**УДК 003.54**

**Эволюция криптографии: от шифра Цезаря до постквантовых алгоритмов**

**Болотбеков Н.Ш,** студент 1 курса

*Научный руководитель:* ***Пономарев С.В****., к. ф.-м. н., доцент*

*Калужский филиал Финуниверситета, Калуга*

**Аннотация**. В статье исследуется эволюция криптографии — от древних методов шифрования до современных алгоритмов, устойчивых к атакам квантовых компьютеров. Рассмотрены ключевые этапы развития: появление симметричных и асимметричных систем, внедрение стандартов AES и RSA, а также вызовы, связанные с квантовыми вычислениями. Особое внимание уделено перспективам постквантовой криптографии и её роли в защите данных будущего.

**Ключевые слова:** криптография, шифр Цезаря, RSA, AES, блокчейн, квантовые вычисления.

Криптография, как наука о защите информации, сопровождает человечество на протяжении тысячелетий. Её эволюция отражает непрерывную борьбу между создателями шифров и теми, кто стремится их взломать. В условиях цифровой эпохи, когда данные стали ключевым ресурсом, понимание истории криптографии позволяет оценить современные технологии и спрогнозировать будущие тренды в области информационной безопасности.

История криптографии началась с простых методов замены и перестановки символов. Одним из первых известных шифров стал шифр Цезаря (I век до н.э.), где каждая буква заменялась на другую, смещённую на фиксированное число позиций в алфавите. Несмотря на примитивность, этот метод использовался для защиты военных и дипломатических сообщений.

В Древней Греции применялось устройство «Скитала» — цилиндр, на который наматывалась лента с текстом. Без аналогичного цилиндра прочитать сообщение было невозможно. Эти ранние методы, однако, легко взламывались при наличии частотного анализа, разработанного арабским учёным Аль-Кинди в IX веке.

В эпоху Возрождения криптография стала инструментом политиков и учёных. Леон Баттиста Альберти в XV веке предложил полиалфавитный шифр, где для замены символов использовалось несколько алфавитов. Это значительно усложнило частотный анализ.

В XVI веке француз Блез де Виженер разработал шифр Виженера, основанный на ключевом слове. Метод оставался неуязвимым до XIX века, когда Чарльз Бэббидж и Фридрих Казиский независимо друг от друга нашли способ его взлома.

XX век стал переломным этапом благодаря двум событиям:

1. Создание электромеханических шифровальных машин (например, немецкая «Энигма»), которые использовались во время Второй мировой войны. Взлом «Энигмы» командой Алана Тьюринга ускорил победу союзников.

2. Разработка теоретических основ криптографии. В 1949 году Клод Шеннон опубликовал работу «Теория связи в секретных системах», заложив математическую базу для симметричного шифрования.

В 1970-х годах появились первые асимметричные алгоритмы. Статья Уитфилда Диффи и Мартина Хеллмана «Новые направления в криптографии» (1976) представила концепцию открытого ключа, что решило проблему безопасного обмена ключами. В 1977 году был разработан RSA — первый практический асимметричный алгоритм, ставший основой интернет-безопасности.

В 2001 году AES (Advanced Encryption Standard) заменил устаревший DES, предложив 128-256-битные ключи и устойчивость к линейному и дифференциальному криптоанализу. AES стал стандартом для защиты государственных и корпоративных данных

С появлением блокчейна криптография вышла за рамки шифрования. Алгоритмы вроде SHA-256 и ECDSA (Elliptic Curve Digital Signature Algorithm) обеспечивают целостность и неизменность данных в распределённых системах.

Однако развитие квантовых компьютеров поставило под угрозу традиционные алгоритмы. В 1994 году Питер Шор разработал алгоритм, способный взломать RSA и ECDSA за полиномиальное время. Это заставило криптографов искать постквантовые алгоритмы, устойчивые к квантовым атакам.

Проблемы и перспективы постквантовой криптографии

1. Стандартизация. NIST с 2016 года проводит конкурс на выбор постквантовых алгоритмов. Финалисты включают методы на основе решёток (Kyber), хеш-функций (SPHINCS+) и код-базированных систем (Classic McEliece).

2. Совместимость. Интеграция новых алгоритмов в существующие протоколы (TLS, VPN) требует времени и ресурсов.

3. Производительность. Многие постквантовые методы требуют больше вычислительных мощностей, чем RSA или ECC.

Перспективные направления:

- Гибридные системы, сочетающие классические и постквантовые алгоритмы.

- Квантовое распределение ключей (QKD) для защиты каналов связи.

- Использование ИИ для автоматического обнаружения уязвимостей в шифрах.

От шифра Цезаря до квантово-устойчивых алгоритмов криптография прошла путь от искусства к строгой науке. Современные вызовы, такие как квантовые вычисления и IoT-устройства, требуют непрерывного совершенствования методов защиты. Успех постквантовой криптографии будет зависеть от сотрудничества учёных, инженеров и регуляторов. Будущие исследования должны фокусироваться на оптимизации алгоритмов, снижении затрат и повышении осведомлённости о новых угрозах.

**Библиографический список**

1. Шнайер Б. Прикладная криптография. – М.: Диалектика, 2021.

2. Diffie W., Hellman M. New Directions in Cryptography // IEEE Transactions on Information Theory. 1976.

3. Singh S. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. – Anchor, 2000.

4. NIST Post-Quantum Cryptography Standardization Project. URL: https://csrc.nist.gov/projects/post-quantum-cryptography

5. Гост Р 34.12-2015. Алгоритм шифрования «Кузнечик».

6. Шор П. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Computing. 1997.

7. RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3.

-