

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ИНГУШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**ФИЗИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра «Информационные системы и технологии»**

СОГЛАСОВАНО

Руководитель образовательной программы

_____/М.Х. Мальсагов
от «03» марта 2025г.

УТВЕРЖДАЮ

И.о. декана физико-математического
факультета

_____/Б.С.Кульбужев
от «14» марта 2025г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.06.01 Постквантовая криптография и основы современных методов криптографии

Направление подготовки

09.03.02 Информационные системы и технологии

Направленность (профиль подготовки)

Безопасность информационных систем

Квалификация выпускника

Бакалавр

Форма обучения

Очная, очно-заочная

Магас, 2025г.

Цели и задачи освоения дисциплины «Постквантовая криптография и основы современных методов криптографии»

- Целью дисциплины является формирование у студентов теоретических знаний и практических навыков, необходимых для:
 - понимания основ современных криптографических алгоритмов и протоколов, включая симметричные и асимметричные методы защиты информации;
 - изучения угроз, возникающих в связи с развитием квантовых вычислений, и освоения принципов постквантовой криптографии как одного из направлений противодействия данным угрозам;
 - анализа, выбора и применения криптографических решений в информационных системах с учётом их устойчивости к потенциальным квантовым атакам;
 - практического применения современных и постквантовых криптографических алгоритмов в задачах обеспечения конфиденциальности, целостности и подлинности данных;
 - освоения подходов к проектированию и внедрению криптографических механизмов в реальных ИТ-инфраструктурах и протоколах связи.

- Код и - наименова ние профессион ально го - стандарта	Обобщенные трудовые функции			Трудовые функции		
	Код	Наименование	Урове нь квали фикац ии	Наименование	Код	Уровень (подуров ень) квалифи кации
06.026 Системный администратор информационно-коммуникационных систем	D	Обслуживание серверных операционных систем информационно-коммуникационной системы	6	Выполнение работ по выявлению и устранению нетипичных инцидентов, возникающих в серверных операционных системах информационно-коммуникационной системы	D/01.6	6
				Проведение анализа и определение основных причин сложных проблем, возникающих на серверах и в серверных операционных системах	D/02.6	6

			Выполнение планирования резервного копирования, архивирования и восстановления конфигурации серверов и серверных операционных систем	D/03.6	6
			Планирование изменений параметров работы серверов и серверных операционных систем	D/04.6	6
			Выполнение обновления программного обеспечения серверных операционных систем	D/05.6	6
			Прогнозирование влияния внешних и внутренних воздействий на поведение серверных операционных систем	D/06.6	6
			Прогнозирование потребности в изменении объемов необходимых ресурсов для обеспечения бесперебойной работы серверов и серверных операционных систем	D/07.6	6
			Планирование и проведение работ по распределению нагрузки между имеющимися ресурсами, снятию нагрузки на серверы и серверные операционные системы перед проведением регламентных работ, восстановлению штатной схемы работы в случае сбоев	D/08.6	6
			Определение потребностей в приобретении специализированных средств контроля и тестирования серверов и серверных операционных систем	D/09.6	6

Место учебной дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Постквантовая криптография и основы современных методов криптографии» относится к профессиональному циклу дисциплин, является дисциплиной по выбору.

Для освоения данной дисциплины необходимы знания, умения и компетенции, полученные обучающимися при изучении курсов «Математическая логика», «Дискретная математика», «Теория алгоритмов», «Информационная безопасность», «Программирование», «Операционные системы».

Дисциплина обеспечивает теоретическую и прикладную базу для последующего изучения специализированных курсов в области криптографической защиты информации и построения безопасных информационных систем.

В результате освоения дисциплины обучающийся должен:

Знать:

- принципы построения современных криптографических алгоритмов и протоколов (симметричных, асимметричных, хеш-функций, протоколов распределения ключей и цифровой подписи);
- математические основы криптографии, включая теорию чисел, алгебраические структуры и комбинаторику;
- угрозы, возникающие в связи с развитием квантовых вычислений (алгоритмы Шора и Гровера);
- классификацию и особенности постквантовых криптографических алгоритмов (решётки, хеш-криптография, мультивариантные и кодовые методы);
- нормативные и международные стандарты в области криптографической защиты информации.

Уметь:

- анализировать стойкость криптографических решений с учётом квантовой модели атакующего;
- применять криптографические алгоритмы в типовых задачах защиты информации (конфиденциальность, аутентификация, целостность);
- разрабатывать и реализовывать криптографические протоколы с использованием современных и постквантовых алгоритмов;
- использовать программные библиотеки и средства для реализации криптографических решений в программных продуктах и ИТ-системах;
- оценивать уязвимости криптографических механизмов и предлагать меры по их устранению.

Владеть:

- практическими навыками работы с криптографическими библиотеками (например, OpenSSL, libsodium, NIST PQC API);
- методами построения защищённых коммуникационных каналов на базе криптографии;
- средствами внедрения криптографической защиты в архитектуру информационных систем;
- навыками применения постквантовых алгоритмов в условиях практических ограничений (производительность, совместимость, масштабируемость).

Процесс изучения дисциплины направлен на формирование следующих компетенций:

<p>ПК-7. Способен к коммуникации и кооперации в цифровой среде, использованию различных цифровых средств, позволяющих во взаимодействии с другими людьми достигать поставленных целей</p>	<p>ПК-7.1 Знать: основные характеристики коммуникационных процессов в цифровой среде, включая глобальные информационно-коммуникационные сети. ПК-7.2 Уметь: выбирать и использовать средства цифровой коммуникации исходя из решаемых задач. ПК-7.3 Имеет навыки: осуществлять деловых и межличностных коммуникаций в цифровой среде, в том числе с использованием интернет технологий</p>
<p>УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде.</p>	<p>УК-3.1. Знать: основные приемы и нормы социального взаимодействия; основные понятия и методы конфликтологии, технологии межличностной и групповой коммуникации в деловом взаимодействии.</p>
	<p>УК-3.2. Уметь: устанавливать и поддерживать контакты, обеспечивающие успешную работу в коллективе; применять основные методы и нормы социального взаимодействия для реализации своей роли и взаимодействия внутри команды.</p>
	<p>УК-3.3. Владеть: простейшими методами и приемами социального взаимодействия и работы в команде.</p>

Структура и содержание дисциплины

Постквантовая криптография и основы современных методов криптографии

Структура дисциплины (модуля) Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

	Всего	Порядковый номер семестра		
		7		
Общая трудоемкость дисциплины, в том числе:	108			
Курсовой проект (работа)				
Аудиторные занятия всего В том числе:		+		
Лекции	16	+		
Практические занятия, семинары		+		
Лабораторные работы	16			
Самостоятельная работа	76	+		
Вид итоговой аттестации:				
Зачет/дифф.зачет		+		
К.С.Р.				
Экзамен				
Общая трудоемкость дисциплины	144			

Наименование разделов и тем дисциплины и распределение учебных часов

№	Наименование разделов и тем	Лекции (ч)	Практические занятия (ч)	Самостоятельная работа (ч)
1	Введение в криптографию. Роль криптографии в обеспечении информационной безопасности	2	–	4
2	Математические основы современной криптографии (модульная арифметика, решётки, многочлены)	2	2	10
3	Современные криптографические методы: симметричные и асимметричные алгоритмы	2	2	8
4	Угрозы квантовых вычислений. Алгоритмы Шора и Гровера	2	–	8
5	Основы постквантовой криптографии. Классификация и принципы работы PQ-алгоритмов	2	2	8
6	Криптография на основе решёток (NTRU, Kyber, Saber и др.)	2	2	10
7	Хеш-криптография, кодовые и мультивариантные алгоритмы (SPHINCS+, Rainbow и др.)	2	2	10
8	Применение постквантовой криптографии в ИС: протоколы, библиотеки, стандарты NIST PQC	2	2	10
9	Проектная работа: анализ и реализация криптографической подсистемы	–	2	8
	Итого	16	16	76

Содержание учебной дисциплины

Тема 1: Введение в криптографию и её роль в ИБ

Содержание темы:

- **История развития криптографии:** от классических методов до квантовых угроз.
- **Роль криптографии в обеспечении конфиденциальности, целостности и аутентичности данных.**
- **Классификация криптографических методов:** симметричные, асимметричные, хеш-функции.

Формы и методы проведения занятий:

- **Лекция с презентацией.**

- Обсуждение современных криптографических инцидентов.
 - Лабораторная работа №1:
Ознакомление с криптобиблиотекой cryptography (Python). Генерация и шифрование симметричного ключа.
-

Тема 2: Математические основы криптографии

Содержание темы:

- Арифметика по модулю, группы, поля, решётки.
- Сложность задач: факторизация, дискретный логарифм, ближайший вектор.
- Алгоритмы Шора и Гровера: квантовые угрозы классическим алгоритмам.

Формы и методы проведения занятий:

- Лекция с элементами математического моделирования.
 - Решение задач по ручному вычислению.
 - Лабораторная работа №2:
Реализация в Python простых операций модульной арифметики.
Визуализация примера с решётками.
-

Тема 3: Современные криптографические методы

Содержание темы:

- Симметричные алгоритмы: AES, ChaCha20.
- Ассиметричные алгоритмы: RSA, DSA, ElGamal.
- Стандарты и применение (TLS, VPN, PKI).

Формы и методы проведения занятий:

- Лекция с разбором алгоритмов.
 - Анализ криптографических протоколов.
 - Лабораторная работа №3:
Реализация шифрования/дешифрования с помощью AES и RSA
(библиотека cryptography, pyca).
-

Тема 4: Основы постквантовой криптографии (PQC)

Содержание темы:

- **Введение в постквантовую криптографию. Обоснование необходимости.**
- **Классы постквантовых алгоритмов: решёточные, хеш-криптография, кодовые, мультивариантные.**
- **Обзор конкурса NIST PQC и финалистов.**

Формы и методы проведения занятий:

- **Лекция с примерами протоколов.**
- **Просмотр и разбор стандартов NIST.**
- **Лабораторная работа №4:**
Установка и работа с библиотекой pqcrypto. Использование Kyber для шифрования сообщений.

Тема 5: Решётки и кодовые алгоритмы

Содержание темы:

- **Алгоритмы на основе решёток: NTRU, Kyber, Saber.**
- **Алгоритмы на основе кодов: BIKE, Classic McEliece.**
- **Преимущества и недостатки.**

Формы и методы проведения занятий:

- **Лекция с разбором схем.**
- **Анализ криптостойкости.**
- **Лабораторная работа №5:**
Сравнение скорости и объёма ключей в NTRU и Kyber. Тестирование на практических примерах.

Тема 6: Хеш-криптография и цифровые подписи

Содержание темы:

- **Многоразовые и одноразовые подписи. SPHINCS+, Picnic.**
- **Хеш-функции и стойкость к коллизиям.**
- **Внедрение цифровых подписей в документооборот.**

Формы и методы проведения занятий:

- **Лекция с демонстрацией.**
- **Обсуждение кейсов (электронная подпись, eIDAS).**

- **Лабораторная работа №6:**

Реализация хеширования с помощью SHA-3 и подписание сообщения с SPHINCS+ (с помощью oqs-python).

Тема 7: Применение постквантовой криптографии

Содержание темы:

- **Интеграция PQC в протоколы TLS, VPN, SSH.**
- **Анализ совместимости и рисков внедрения.**
- **Международные инициативы и стандарты.**

Формы и методы проведения занятий:

- **Лекция с анализом практических кейсов.**
- **Работа с протоколами связи.**
- **Лабораторная работа №7:**

Установка и использование OpenSSL с поддержкой PQC (OQS OpenSSL).

Генерация ключей Kyber и реализация шифрованного соединения.

Тема 8: Проектная деятельность

Содержание темы:

- **Планирование проекта по реализации защищённого обмена данными.**
- **Использование PQ-алгоритмов в реальных задачах.**
- **Презентация и защита проектов.**

Формы и методы проведения занятий:

- **Консультации и работа в группах.**
- **Анализ задач безопасности в организациях.**
- **Лабораторная работа №8:**

Разработка собственного криптографического протокола на базе постквантовых алгоритмов. Документация и защита проекта.

Экзаменационные вопросы по дисциплине

- 1. Понятие криптографии и её роль в обеспечении информационной безопасности.**
- 2. Классификация криптографических методов: симметричные, асимметричные, хеш-функции.**
- 3. Современные угрозы криптографии: влияние квантовых вычислений.**
- 4. Принцип работы симметричных алгоритмов шифрования (на примере AES, ChaCha20).**
- 5. Основы асимметричной криптографии: алгоритмы RSA, ElGamal, Diffie-Hellman.**
- 6. Применение хеш-функций в криптографии: свойства и устойчивость.**
- 7. Математические основы криптографии: модульная арифметика, поля, решётки.**
- 8. Квантовые алгоритмы Шора и Гровера: их влияние на безопасность современных систем.**
- 9. Постквантовая криптография: цели, задачи и подходы.**
- 10. Обзор финалистов конкурса NIST по постквантовой криптографии.**
- 11. Решётко-ориентированные алгоритмы: Kyber, Saber, NTRU – особенности и применение.**
- 12. Криптография на основе кодов: McEliece, BIKE – принципы работы.**
- 13. Мультивариантные и хеш-подписи: SPHINCS+, Picnic и их особенности.**
- 14. Преимущества и недостатки постквантовых алгоритмов в сравнении с классическими.**
- 15. Безопасность цифровых подписей в условиях квантовой угрозы.**
- 16. Практическое применение PQ-алгоритмов в VPN, TLS, SSH.**
- 17. Обзор библиотек и инструментов для работы с PQC (например, liboqs, pqcrypto).**
- 18. Основы использования PQ-алгоритмов в протоколах обмена ключами.**
- 19. Форматы и объёмы ключей в постквантовых алгоритмах: проблемы совместимости.**
- 20. Принципы перехода организаций на криптографию, стойкую к квантовым**

атакам.

- 21. Угрозы при реализации криптографических алгоритмов: побочные каналы, ошибки реализации.**
- 22. Аудит и тестирование криптографических протоколов.**
- 23. Этапы внедрения криптографической защиты в ИС: от проектирования до контроля.**
- 24. Пример интеграции постквантовых алгоритмов в существующую систему (кейсы).**
- 25. Применение PQС в электронных подписях и документообороте.**
- 26. Проблемы стандартизации и международной координации в области PQС.**
- 27. Пример атаки на классический алгоритм и устойчивость аналогичного PQ-решения.**
- 28. Обзор новых протоколов и архитектур, адаптированных под PQС.**
- 29. Этические и правовые аспекты внедрения новых криптографических стандартов.**
- 30. Перспективы развития криптографии в условиях массового появления квантовых вычислений.**

**Перечень основной и дополнительной учебной литературы,
Необходимой для освоения дисциплины**

1. Угрюмов, Евгений Павлович. Цифровая схемотехника : учебное пособие / Е. П. Угрюмов. - 2-е изд., перераб. и доп. - СПб. : БХВ - Петербург, 2007. - 782 с
2. Зиатдинов, Сергей Ильич (проф.). Схемотехника телекоммуникационных устройств [Текст] : учебник / С. И. Зиатдинов, Т. А. Суетина, Н. В. Поваренкин. - М. : Академия, 2013. - 368 с
3. Шишмарев, В. Ю. Основы автоматического управления [Текст] : учебное пособие / В. Ю. Шишмарев. - М. : Академия, 2008. - 352 с
4. Технические средства автоматизации и управления: Учебное пособие / Шишов О.В. - М.: НИЦ ИНФРА-М, 2016. - 396 с

Перечень ресурсов информационно-телекоммуникационной сети

«Интернет»

1. <http://mexalib.com/view/2880> - Петров И.В. Программируемые контроллеры. Стандартные языки и приемы прикладного проектирования. 2004
2. <http://freecomputerbooks.com/AutomatingManufacturing-Systems-with-PLCs.html> <http://www.razym.ru/79485-programmiruemye-kontrollery-rukovodstvo-dlya.html> Э. Папп - Программируемые контроллеры: руководство для инженера. 200
3. <https://www.arduino.cc/>

Перечень информационных технологий

Для проведения лекционных и лабораторных занятий рекомендуется использовать программное обеспечение: операционная система Linux с ядром 3.2 и выше, обслуживающие программы и среды разработки программ по выбору преподавателей.

Электронная поддержка дисциплины

При изучении дисциплины для проработки всех тем и выполнения заданий по всем темам студенты могут использовать различные учебно-методические материалы, размещаемые в электронном виде преподавателями на файловом ftp- сервере, в хранилище полнотекстовых материалов, а также в электронной образовательной среде, которая предполагает также возможность обмена информацией с преподавателем для подготовки заданий. Доступ студентов к студенческому файловому серверу, хранилищу полнотекстовых материалов, электронной образовательной среде осуществляется с использованием с использованием учетных записей студентов.

Рабочая программа дисциплины «Цифровые системы автоматизации и управления» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.02 «Информационные системы и технологии», утвержденного приказом Министерства образования и науки Российской Федерации от «__19__» сентября 2017 г. No 926(ред.8.02.2021).

Программу составили: ст. препод. кафедры «Информационные системы и технологии» Аушев А.А.

Программа одобрена на заседании кафедры «Информационные системы и технологии»

Протокол №6 от «03» марта 2025 года

Программа одобрена Учебно-методическим советом физико-математического факультета

Протокол №7 от «13» марта 2025 года

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата)	Внесенные изменения	Подпись зав. кафедрой

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Б1.В.ДВ.06.01 Постквантовая криптография и основы современных методов
криптографии**

Направление подготовки

09.03.02 Информационные системы и технологии

-

Направленность (профиль подготовки)

Безопасность информационных систем

Квалификация выпускника

Бакалавр

Форма обучения

Очная,очно-заочная

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Типовой тест промежуточной аттестации

1. Что из перечисленного относится к **асимметричным криптографическим алгоритмам**?
a) AES
+ **b) RSA**
c) SHA-256
d) DES
2. Какая криптосистема основана на **решении задачи о дискретном логарифме**?
a) AES
+ **b) ElGamal**
c) RSA
d) McEliece
3. Какой из следующих алгоритмов является кандидатом в стандарты NIST по **постквантовой криптографии**?
a) SHA-1
b) RSA
+ **c) Kyber**
d) DES
4. Алгоритм хеширования SHA-3 относится к:
a) Симметричным алгоритмам
b) Протоколам шифрования
+ **c) Криптографическим хеш-функциям**
d) Алгоритмам цифровой подписи
5. Какой алгоритм **стойкий к атакам квантового компьютера**?
a) RSA
b) ECC
+ **c) Crystals-Kyber**
d) Diffie-Hellman
6. Какой тип уязвимости наиболее актуален для классических криптосистем при появлении квантовых вычислений?
a) SQL-инъекция
+ **b) Криптоанализ с использованием квантового компьютера**
c) XSS
d) Буферный переполнение
7. К какому классу относится криптосистема McEliece?
a) Хеш-функции
b) Алгоритмы на основе факторизации
+ **c) Кодовые криптосистемы**
d) Симметричные алгоритмы
8. Что является основной задачей алгоритма цифровой подписи?
a) Шифрование данных
+ **b) Проверка подлинности и целостности данных**
c) Сжатие данных
d) Защита от вирусов
9. Какой из алгоритмов не является постквантовым?
a) Kyber
+ **b) RSA**
c) Dilithium
d) SPHINCS+
10. Какой криптографический метод обеспечивает **двустороннюю секретность** при передаче данных?
+ **a) Протокол Диффи–Хеллмана**
b) Хеш-функция

- c) Электронная подпись
- d) DES

Типовой вариант задания на контрольную работу

Часть 1. Теоретическая (ответить письменно на 3 из 5 вопросов по выбору)

1. Сравните основные симметричные и асимметричные алгоритмы шифрования по принципам действия, скорости и устойчивости к взлому.
 2. Объясните криптографические риски, связанные с появлением квантовых компьютеров. Какие алгоритмы под угрозой?
 3. Дайте определение постквантовой криптографии. Назовите и кратко охарактеризуйте 2–3 современных постквантовых алгоритма.
 4. Что такое криптографическая хеш-функция? Каковы её основные свойства?
 5. В чём состоит принцип работы алгоритма цифровой подписи? Какие угрозы он нейтрализует?
-

Часть 2. Практическая

Выберите **одно** из заданий и выполните его:

Вариант А (теоретико-аналитический):

Проведите сравнительный анализ следующих алгоритмов:

- RSA (асимметричный, устаревающий);
- Crystals-Kyber (постквантовый);
- AES (симметричный).

Сравните их:

- по области применения;
- алгоритмической стойкости;
- устойчивости к квантовым атакам;
- скорости и ресурсозатратности.

Оформите вывод в таблице + краткое пояснение (1–2 абзаца).

Вариант Б (практико-прикладной):

С помощью библиотеки [Python cryptography, PyCryptodome или аналогичной] реализуйте:

- Шифрование и дешифрование строки с помощью алгоритма AES.
- Моделирование цифровой подписи (используйте RSA или Ed25519).
- Сформулируйте, какие уязвимости могут возникнуть при передаче зашифрованных данных через незащищённый канал и как их можно минимизировать с учётом требований постквантовой безопасности.

Экзаменационные вопросы по дисциплине

- 31. Понятие криптографии и её роль в обеспечении информационной безопасности.**
- 32. Классификация криптографических методов: симметричные, асимметричные, хеш-функции.**
- 33. Современные угрозы криптографии: влияние квантовых вычислений.**
- 34. Принцип работы симметричных алгоритмов шифрования (на примере AES, ChaCha20).**
- 35. Основы асимметричной криптографии: алгоритмы RSA, ElGamal, Diffie-Hellman.**
- 36. Применение хеш-функций в криптографии: свойства и устойчивость.**
- 37. Математические основы криптографии: модульная арифметика, поля, решётки.**
- 38. Квантовые алгоритмы Шора и Гровера: их влияние на безопасность современных систем.**
- 39. Постквантовая криптография: цели, задачи и подходы.**
- 40. Обзор финалистов конкурса NIST по постквантовой криптографии.**
- 41. Решётко-ориентированные алгоритмы: Kyber, Saber, NTRU – особенности и применение.**
- 42. Криптография на основе кодов: McEliece, BIKE – принципы работы.**
- 43. Мультивариантные и хеш-подписи: SPHINCS+, Picnic и их особенности.**
- 44. Преимущества и недостатки постквантовых алгоритмов в сравнении с классическими.**
- 45. Безопасность цифровых подписей в условиях квантовой угрозы.**
- 46. Практическое применение PQ-алгоритмов в VPN, TLS, SSH.**
- 47. Обзор библиотек и инструментов для работы с PQC (например, liboqs, pqcrypto).**
- 48. Основы использования PQ-алгоритмов в протоколах обмена ключами.**
- 49. Форматы и объёмы ключей в постквантовых алгоритмах: проблемы совместимости.**
- 50. Принципы перехода организаций на криптографию, стойкую к квантовым атакам.**

- 51. Угрозы при реализации криптографических алгоритмов: побочные каналы, ошибки реализации.**
- 52. Аудит и тестирование криптографических протоколов.**
- 53. Этапы внедрения криптографической защиты в ИС: от проектирования до контроля.**
- 54. Пример интеграции постквантовых алгоритмов в существующую систему (кейсы).**
- 55. Применение PQС в электронных подписях и документообороте.**
- 56. Проблемы стандартизации и международной координации в области PQС.**
- 57. Пример атаки на классический алгоритм и устойчивость аналогичного PQ-решения.**
- 58. Обзор новых протоколов и архитектур, адаптированных под PQС.**
- 59. Этические и правовые аспекты внедрения новых криптографических стандартов.**
- 60. Перспективы развития криптографии в условиях массового появления квантовых вычислений.**

Типовая лабораторная работа по дисциплине "

Лабораторная работа №1

Тема: Основы симметричного шифрования и использование алгоритма AES

Цель работы:

Познакомиться с принципами симметричного шифрования, научиться использовать алгоритм AES для шифрования и дешифрования данных.

Задачи:

- Изучить структуру и основные характеристики алгоритма AES.
 - Освоить работу с криптографическими библиотеками (например, PyCryptodome для Python).
 - Научиться реализовывать шифрование и дешифрование строк.
 - Понять важность правильного выбора ключа и режима работы.
-

Оборудование и ПО:

- Персональный компьютер с установленным Python 3.x
 - Установленная библиотека PyCryptodome (установка: `pip install pycryptodome`)
 - Текстовый редактор или IDE (например, VS Code, PyCharm)
-

Ход работы:

1. Теоретический блок:

- Кратко изучите алгоритм AES (блоки, ключи, режимы шифрования CBC, ECB и т.д.).
- Объясните, почему симметричное шифрование быстрее асимметричного.

2. Практическая часть:

python

КопироватьРедактировать

```
from Crypto.Cipher import AES
from Crypto.Random import get_random_bytes
from Crypto.Util.Padding import pad, unpad
```

```
# Ключ должен быть 16, 24 или 32 байта
```

```
key = get_random_bytes(16)
```

```
# Исходное сообщение
```

```
data = b'Hello, post-quantum cryptography!'
```

```
# Создаем шифратор в режиме CBC
```

```
cipher = AES.new(key, AES.MODE_CBC)
```

```
# Шифруем с добавлением паддинга
```

```
ciphertext = cipher.encrypt(pad(data, AES.block_size))
```

```
print("Зашифрованные данные:", ciphertext.hex())
```

```
# Для расшифровки нам нужен IV (вектор инициализации)
```

```
iv = cipher.iv
```

```
# Создаем дешифратор
```

```
decipher = AES.new(key, AES.MODE_CBC, iv)
```

```
# Расшифровываем с удалением паддинга
```

```
plaintext = unpad(decipher.decrypt(ciphertext), AES.block_size)
```

```
print("Расшифрованные данные:", plaintext.decode())
```

3. Анализ результатов:

- Проверьте, что расшифрованные данные совпадают с исходными.
 - Обсудите роль ключа и вектора инициализации.
 - Какие угрозы могут возникнуть при повторном использовании ключа или IV?
-

Вопросы для самопроверки:

1. Что такое симметричное шифрование и в чем его отличие от асимметричного?
 2. Какие режимы работы AES существуют и чем они отличаются?
 3. Почему нельзя использовать одинаковый вектор инициализации для разных сообщений?
 4. Какова длина ключа AES и как это влияет на безопасность?
-

Отчёт по лабораторной работе:

В отчёте укажите:

- Цель и задачи работы.
- Краткие теоретические сведения по AES.
- Код программы с комментариями.
- Результаты работы и их анализ.
- Ответы на вопросы для самопроверки.