

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
БУРЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ ДОРЖИ БАНАЗАРОВА  
ИНСТИТУТ МАТЕМАТИКИ, ФИЗИКИ И КОМПЬЮТЕРНЫХ НАУК  
КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И ИНФОРМАТИКИ

Утверждена на заседании  
Ученого совета ИМФКН  
«\_\_»\_\_\_\_\_ 202\_\_ г.  
Протокол № \_\_

**Рабочая программа дисциплины**  
**Основы криптографии**

Направление подготовки / специальность  
**09.04.02 Информационные системы и технологии**  
Профиль

**Проектирование, разработка и эксплуатация информационных систем**

Квалификация (степень) выпускника  
**Магистр**

Форма обучения  
**Очная**

Улан-Удэ  
2025

# Пояснительная записка

## Цели освоения дисциплины

Сформировать у студентов теоретические знания и практические навыки в области современной криптографии, необходимые для понимания принципов построения и анализа криптографических систем, а также для их применения в информационных системах и технологиях.

Задачи:

- Изучить основные понятия и определения криптографии.
- Освоить классические и современные криптографические алгоритмы шифрования и хеширования.
- Познакомиться с принципами криптографической стойкости и методами криптоанализа.
- Изучить протоколы аутентификации, электронной подписи и управления ключами.
- Рассмотреть применение криптографии в различных областях информационных технологий, включая сетевую безопасность, защиту данных и электронную коммерцию.
- Развить навыки практического применения криптографических алгоритмов и протоколов.

## Место дисциплины в структуре образовательной программы

Дисциплина "Основы криптографии" относится к части, формируемой участниками образовательных отношений, учебного плана направления 09.04.02 "Информационные системы и технологии".

**В результате освоения дисциплины студент должен:**

**Планируемые результаты обучения по дисциплине и индикаторы достижения компетенций.**

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

УК-1.1 анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними

УК-1.3 критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников

ПК-1. Способен планировать работы в проектах в области ИТ малого и среднего уровня сложности

ПК-1.1. Назначает и распределяет ресурсы в рамках управления работами по сопровождению и проектами создания (модификации) ИС

**Знать:**

- Основные понятия и определения криптографии (шифрование, дешифрование, криптографическая стойкость, криптоанализ, ключ, алгоритм).
- Классические и современные криптографические алгоритмы шифрования (DES, AES, RSA, ECC).
- Алгоритмы хеширования (MD5, SHA-1, SHA-256).
- Принципы криптографической стойкости и основные методы криптоанализа.
- Протоколы аутентификации (Kerberos, RADIUS).
- Механизмы электронной подписи (ГОСТ Р 34.10-2012, RSA, DSA).
- Принципы управления ключами (PKI).
- Области применения криптографии в информационных технологиях.

**Уметь:**

- Реализовывать базовые криптографические алгоритмы на языке программирования.
- Применять криптографические инструменты для защиты информации.
- Анализировать криптографическую стойкость алгоритмов.
- Использовать протоколы аутентификации и электронной подписи.

- Оценивать риски, связанные с использованием криптографических систем.
- Выбирать подходящие криптографические решения для конкретных задач.

#### **Владеть:**

- Навыками использования криптографических библиотек и инструментов.
- Методами анализа и оценки криптографической стойкости.
- Методами разработки и внедрения криптографических решений.
- Навыками работы с криптографическими стандартами и протоколами.

#### **Планируемые результаты освоения образовательной программы:**

### **Объем дисциплины в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся**

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часа.

№ Название разделов дисциплины	Лекция	Лабораторная работа	Самостоятельная работа
Семестр 3	12	12	84
1 Введение в криптографию	2	2	12
2 Криптографические алгоритмы	6	8	48
3 Алгоритмы хеширования. Протоколы аутентификации и электронной подписи	4	2	24

## **Тематическое планирование курса**

### **Темы**

### **Введение в криптографию**

Семестр 3

#### **Введение в криптографию**

Лекция. 2(0) ч. История развития криптографии. Основные понятия: шифрование, дешифрование, ключ, алгоритм, криптографическая стойкость, криптоанализ. Виды криптографических систем: симметричные и асимметричные. Основные задачи криптографии: конфиденциальность, целостность, аутентификация, неотказуемость. Криптографические стандарты и протоколы.

Лабораторная работа. 2(0) ч. Реализация шифра Цезаря на выбранном языке программирования.

Самостоятельная работа. 12(0) ч. Исторический обзор и современное состояние криптографии.

### **Криптографические алгоритмы**

Семестр 3

#### **Классические криптографические алгоритмы.**

Лекция. 2(0) ч. Шифры подстановки: шифр Цезаря, шифр простой подстановки, полиалфавитные шифры (Виженера, Бофорта). Шифры перестановки. Анализ криптографической стойкости классических шифров.

Лабораторная работа. 2(0) ч. Реализация полиалфавитного шифра (Виженера) на выбранном языке программирования.

Самостоятельная работа. 16(0) ч. Анализ криптографической стойкости алгоритма шифрования: Выбрать алгоритм шифрования и провести его анализ на уязвимости с использованием доступных инструментов и методов.

#### **Симметричные криптографические алгоритмы**

Лекция. 2(0) ч. DES (Data Encryption Standard). AES (Advanced Encryption Standard). Режимы работы блочных шифров (ECB, CBC, CTR, OFB). Практическое применение симметричных алгоритмов.

Лабораторная работа. 2(0) ч. Реализация блочного шифра DES или AES (упрощенная версия) на выбранном языке программирования.

Лабораторная работа. 2(0) ч. Использование криптографической библиотеки для шифрования данных с помощью AES.

Самостоятельная работа. 16(0) ч. Анализ криптографической стойкости алгоритма шифрования: Выбрать алгоритм шифрования и провести его анализ на уязвимости с использованием доступных инструментов и методов.

### **Асимметричные криптографические алгоритмы**

Лекция. 2(0) ч. RSA (Rivest-Shamir-Adleman). Алгоритмы на основе эллиптических кривых (ECC). Диффи-Хеллман (Diffie-Hellman). Практическое применение асимметричных алгоритмов.

Лабораторная работа. 2(0) ч. Реализация алгоритма RSA (упрощенная версия) на выбранном языке программирования.

Самостоятельная работа. 16(0) ч. Исследование уязвимостей веб-приложений, связанных с криптографией: Провести анализ веб-приложения на наличие уязвимостей, связанных с использованием криптографии (например, использование слабых алгоритмов шифрования, неправильная генерация ключей).

## **Алгоритмы хеширования. Протоколы аутентификации и электронной подписи**

Семестр 3

### **Хеширование. Электронная подпись**

Лекция. 2(0) ч. Свойства хеш-функций: однонаправленность, стойкость к коллизиям. Алгоритмы хеширования: MD5, SHA-1, SHA-256, SHA-3. Применение хеш-функций: контроль целостности данных, хранение паролей, цифровая подпись.

Лекция. 2(0) ч. Протоколы аутентификации: Kerberos, RADIUS. Электронная подпись: ГОСТ Р 34.10-2012, RSA, DSA. Инфраструктура открытых ключей (PKI). Практическое применение протоколов аутентификации и электронной подписи.

Лабораторная работа. 2(0) ч. Использование криптографической библиотеки для создания и проверки электронной подписи.

Самостоятельная работа. 24(0) ч. Сравнение различных криптографических библиотек: Провести сравнение различных криптографических библиотек (например, OpenSSL, Crypto++, Bouncy Castle) по критериям производительности, функциональности и безопасности.

## **БРС**

Семестр	Контрольные точки	Баллы
3	<b>Текущий контроль в разделе «Введение в криптографию»</b>	
	Выполнение и оформление отчетности по лабораторной работе	10
	Доклад, сообщение	10
3	<b>Текущий контроль в разделе «Криптографические алгоритмы»</b>	

Семестр	Контрольные точки	Баллы
	Выполнение и оформление отчетности по лабораторной работе	25
3	<b>Текущий контроль</b> в разделе «Алгоритмы хеширования. Протоколы аутентификации и электронной подписи»	
	Выполнение и оформление отчетности по лабораторной работе	5
	Тест	10
3	<b>Экзамен</b>	
	Ответ на теоретический вопрос	10
	Защита проекта	30
Итого за семестр 3:		100

## Учебно-методическое и информационное обеспечение учебного процесса

### Образовательные технологии (в том числе на занятиях, проводимых в интерактивных формах).

При реализации дисциплины используются следующие образовательные технологии:

- Лекции с использованием мультимедийных презентаций и демонстраций.
- Лабораторные работы с использованием специализированного программного обеспечения.
- Разбор кейсов (анализ реальных примеров применения ИИ в информационных системах).
- Проектная работа (разработка прототипа интеллектуальной системы).
- Работа в команде (при выполнении лабораторных работ и проектов).
- Самостоятельная работа с использованием электронных образовательных ресурсов.
- Дискуссии и обсуждения в аудитории.

### Учебно-методические материалы, в том числе методические указания для обучающихся по освоению дисциплины

Теоретическая часть курса, общие вопросы методики и технологий применения компьютерных средств излагаются преподавателем в лекционном курсе. Отдельные вопросы могут выноситься на самостоятельное изучение. Студент должен иметь в виду, что на лекциях преподаватель определяет такие вопросы и рекомендует необходимую для их изучения литературу, источники и др. ресурсы. Для успешного освоения курса необходимо внимательно фиксировать основные положения лекции, своевременно их усваивать, при необходимости самостоятельно прорабатывать, используя основную и дополнительную литературу.

Для приобретения навыков общения с ПК в процессе освоения инструментальных систем и отладки программ предназначены лабораторные занятия. Лабораторные занятия проводятся в специальных классах, оборудованных средствами вычислительной техники. На первом лабораторном занятии студенты получают инструктаж по технике безопасности при работе в классе и знакомятся с особенностями работы на конкретной вычислительной машине. Последующие лабораторные работы заключаются в освоении

инструментальных систем и отладке программ решения типовых задач. Индивидуальные задания и методические указания к выполнению каждой последующей лабораторной работы студент получает, как правило, на предыдущем занятии. Подготовка к выполнению лабораторных работ осуществляется в часы самостоятельной работы. Студенты, не подготовившиеся к занятиям, к работе на компьютере не допускаются. По каждой выполненной лабораторной работе студент оформляет отчет по установленной форме.

Самостоятельные занятия под контролем преподавателя предназначены для самостоятельного изучения студентами тех разделов курса, по которым не предусмотрено чтение лекций, либо проводятся лекции обзорного характера. По усмотрению преподавателя в часы индивидуальных занятий студентам может поручаться выполнение других заданий.

Занятия проводятся с академической группой или с половиной группы в часы, установленные расписанием занятий. На занятиях студент должен иметь конспект лекций, учебную и справочную литературу, отдельную тетрадь для записей. Весь теоретический материал, изученный в процессе индивидуальных занятий, должен быть законспектирован.

### **Оценочные средства**

По данной дисциплине разработаны оценочные средства, критерии их оценивания, а также методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

- [ФОС\\_осн\\_криптографии.doc](#)

### **Список литературы**

Перечень основной и дополнительной литературы, необходимой для освоения дисциплины.

#### **Основная**

1. [Криптографические методы защиты информации](#): Учебник и практикум для вузов/Васильева И. Н.. —Москва: Юрайт, 2022. —349 с.  
Режим доступа: <https://urait.ru/bcode/489919>
2. [Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты](#): Учебник для вузов/Фомичёв В. М., Мельников Д. А. ; под ред. Фомичёва В.М.. —Москва: Юрайт, 2022. —209 с.  
Режим доступа: <https://urait.ru/bcode/489745>
3. [Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты](#): Учебник для вузов/Фомичёв В. М., Мельников Д. А. ; под ред. Фомичёва В.М.. —Москва: Юрайт, 2021. —245 с.  
Режим доступа: <https://urait.ru/bcode/470279>
4. [Криптографические методы защиты информации](#): Учебник для вузов/Запечников С. В., Казарин О. В., Тарасов А. А.. —Москва: Юрайт, 2021. —309 с.  
Режим доступа: <https://urait.ru/bcode/468902>
5. [Криптографическая защита информации: симметричное шифрование](#): Учебное пособие для вузов/Бабенко Л. К., Ищукова Е. А.. —Москва: Юрайт, 2021. —220 с.  
Режим доступа: <https://urait.ru/bcode/471695>

#### **Дополнительная**

1. [Криптографические основы блокчейн-технологий](#)/Ищукова Е. А.,Панасенко С. П.,Романенко К. С.,Салманов В. Д.. —Москва: ДМК Пресс, 2022. —300 с.  
Режим доступа: <https://e.lanbook.com/book/314915>
2. [Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии](#)/Глухов М. М., Круглов И. А.. —Санкт-Петербург: Лань, 2021. —176 с.  
Режим доступа: <https://e.lanbook.com/book/168829>
3. [Криптографические методы защиты информации для изучающих компьютерную безопасность](#): Учебник для вузов/Лось А. Б., Нестеренко А. Ю., Рожков М. И.. —Москва: Юрайт, 2021. —424 с.  
Режим доступа: <https://urait.ru/bcode/469133>
4. [Алгебра и теория чисел для криптографии](#): учебное пособие/Мартынов Л. М.. —Санкт-Петербург: Лань, 2020. —456 с.  
Режим доступа: <https://e.lanbook.com/book/140740>
5. [КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ](#): Учебник/Лось А.Б., Нестеренко А.Ю., Рожков М.И.. —М.: Издательство Юрайт, 2016. —473 с.  
Режим доступа: <http://www.biblio-online.ru/book/1205A26D-FBAB-4CFE-B5C5-1CF25011A202>
6. [КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ](#): Учебник и практикум/Васильева И.Н.. —М.: Издательство Юрайт, 2016. —349 с.  
Режим доступа: <http://www.biblio-online.ru/book/BFCBD8F6-8A9A-41E8-875E-43CF2D02C53A>
7. [Компьютерная безопасность. Криптографические методы защиты](#)/Петров А.А.. —Москва: ДМК Пресс, 2008  
Режим доступа: [http://e.lanbook.com/books/element.php?pl1\\_cid=25&pl1\\_id=3027](http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=3027)

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

Федеральный портал. Российское образование. <http://www.edu.ru/>  
 Российский образовательный портал. <http://www.school.edu.ru/default.asp>  
 Российский портал открытого образования. <http://www.openet.edu.ru/>  
 Федеральный образовательный портал. Инженерное образование.  
<http://www.techno.edu.ru/>

**Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)**

Портал электронного обучения БГУ [e.bsu.ru](http://e.bsu.ru)  
 Личный кабинет преподаватели или студента БГУ <https://my.bsu.ru/>  
 Электронные библиотечные системы: Рукопт, издательство «Лань», Консультант студента  
 Тестовый доступ: American Institute of Physics, Znanium.com, CASC, Редакция журналов BMJ Group, БиблиоРоссика, электронная коллекция книг и журналов Informa Healthcare, Polpred, Science Translational Medicine, коллекция журналов BMG Group  
 Python (язык программирования).  
 Библиотеки Python для машинного обучения (scikit-learn, TensorFlow, Keras, PyTorch).  
 Инструменты для визуализации данных (Matplotlib, Seaborn).  
 Среды разработки (Jupyter Notebook, Google Colab).

**Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

1. Аудитория для проведения учебных занятий всех типов - 0419.
2. Компьютер - 13 шт.
3. Проектор - 1 шт.
4. Интерактивная доска - 1 шт.

4. Доска аудиторная настенная - 1 шт.
5. Комплект учебной мебели на 13 посадочных мест.



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФГБОУ ВО «БУРЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИМЕНИ ДОРЖИ БАНЗАРОВА»  
Институт математики, физики и компьютерных наук  
Кафедра вычислительной техники и информатики

**Фонд оценочных средств по дисциплине  
Основы криптографии**

Направление подготовки/ специальность  
**09.04.02**– Информационные системы и технологии

Профиль подготовки /специализация  
Проектирование, разработка и эксплуатация информационных систем

Квалификация (степень) выпускника  
Магистр

Форма обучения  
очная

Улан-Удэ  
2025

**Паспорт**  
**фонда оценочных средств**  
**по учебной дисциплине «Основы криптографии»**  
**09.04.02 – Информационные системы и технологии**

№	Контролируемые разделы, темы, модули <sup>1</sup>	Наименование компетенции	Этапы формирования	Оценочные средства	Количество
1	Введение в криптографию	УК-1.1 УК-1.3	3 семестр	Отчет по лабораторной работе	1
2	Криптографические алгоритмы	ПК-1.1	3 семестр	Отчет по лабораторной работе	4
3	Алгоритмы хеширования. Протоколы аутентификации и электронной подписи	ПК-1.1	3 семестр	Отчет по лабораторной работе	1
По всему курсу				Тест Доклад	1 1

<sup>1</sup>Наименования разделов, тем, модулей соответствуют рабочей программе дисциплины.

УК-1.1 — анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.

УК-1.3 — критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников.

ПК-1.1 — Назначает и распределяет ресурсы в рамках управления работами по сопровождению и проектами создания (модификации) ИС.

## Вопросы к экзамену

1. Основные понятия криптографии: шифрование, дешифрование, ключ, алгоритм, криптографическая стойкость, криптоанализ.
2. Виды криптографических систем: симметричные и асимметричные.
3. Основные задачи криптографии: конфиденциальность, целостность, аутентификация, неотказуемость.
4. Криптографические стандарты и протоколы.
5. Шифры подстановки: шифр Цезаря, шифр простой подстановки, полиалфавитные шифры (Виженера, Бофорта).
6. Шифры перестановки.
7. DES (Data Encryption Standard): структура, режимы работы.
8. AES (Advanced Encryption Standard): структура, режимы работы.
9. Режимы работы блочных шифров (ECB, CBC, CTR, OFB): преимущества и недостатки.
10. RSA (Rivest-Shamir-Adleman): принцип работы, безопасность.
11. Алгоритмы на основе эллиптических кривых (ECC): принцип работы, преимущества.
12. Диффи-Хеллман (Diffie-Hellman): принцип работы, применение.
13. Свойства хеш-функций: однонаправленность, стойкость к коллизиям.
14. Алгоритмы хеширования: MD5, SHA-1, SHA-256, SHA-3.
15. Применение хеш-функций: контроль целостности данных, хранение паролей, цифровая подпись.
16. Протоколы аутентификации: Kerberos, RADIUS.
17. Электронная подпись: ГОСТ Р 34.10-2012, RSA, DSA.
18. Инфраструктура открытых ключей (PKI).
19. Атаки на криптографические системы.
20. Области применения криптографии в информационных технологиях.

### Критерии и шкала оценивания устного ответа:

№ n/n	Характеристика ответа	Баллы	Зачет
1.	- дается комплексная оценка предложенной ситуации; - демонстрируются глубокие знания теоретического материала и умение их применять; - последовательное, правильное выполнение всех заданий; - умение обоснованно излагать свои мысли, делать необходимые выводы	9-10	отлично
2.	- дается комплексная оценка предложенной ситуации; - демонстрируются глубокие знания теоретического материала и умение их применять; - последовательное, правильное выполнение всех заданий; - возможны единичные ошибки, исправляемые самим студентом после замечания преподавателя; - умение обоснованно излагать свои мысли, делать необходимые выводы	7-8	хорошо
3	- затруднения с комплексной оценкой предложенной ситуации; - неполное теоретическое обоснование, требующее наводящих вопросов преподавателя;	4-6	удовлетв

	<ul style="list-style-type: none"> <li>- выполнение заданий при подсказке преподавателя;</li> <li>- затруднения в формулировке выводов</li> </ul>		
4.	<ul style="list-style-type: none"> <li>- неправильная оценка предложенной ситуации;</li> <li>- отсутствие теоретического обоснования выполнения заданий</li> </ul>	3 и менее	неудовл

### Практические задания (проекты)

1. Зашифровать сообщение с помощью шифра Цезаря с заданным ключом.
2. Зашифровать сообщение с помощью шифра Виженера с заданным ключом.
3. Расшифровать сообщение, зашифрованное с помощью шифра Цезаря.
4. Расшифровать сообщение, зашифрованное с помощью шифра Виженера.
5. Реализовать хеш-функцию для вычисления хеша заданной строки.
6. Используя заданные открытый и закрытый ключ RSA, зашифровать и расшифровать сообщение.
7. Используя криптографическую библиотеку, создать и проверить цифровую подпись для заданного файла.
8. Определить, какие криптографические алгоритмы и протоколы следует использовать для обеспечения конфиденциальности и целостности данных при передаче их по сети.

### Критерии и шкала оценивания практического задания:

№ n/n	Характеристика ответа	Баллы
1.	<b>Правильность выбора алгоритма:</b> Обоснованность выбора алгоритма машинного обучения для решения поставленной задачи	5
2.	<b>Корректность кода:</b> Правильность реализации алгоритма (отсутствие синтаксических и логических ошибок)	10
3	<b>Оценка качества модели:</b> Правильность выбора метрик для оценки качества модели и адекватная интерпретация результатов	10
4.	<b>Предобработка данных (если требуется):</b> Правильность выполнения предобработки данных (нормализация, кодирование категориальных признаков и т.д.)	5

## Темы докладов/сообщений

### Общие темы

1. **Влияние криптографии на современное общество:** Рассмотрение влияния криптографии на различные аспекты жизни, включая безопасность, конфиденциальность, коммерцию и политику.
2. **Этические вопросы криптографии:** Дилемма между безопасностью и приватностью, баланс между защитой данных и возможностью их дешифровки правоохранительными органами.
3. **Будущее криптографии:** Обзор перспективных направлений развития криптографии, таких как квантовая и постквантовая криптография, гомоморфное шифрование и др.
4. **Роль криптографии в борьбе с киберпреступностью:** Обзор используемых криптографических методов для защиты от киберугроз и борьбы с киберпреступностью.
5. **История использования криптографии в военных целях:** Обзор ключевых моментов использования криптографии в военной истории, влияние на исход войн.

### Темы, связанные с конкретными алгоритмами и технологиями

6. **Ключевое соглашение Диффи-Хеллмана:** преимущества, недостатки, уязвимости и модификации. (Акцент на практические примеры атак и способов их предотвращения).
7. **Анализ алгоритма шифрования AES:** Детальное описание структуры AES, режимов работы и методов криптоанализа.
8. **Анализ алгоритма RSA:** Особенности выбора ключей, факторы, влияющие на безопасность RSA, практические атаки.
9. **Эллиптическая криптография (ECC):** Преимущества ECC перед RSA, особенности реализации и применения.
10. **Хеш-функции SHA-3:** особенности структуры и преимущества перед SHA-1 и SHA-2.
11. **Электронная подпись на основе ГОСТ Р 34.10-2012:** особенности реализации и применения.
12. **Квантовый алгоритм Шора и его влияние на современную криптографию:** Описание принципов работы алгоритма Шора и анализ угроз для существующих криптосистем.
13. **Криптография на решетках (Lattice-based cryptography):** Принципы работы и перспективы использования в постквантовой криптографии.
14. **Гомоморфное шифрование: методы реализации и области применения.** (Фокус на конкретные примеры применения в реальных задачах, например, в медицине или финансах).

### Темы, связанные с безопасностью и атаками

15. **Атака "человек посередине" (Man-in-the-middle attack):** способы осуществления и методы защиты.
16. **Атаки на основе побочных каналов (Side-channel attacks):** виды, методы обнаружения и предотвращения.
17. **Современные методы взлома паролей:** Обзор методов, используемых для взлома паролей, и рекомендации по созданию надежных паролей.
18. **Фишинг и социальная инженерия в контексте криптографии:** Анализ методов социальной инженерии, используемых для обмана пользователей и получения доступа к криптографическим ключам.
19. **Уязвимости в протоколах TLS/SSL:** Обзор известных уязвимостей в протоколах TLS/SSL и рекомендации по их устранению.

20. **Безопасность облачных хранилищ данных:** Криптографические методы, используемые для защиты данных в облачных хранилищах, анализ угроз.

**Темы, связанные с применением криптографии в различных областях**

21. **Криптография в банковской сфере:** Использование криптографии для защиты банковских транзакций, онлайн-банкинга и банковских карт.

22. **Криптография в электронной коммерции:** Использование криптографии для защиты онлайн-платежей, конфиденциальности данных клиентов и аутентификации пользователей.

23. **Криптография в медицине:** Использование криптографии для защиты конфиденциальности медицинских данных пациентов.

24. **Криптография в государственном управлении:** Использование криптографии для защиты государственных секретов, конфиденциальной информации и обеспечения безопасности государственных информационных систем.

25. **Криптография в Интернете вещей (IoT):** Проблемы безопасности IoT-устройств и использование криптографии для их защиты.

26. **Криптография и цифровая валюта (Bitcoin, Ethereum и др.):** Подробное описание роли криптографии в функционировании криптовалют, включая хеширование, электронные подписи и криптографические протоколы.

При подготовке доклада/сообщения рекомендуется:

- Четко определить цель и задачи доклада.
- Использовать различные источники информации (научные статьи, книги, интернет-ресурсы, статистические данные).
- Приводить примеры из практики социальной работы.
- Учитывать этические и социальные аспекты.
- Предлагать конкретные рекомендации по улучшению использования цифровых сервисов.

*Критерии и шкалы оценивания доклада/сообщения*

Уровень освоения	Критерии	Баллы
Максимальный уровень	– продемонстрировано умение выступать перед аудиторией; – содержание выступления даёт полную информацию о теме; – продемонстрировано умение выделять ключевые идеи; – умение самостоятельно делать выводы, использовать актуальную научную литературу; – высокая степень информативности, компактность слайдов	5
Средний уровень	– продемонстрирована общая ориентация в материале; – достаточно полная информация о теме; – продемонстрировано умение выделять ключевые идеи, но нет самостоятельных выводов; – невысокая степень информативности слайдов; – ошибки в структуре доклада; – недостаточное использование научной литературы	3-4
Минимальный уровень	– продемонстрирована слабая (с фактическими ошибками) ориентация в материале; – ошибки в структуре доклада; – научная литература не привлечена	1-2
Минимальный уровень не достигнут	– выступление не содержит достаточной информации по теме; – продемонстрировано неумение выделять ключевые идеи; – неумение самостоятельно делать выводы, использовать актуальную научную литературу.	0

### Примерные тестовые задания

1. Что такое криптография?
  - а) Наука о создании сложных шифров.
  - б) Наука о методах защиты информации.
  - в) Раздел математики, изучающий функции.
  - г) Раздел информатики, занимающийся базами данных.
2. Какой из перечисленных алгоритмов относится к симметричным алгоритмам шифрования?
  - а) RSA
  - б) DES
  - в) ECC
  - г) Diffie-Hellman
3. Что такое криптоанализ?
  - а) Процесс шифрования данных.
  - б) Процесс расшифрования данных при отсутствии ключа.
  - в) Процесс генерации ключей.
  - г) Процесс создания новых криптографических алгоритмов.
4. Какое свойство является ключевым для хеш-функции?
  - а) Обратимость.
  - б) Стойкость к коллизиям.
  - в) Возможность восстановления исходного сообщения.
  - г) Высокая скорость шифрования.
5. Какой из перечисленных алгоритмов является алгоритмом хеширования?
  - а) AES
  - б) RSA
  - в) SHA-256
  - г) DES
6. Что такое электронная подпись?
  - а) Визуальный образ подписи, добавленный к электронному документу.
  - б) Механизм, позволяющий подтвердить авторство и целостность электронного документа.
  - в) Средство защиты электронной почты от спама.
  - г) Алгоритм сжатия данных.
7. Что такое инфраструктура открытых ключей (PKI)?
  - а) Система управления секретными ключами.
  - б) Система управления открытыми ключами, позволяющая устанавливать доверительные отношения между пользователями.
  - в) Алгоритм шифрования с открытым ключом.
  - г) Метод защиты от DDoS-атак.
8. Какой алгоритм используется в протоколе TLS для обмена ключами?
  - а) DES
  - б) RSA
  - в) AES
  - г) MD5
9. Что такое "атака грубой силой" (brute-force attack)?
  - а) Тип атаки, использующий уязвимости в протоколах.
  - б) Тип атаки, основанный на переборе всех возможных ключей.
  - в) Тип атаки, нацеленный на отказ в обслуживании системы.
  - г) Тип атаки, использующий социальную инженерию.
10. Какая из перечисленных угроз направлена на нарушение целостности данных?
  - а) Прослушивание канала связи.
  - б) Модификация данных.



- в) Отказ в обслуживании.
  - г) Перехват управления системой.
11. Какой режим работы блочного шифра используется для параллельного шифрования?
- а) ECB
  - б) CBC
  - в) CTR
  - г) CFB
12. Какая основная цель использования соли при хранении паролей?
- а) Увеличение скорости хеширования.
  - б) Уменьшение размера хеша.
  - в) Предотвращение атак с использованием радужных таблиц.
  - г) Упрощение процесса восстановления пароля.
13. Какой протокол используется для аутентификации в беспроводных сетях Wi-Fi?
- а) SMTP
  - б) SSH
  - в) WPA2
  - г) HTTP
14. В чем заключается основная идея постквантовой криптографии?
- а) В использовании квантовых компьютеров для шифрования.
  - б) В создании алгоритмов, устойчивых к атакам квантовых компьютеров.
  - в) В использовании более сложных алгоритмов шифрования.
  - г) В создании алгоритмов, которые работают быстрее, чем существующие.
15. Какое свойство отличает гомоморфное шифрование от обычного?
- а) Более высокая скорость шифрования.
  - б) Возможность выполнения операций над зашифрованными данными.
  - в) Возможность сжатия данных без расшифровки.
  - г) Более высокая криптостойкость.
16. Какую роль играет криптография в технологии блокчейн?
- а) Обеспечение безопасности транзакций и идентификации пользователей.
  - б) Управление распределенной базой данных.
  - в) Оптимизация скорости работы сети.
  - г) Сжатие данных, хранящихся в блокчейне.
17. Что такое атака "дней рождения" (birthday attack)?
- а) Атака на алгоритмы шифрования.
  - б) Атака на хеш-функции, основанная на поиске коллизий.
  - в) Атака на протоколы аутентификации.
  - г) Атака на системы контроля доступа.
18. Для чего используется соль в контексте криптографии?
- а) Для усиления стойкости к солевым атакам
  - б) Для усиления стойкости к словарным атакам
  - в) Для ускорения процесса шифрования
  - г) Для усложнения структуры алгоритма шифрования
19. Какой из перечисленных протоколов предназначен для безопасной передачи гипертекста?
- а) HTTP
  - б) FTP
  - в) HTTPS
  - г) SMTP
20. Какой алгоритм обычно используется для шифрования дисков и разделов жесткого диска?
- а) RSA
  - б) AES

в) SHA-256

г) MD5

**Оценивание тестовых заданий – максимальный балл - 5:**

Баллы для учета в рейтинге	Степень удовлетворения критериям
5 баллов	количество правильных ответов >85%
4 балла	количество правильных ответов 70..84%
3 балла	количество правильных ответов 60..69%
2 балла	количество правильных ответов 40..59%
1 балл	количество правильных ответов 20..39%
0 баллов	количество правильных ответов 0..19%

### **Лабораторные работы**

1. Реализация шифра Цезаря на выбранном языке программирования.
2. Реализация полиалфавитного шифра (Виженера) на выбранном языке программирования.
3. Реализация блочного шифра DES или AES (упрощенная версия) на выбранном языке программирования.
4. Использование криптографической библиотеки для шифрования данных с помощью AES.
5. Реализация алгоритма RSA (упрощенная версия) на выбранном языке программирования.
6. Использование криптографической библиотеки для создания и проверки электронной подписи.

### **Правила выполнения и защиты практических работ**

Практические занятия проводятся в компьютерном классе. Каждая работа засчитывается при удовлетворении всем требованиям протокола оценки и может быть оценена в зависимости от срока защиты. Для допуска к зачету должны быть сданы все работы.

Отчет состоит из следующих разделов:

#### **1. Титульный лист**

На титульном указываем название образовательного учреждения, кафедры, работы, ФИО студента (по всем правилам оформления титульного листа работ).

#### **2. Введение**

Во введении указываются цели работы (из описания заданий в практических работах) и используемые ОС.

#### **3. Постановка задачи**

Формулируется постановка задачи своего варианта задания, где даются задания для выполнения.

#### **4. Выполнение заданий**

Приводятся результаты выполнения заданий своего варианта. Графический материал оформляется в соответствии с ГОСТ.

#### **5. Выводы**

Приводятся выводы по выполненной работе.

Работы, не соответствующие вышеперечисленным требованиям к защите не допускаются.

#### **Критерии оценки:**

«5» (4,5-5 балла) - правильные ответы на вопросы + правильно оформленный отчет;

«4» (3,5-4,4 баллов) - неполные ответы на вопросы + правильно оформленный отчет;

«3» (2,5-3,4 баллов) - правильный или неполный ответ на один вопрос + правильно оформленный отчет;

«2 или неуд» (0-2,4 баллов) - нет правильных ответов на вопросы.

#### **Снижение баллов:**

*Минус 0,3 балл за:*

- отсутствие правильно оформленного отчета по работе на момент начала работы;
- отсутствие выполненной работы (заполненный отчет, собранные схемы) к концу пары;
- отсутствие на паре без уважительной причины (без предупреждения преподавателя) минимум за 24 ч до начала пары;

*Минус 0,2 балла за:*

- каждую дополнительную попытку защиты;
- опоздание более чем на 15 мин;

- защиту работы позднее второго занятия после ее выполнения.

*Примечание:* при наборе  $\leq$  «2» балла студент не может получить оценку за работу выше «3». В этом случае для получения оценки «3» необходимо защитить работу на «5», иначе оценка «неуд».

Если вы НЕ отвечаете на поставленные вопросы, другой вопрос попросить «чтобы еще разок попробовать» СЕГОДНЯ НЕЛЬЗЯ.

Защита проделанных работ осуществляется в порядке их возрастания. При неудачной попытке защитить работу № N, «попробовать» защитить работу N+1 нельзя.

Составитель \_\_\_\_\_ Т.С. Цыбикова  
(подпись)

« \_\_\_\_ » \_\_\_\_\_ 202\_ г.