скорости 1000 ключей/сек.
2. **Корреляционный анализ**
   - Изучите возможность применения корреляционных атак для взлома шифра.
   - Оцените эффективность этого метода для восстановления ключа.

Задание 4. Сравнение с другими алгоритмами

Создайте таблицу сравнения:

Параметр	**Многотактовые кодовые фильтры**	**LFSR**	**RC4**
Тип генератора	Многотактовый	LFSR	LFSR
Применение	Криптография	Криптография	Криптография
Скорость	Высокая	Высокая	Высокая
Безопасность	Высокая	Низкая	Средняя

Вопросы для защиты

1. Как свойства многотактовых кодовых фильтров влияют на криптостойкость шифра?

2. Какие методы могут быть использованы для повышения безопасности шифра на основе многотактовых кодовых фильтров?
3. Как сравнить эффективность многотактовых кодовых фильтров с другими генераторами ПСЧ в криптографии?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 13. Шифрование с помощью самосинхронизирующихся поточных шифров.

Цель: изучить принципы работы самосинхронизирующихся поточных шифров, реализовать простой алгоритм шифрования на их основе и оценить его эффективность.

Задание 1. Теоретическая часть

1. **Описание самосинхронизирующихся поточных шифров**
   - Объясните принцип работы шифров, где каждый бит открытого текста шифруется с учетом предыдущих битов шифртекста.
   - Опишите преимущества самосинхронизирующихся шифров перед синхронными и блочными шифрами.
2. **Сравнение с другими типами шифров**
   - Создайте таблицу сравнения самосинхронизирующихся поточных шифров с синхронными поточными и блочными шифрами.

Задание 2. Программная реализация

Реализуйте на Python:

1. **Генератор ключевой последовательности**

python

```
def generate_key_sequence(cipher_text, key, n):
    # Инициализация ключевой последовательности
```

```
    key_sequence = []
    for i in range(n):
        # Функция шифрования, зависящая от предыдущих битов шифртекста
        key_bit = (cipher_text[i-1] if i > 0 else key) ^ (cipher_text[i-2] if i > 1 else key)
        key_sequence.append(key_bit)
    return key_sequence
```

2. **Шифрование**

```
python
def encrypt(plaintext, key):
    # Генерация ключевой последовательности
    key_sequence = generate_key_sequence(plaintext, key, len(plaintext))
    # XOR с открытым текстом
    return [p ^ k for p, k in zip(plaintext, key_sequence)]
```

3. **Пример работы:**

```
text
Вход: "Привет"
Ключ: 12345
Шифротекст: "..."
```

Задание 3. Криптоанализ

1. **Атака на слабый ключ**
   - Оцените вероятность успешной атаки на шифр с помощью брутфорса.
   - Рассчитайте время, необходимое для перебора всех возможных ключей при скорости 1000 ключей/сек.
2. **Корреляционный анализ**
   - Изучите возможность применения корреляционных атак для взлома шифра.
   - Оцените эффективность этого метода для восстановления ключа.

Задание 4. Сравнение с другими алгоритмами

Создайте таблицу сравнения:

Параметр	**Самосинхронизирующиеся поточные шифры**	**Синхронные поточные шифры**	**Блочные шифры**
Тип шифра	Поточный	Поточный	Блочный
Синхронизация	Не требуется	Требуется	Не требуется
Скорость	Высокая	Высокая	Низкая
Безопасность	Средняя	Низкая	Высокая

Вопросы для защиты

1. Как самосинхронизирующиеся поточные шифры устойчивы к ошибкам передачи?
2. Какие методы могут быть использованы для повышения безопасности самосинхронизирующихся шифров?
3. Как сравнить эффективность самосинхронизирующихся шифров с синхронными и блочными шифрами?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 14. Расшифрование с помощью самосинхронизирующихся поточных шифров.

Цель: изучить принципы работы самосинхронизирующихся поточных шифров, реализовать простой алгоритм расшифрования на их основе и оценить его эффективность.

Задание 1. Теоретическая часть

1. **Описание самосинхронизирующихся поточных шифров**
   - Объясните принцип работы шифров, где каждый бит открытого текста шифруется в зависимости от функции ключа и предыдущих битов шифртекста.
   - Опишите преимущества самосинхронизирующихся шифров перед синхронными и блочными шифрами.
2. **Сравнение с другими типами шифров**
   - Создайте таблицу сравнения самосинхронизирующихся поточных шифров с синхронными поточными и блочными шифрами.

Задание 2. Программная реализация

Реализуйте на Python:

1. **Генератор ключевой последовательности**

python

```
def generate_key_sequence(cipher_text, n):
    # Инициализация ключевой последовательности
    key_sequence = []
    for i in range(len(cipher_text)):
        if i < n:
            key_bit = cipher_text[i]
        else:
            key_bit = cipher_text[i-n] ^ cipher_text[i-n+1]
```

```
        key_sequence.append(key_bit)
    return key_sequence
```

2. **Расшифрование**

```
python
def decrypt(cipher_text, n):
    # Генерация ключевой последовательности
    key_sequence = generate_key_sequence(cipher_text, n)
    # XOR с шифротекстом
    return [c ^ k for c, k in zip(cipher_text, key_sequence)]
```

3. **Пример работы:**

```
text
Вход: Зашифрованный текст "..."
n = 3 (количество предыдущих битов, используемых для генерации ключа)
Расшифрованный текст: "..."
```

Задание 3. Криптоанализ

1. **Атака на слабый ключ**
   - Оцените вероятность успешной атаки на шифр с помощью брутфорса.
   - Рассчитайте время, необходимое для перебора всех возможных ключей при скорости 1000 ключей/сек.
2. **Корреляционный анализ**
   - Изучите возможность применения корреляционных атак для взлома шифра.
   - Оцените эффективность этого метода для восстановления ключа.

Задание 4. Сравнение с другими алгоритмами

Создайте таблицу сравнения:

Параметр	**Самосинхронизирующиеся поточные шифры**	**Синхронные поточные шифры**	**Блочные шифры**
Тип шифра	Поточный	Поточный	Блочный
Синхронизация	Не требуется	Требуется	Не требуется
Скорость	Высокая	Высокая	Низкая
Безопасность	Средняя	Низкая	Высокая

Вопросы для защиты

1. Как самосинхронизирующиеся поточные шифры устойчивы к ошибкам передачи?
2. Какие методы могут быть использованы для повышения безопасности самосинхронизирующихся шифров?
3. Как сравнить эффективность самосинхронизирующихся шифров с синхронными и блочными шифрами?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks

2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 15. Основы построения поточного шифра S-A5.

Цель: изучить принципы работы поточных шифров на основе алгоритма A5, реализовать упрощенную версию S-A5 и оценить ее криптостойкость.

Задание 1. Теоретическая часть

1. **Описание алгоритма A5**
   - Объясните принцип работы A5: использование трех регистров сдвига с обратной связью для генерации псевдослучайной последовательности и операция XOR для шифрования.
   - Опишите схему инициализации регистров с помощью ключа и номера кадра.
2. **Преимущества поточных шифров**
   - Обсудите преимущества поточных шифров перед блочными: скорость, простота реализации и устойчивость к ошибкам передачи.

Задание 2. Упрощенная модель S-A5

1. **Упрощение регистров сдвига**
   - Используйте два регистра сдвига вместо трех, с меньшими длинами (например, 8 и 10 бит).
   - Реализуйте упрощенную схему управления сдвигами, где оба регистра сдвигаются на каждом такте.
2. **Программная реализация**

python

```
def s_a5_encrypt(plaintext, key):
    # Инициализация регистров
    reg1 = [0]*8
    reg2 = [0]*10
    for i in range(len(key)):
        reg1[i % 8] ^= key[i]
        reg2[i % 10] ^= key[i]
```

```
    # Генерация ключевой последовательности
    key_sequence = []
    for _ in range(len(plaintext)):
        bit1 = reg1[0]
        bit2 = reg2[0]
        key_sequence.append(bit1 ^ bit2)
        reg1 = [bit1] + reg1[:-1]
        reg2 = [bit2] + reg2[:-1]

    # Шифрование
    return [p ^ k for p, k in zip(plaintext, key_sequence)]
```

3. **Пример работы:**

text
Вход: "Привет"
Ключ: [1, 0, 1, 0, 1, 0, 1, 0]
Шифротекст: "..."

Задание 3. Криптоанализ

1. **Атака на слабый ключ**
   - Оцените вероятность успешной атаки на S-A5 с помощью брутфорса.
   - Рассчитайте время, необходимое для перебора всех возможных ключей при скорости 1000 ключей/сек.
2. **Частотный анализ**
   - Расшифруйте текст, зашифрованный с помощью S-A5.
   - Постройте гистограмму распределения битов в расшифрованном тексте и сравните с распределением в исходном тексте.

Задание 4. Сравнение с A5

Создайте таблицу сравнения:

Параметр	**S-A5**	**A5**
Количество регистров	2	3
Длина регистров	8 и 10 бит	19, 22, 23 бита
Скорость	Высокая	Высокая
Безопасность	Низкая	Средняя

Вопросы для защиты

1. Как упрощение регистров сдвига влияет на криптостойкость S-A5?
2. Какие методы могут быть использованы для повышения безопасности S-A5?
3. Как сравнить эффективность S-A5 и A5 в реальных приложениях?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks

2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 16. Расшифрование с помощью поточного шифра S-A5.

Цель: изучить принципы работы упрощенного поточного шифра S-A5, реализовать простой алгоритм расшифрования на его основе и оценить его эффективность.

Задание 1. Теоретическая часть

1. **Описание алгоритма A5**
   - Объясните принцип работы A5: использование трех регистров сдвига с обратной связью для генерации псевдослучайной последовательности и операция XOR для шифрования.
   - Опишите схему инициализации регистров с помощью ключа и номера кадра.
2. **Упрощение для S-A5**
   - Объясните, как можно упростить A5 для образовательных целей, например, уменьшив количество регистров или их длину.

Задание 2. Программная реализация

Реализуйте на Python:

1. **Генератор ключевой последовательности**

python

```
def generate_key_sequence(cipher_text, key, n):
    # Инициализация регистров
    reg1 = [0]*8
    reg2 = [0]*10
    for i in range(len(key)):
        reg1[i % 8] ^= key[i]
        reg2[i % 10] ^= key[i]

    # Генерация ключевой последовательности
    key_sequence = []
    for _ in range(len(cipher_text)):
        bit1 = reg1[0]
        bit2 = reg2[0]
        key_sequence.append(bit1 ^ bit2)
```

```
        reg1 = [bit1] + reg1[:-1]
        reg2 = [bit2] + reg2[:-1]
    return key_sequence
```

2. **Расшифрование**

```
python
def decrypt(cipher_text, key):
    # Генерация ключевой последовательности
    key_sequence = generate_key_sequence(cipher_text, key, len(cipher_text))
    # XOR с шифротекстом
    return [c ^ k for c, k in zip(cipher_text, key_sequence)]
```

3. **Пример работы:**

```
text
Вход: Зашифрованный текст "..."
Ключ: [1, 0, 1, 0, 1, 0, 1, 0]
Расшифрованный текст: "..."
```

Задание 3. Криптоанализ

1. **Атака на слабый ключ**
   - Оцените вероятность успешной атаки на S-A5 с помощью брутфорса.
   - Рассчитайте время, необходимое для перебора всех возможных ключей при скорости 1000 ключей/сек.
2. **Частотный анализ**
   - Расшифруйте текст, зашифрованный с помощью S-A5.
   - Постройте гистограмму распределения битов в расшифрованном тексте и сравните с распределением в исходном тексте.

Задание 4. Сравнение с A5

Создайте таблицу сравнения:

Параметр	**S-A5**	**A5**
Количество регистров	2	3
Длина регистров	8 и 10 бит	19, 22, 23 бита
Скорость	Высокая	Высокая
Безопасность	Низкая	Средняя

Вопросы для защиты

1. Как упрощение регистров сдвига влияет на криптостойкость S-A5?
2. Какие методы могут быть использованы для повышения безопасности S-A5?
3. Как сравнить эффективность S-A5 и A5 в реальных приложениях?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks

2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 17. Алгоритм шифрования без передачи ключа.

Цель: изучить принципы шифрования без передачи ключа, реализовать протокол Диффи — Хеллмана для обмена ключами и оценить его эффективность.

Задание 1. Теоретическая часть

1. **Протокол Диффи — Хеллмана**
   - Объясните принцип работы протокола: обмен публичными значениями для получения общего секретного ключа без его передачи.
   - Опишите математические основы протокола, основанные на дискретном логарифмировании.
2. **Преимущества шифрования без передачи ключа**
   - Обсудите преимущества использования протокола Диффи — Хеллмана для безопасного обмена ключами.

Задание 2. Программная реализация

Реализуйте на Python:

1. **Протокол Диффи — Хеллмана**

python

```
def diffie_hellman(p, g, a, b):
    A = pow(g, a, p)
    B = pow(g, b, p)
    K_A = pow(B, a, p)
```

```
    K_B = pow(A, b, p)
    return K_A, K_B
```

2. **Шифрование с общим ключом**

```
python
def encrypt(plaintext, key):
    # Симметричное шифрование с помощью общего ключа
    return [p ^ k for p, k in zip(plaintext, key)]
```

3. **Пример работы:**

```
text
Вход: "Привет"
p = 23, g = 5, a = 6, b = 15
K_A = K_B = 8
Шифротекст: "..."
```

Задание 3. Криптоанализ

1. **Атака на протокол Диффи — Хеллмана**
   - Оцените вероятность успешной атаки на протокол с помощью метода "человек посередине".
   - Рассчитайте время, необходимое для взлома ключа при скорости 1000 вычислений/сек.
2. **Корреляционный анализ**
   - Изучите возможность применения корреляционных атак для взлома шифра.
   - Оцените эффективность этого метода для восстановления ключа.

Задание 4. Сравнение с другими алгоритмами

Создайте таблицу сравнения:

Параметр	**Протокол Диффи — Хеллмана**	**RSA**	**AES**
Тип шифра	Обмен ключами	Асимметричный	Симметричный
Безопасность	Высокая	Высокая	Высокая
Скорость	Низкая	Низкая	Высокая

Параметр	Протокол Диффи — Хеллмана	RSA	AES
Применение	Обмен ключами	Шифрование и подпись	Шифрование данных

Вопросы для защиты

1. Как протокол Диффи — Хеллмана обеспечивает безопасный обмен ключами?
2. Какие методы могут быть использованы для повышения безопасности протокола Диффи — Хеллмана?
3. Как сравнить эффективность протокола Диффи — Хеллмана с другими алгоритмами обмена ключами?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

Практическое занятие 18. Алгоритм шифрования Эль-Гамаля.

Цель: изучить принципы работы криптосистемы Эль-Гамаля, реализовать алгоритм шифрования и расшифрования на его основе и оценить его эффективность.

Задание 1. Теоретическая часть

1. **Описание алгоритма Эль-Гамаля**
    - Объясните принцип работы алгоритма: использование дискретных логарифмов в конечном поле для шифрования и расшифрования.
    - Опишите схему генерации ключей и процесс шифрования/расшифрования.

2. **Преимущества и недостатки**

- Обсудите преимущества и недостатки алгоритма Эль-Гамаля по сравнению с другими криптосистемами (например, RSA).

Задание 2. Программная реализация

Реализуйте на Python:

1. **Генерация ключей**

```
python
def generate_keys(p, g):
    x = random.randint(1, p-1)  # Секретный ключ
    y = pow(g, x, p)  # Открытый ключ
    return x, y
```

2. **Шифрование**

```
python
def encrypt(message, p, g, y):
    k = random.randint(1, p-2)  # Сессионный ключ
    a = pow(g, k, p)
    b = (message * pow(y, k, p)) % p
    return a, b
```

3. **Расшифрование**

```
python
def decrypt(a, b, p, x):
    message = (b * pow(a, p-1-x, p)) % p
    return message
```

4. **Пример работы:**

```
text
Вход: Сообщение m = 15
p = 23, g = 5, x = 8 (секретный ключ)
y = 5^8 mod 23 = 21 (открытый ключ)
k = 7 (сессионный ключ)
Шифротекст: (a, b) = (17, 12)
Расшифрованный текст: m' = 15
```

Задание 3. Криптоанализ

1. **Атака на дискретные логарифмы**
    - Оцените вероятность успешной атаки на алгоритм Эль-Гамаля с помощью методов вычисления дискретных логарифмов.
    - Рассчитайте время, необходимое для взлома ключа при скорости 1000 вычислений/сек.
2. **Атака на сессионный ключ**
    - Изучите возможность применения атак на сессионный ключ для взлома шифра.
    - Оцените эффективность этого метода для восстановления ключа.

Задание 4. Сравнение с другими алгоритмами

Создайте таблицу сравнения:

Параметр	**Эль-Гамаль**	**RSA**	**Диффи-Хеллман**
Тип шифра	Асимметричный	Асимметричный	Обмен ключами
Безопасность	Высокая	Высокая	Высокая
Скорость	Низкая	Низкая	Низкая
Применение	Шифрование и подпись	Шифрование и подпись	Обмен ключами

Вопросы для защиты

1. Как алгоритм Эль-Гамаля обеспечивает безопасность передачи данных?
2. Какие методы могут быть использованы для повышения безопасности алгоритма Эль-Гамаля?
3. Как сравнить эффективность алгоритма Эль-Гамаля с другими криптосистемами?

Перечень основной литературы

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

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

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии
4. https://ur-l.ru/LLEbZ – Тимбилдинг и эффективное командообразование
5. http://www.myersbriggs.org
6. http://keirsey.com

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ

УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

для обучающихся по организации и проведению самостоятельной работы

по дисциплине «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ КОМАНДНОЙ РАБОТЫ И ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ»

для студентов направления подготовки

_____

направленность (профиль):

_____

Ставрополь

2024

СОДЕРЖАНИЕ

1. Общие положения

Самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов). Владиславу Вячеславовичу

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

– формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

– написание докладов;

– подготовка к семинарам, практическим и лабораторным работам, их оформление;

– составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);

– выполнение учебно-исследовательских работ, проектная деятельность;

– подготовка практических разработок и рекомендаций по решению проблемной ситуации;

– выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;

– компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;

– выполнение курсовых работ (проектов) в рамках дисциплин;

– выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

- подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);
- основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);
- заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Информационные технологии командной работы и проектной деятельности» направлена на формирование следующих **компетенций**:

Код	Формулировка
ОПК-3	Способен самостоятельно создавать прикладные программные средства на основе современных информационных технологий и сетевых ресурсов, в том числе отечественного производства

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и универсальных компетенций будущего бакалавра.

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;

- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельной работы и лабораторных занятий.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе (астр.)		
				СРС	Контактная работа с преподавателем	Всего
2 семестр						
ОПК-3	Подготовка к лекциям	Конспект лекций	Собеседование	27,0	18,0	45,0
ОПК-3	Подготовка к практическим занятиям	Отчет в электронном виде	Собеседование	27,0	18,0	45,0
ОПК-3	Самостоятельное изучение литературы	Конспект	Собеседование	27,0	18,0	45,0
ОПК-3	Самотестирование, подготовка к тестированию	Тестирование	Тестовые задания	27,0	18,0	45,0
Итого за 2 семестр				108,0	72,0	180,0
Итого				108,0	72,0	180,0

4. Контрольные точки и виды отчетности по ним

Контроль качества и сроков самостоятельной работы выполняется в соответствии с учебным графиком и оформляется в соответствии с заданием. Предусмотрена следующая рейтинговая оценка знаний

Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

5. Порядок выполнения самостоятельной работы студентом

5.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

5.2. Методические рекомендации по составлению конспекта лекций:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта.

2. Выделите главное, составьте план.

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора.

4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

5.3. Методические рекомендации по подготовке к практическим занятиям

Для того чтобы практические занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на лабораторных занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

Практические работы № 1-5,8 выполняются студентами заочной и очно-заочной формы обучения самостоятельно.

5.4. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно

студенту рекомендуется провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение отвечать на вопросы для собеседования.

Критерии оценки:

Оценка «отлично» выставляется студенту, если он, отлично знает, как находить и формулировать значимые проблемы прикладной и компьютерной математики. Уверенно анализирует задачи, точно выделяет ключевые аспекты и применяет оптимальные математические методы для их решения, отлично знает и уверенно умеет находить современные информационные технологии, в том числе отечественного производства, необходимые для создания прикладных программных продуктов. Свободно ориентируется в ИТ-решениях, анализирует их возможности и эффективно применяет для разработки программного обеспечения.

Оценка «хорошо» выставляется студенту, если он, знает, как находить и формулировать значимые проблемы прикладной и компьютерной математики. Умеет анализировать задачи, выявлять основные проблемы и применять соответствующие математические методы, но может допускать отдельные неточности, знает и умеет находить современные информационные технологии, в том числе отечественного производства, необходимые для создания прикладных программных продуктов. Может анализировать доступные технологии, выбирать подходящие решения и применять их в разработке, но допускает отдельные неточности.

Оценка «удовлетворительно» выставляется студенту, если он, плохо знает, как находить и формулировать значимые проблемы прикладной и компьютерной математики. Испытывает затруднения при анализе задач, допускает ошибки в выделении ключевых аспектов и выборе математических методов для их решения, плохо знает и с трудом умеет находить современные информационные технологии, в том числе отечественного производства, необходимые для создания прикладных программных продуктов. Испытывает сложности при анализе и выборе подходящих инструментов, допускает ошибки при их применении.

Оценка «неудовлетворительно» выставляется студенту, если он, не знает, как находить и формулировать значимые проблемы прикладной и компьютерной математики. Не умеет анализировать поставленные задачи, выделять ключевые аспекты и применять математические методы для их исследования, не знает и не умеет находить современные информационные технологии, в том числе отечественного производства, необходимые для создания прикладных программных продуктов. Не ориентируется в современных ИТ-решениях, не способен анализировать их возможности и применять их на практике.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

5.6. Методические рекомендации по подготовке к зачетам

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка выполнения доклада и его презентации.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

6. Список литературы для выполнения СРС

Перечень основной литературы:

1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks
2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2021. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7

Перечень дополнительной литературы:

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Методы и средства криптографической защиты информации». Ставрополь : СКФУ, 2026.
2. Методические указания к практическим занятиям по дисциплине «Методы и средства криптографической защиты информации». Ставрополь : СКФУ, 2026.

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

www.biblioclub.ru - Электронная библиотечная система «Университетская библиотека онлайн»

www.eLibrary.ru - Научная электронная библиотека

www.iprbookshop.ru - Электронно-библиотечная система IPRbooks