Тонковид Ирина Дмитриевна
студент, кафедра защищенных систем связи
Санкт-Петербургский государственный университет
РФ, г. Санкт-Петербург
E-mail: irtonkovid@yandex.ru

ИННОВАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ДАННЫХ В ОБЛАСТИ КВАНТОВЫХ ТЕЛЕКОММУНИКАЦИЙ

С ростом объемов передаваемой информации безопасность данных становится ключевой проблемой. В статье исследуются современные подходы к защите информации с использованием квантовых технологий, таких как квантовое ключевое распределение и генерация случайных ключей. Рассматривается роль квантовой криптографии в условиях киберугроз и необходимость инноваций для защиты конфиденциальности. Статья подчеркивает потенциал квантовых технологий в телекоммуникациях и их значимость для будущей безопасности данных.

With the increasing volume of information being transmitted, data security has become a key concern. This article explores current approaches to protecting information using quantum technologies, such as quantum key distribution and random key generation. It examines the role of quantum cryptography in the face of cyber threats and the need for innovation to safeguard privacy. The article highlights the potential of quantum technologies in telecommunications and their significance for future data security.

Ключевые слова: квантовая криптография; квантовое ключевое распределение; генерация случайных ключей; защита данных; квантовая невозможность клонирования; телекоммуникации; инновационные методы; безопасность данных; квантовые технологии.

Keywords: quantum cryptography; quantum key distribution; random key generation; data protection; quantum impossibility of cloning; telecommunications; innovative methods; data security; quantum technologies.

Введение

В эпоху цифровой трансформации обмен и хранение данных становятся ключевыми для телекоммуникационных систем. Увеличение объемов информации повышает риски для конфиденциальности и целостности данных, что делает защиту от кибератак важной задачей. Традиционные методы шифрования имеют ограничения из-за роста вычислительных мощностей. Перспективным направлением является квантовая криптография, которая использует принципы квантовой механики для создания защищенных систем. Статья рассматривает инновационные методы защиты данных в квантовых телекоммуникациях и потенциал квантовой криптографии для надежной защиты информации.

Основные методы защиты данных с использованием квантовых технологий

Квантовое ключевое распределение (QKD) — это метод квантовой криптографии, обеспечивающий безопасную передачу секретных ключей на основе квантовой механики. При перехвате состояние квантовой системы изменяется, что позволяет обнаружить вмешательство и предотвращает копирование ключа. QKD осуществляется через передачу фотонов и алгоритмы кодирования, обеспечивая абсолютную безопасность и выявление злоумышленников. Существуют два основных подхода: протоколы подготовки и измерения, а также протоколы на основе запутанных состояний, каждый из которых способствует развитию безопасных коммуникационных систем. QKD является важной технологией для защиты сетевых коммуникаций [6, с. 63-67].

Квантовая энтропия и генерация случайных ключей играют важную роль в обеспечении безопасности данных. Они создают неопределенность, что делает ключи устойчивыми к взлому, а также позволяют быстро генерировать безопасные ключи в динамичных коммуникационных средах. Доказуемость безопасности генерации ключей укрепляет доверие между сторонами обмена. Кроме того, квантовая генерация ключей применяется в различных областях, включая кибербезопасность, финансы и медицинские информационные системы, где конфиденциальность данных критична. Таким образом,

квантовая энтропия и генерация случайных ключей являются основными элементами кибербезопасности, обеспечивая надежность и безопасность информационных процессов в цифровом мире.

Квантовая невозможность клонирования, также известная как «Теорема о запрете клонирования – утверждение квантовой теории о невозможности создания идеальной копии произвольного неизвестного квантового состояния» [3]. Квантовая невозможность клонирования утверждает, что точную копию квантового состояния создать нельзя. Это делает скрытое копирование квантовых ключей и конфиденциальной информации невозможным, так как любая попытка клонирования нарушает состояние системы и выявляет вмешательство. В квантовых методах передачи данных подслушивание невозможно без изменения состояния системы, что позволяет обнаружить несанкционированный доступ и гарантирует конфиденциальность. Эти принципы обеспечивают высокую защиту от киберугроз и сохранение конфиденциальности данных.

Квантовые сети обеспечивают безопасную передачу данных с помощью квантовой криптографии, используя квантовые состояния частиц, такие как фотоны. Они защищают информацию от перехвата, так как попытки вмешательства становятся заметными. Копирование данных невозможно без изменения их состояния, что обеспечивает конфиденциальность и целостность информации. Квантовые протоколы позволяют аутентифицировать участников сети и защищены от современных атак на криптосистемы. Несмотря на сложности внедрения, с развитием технологий квантовые сети становятся важными для защиты данных в цифровом мире.

Сравнение эффективности квантовых методов защиты данных с классическими криптографическими методами

Для проведения экспериментального сравнения между квантовыми и классическими криптографическими методами можно рассмотреть несколько ключевых показателей: безопасность, скорость обработки данных и устойчивость к различным атакам.

Таблица 1.

Сравнение классических и квантовые криптографических методов

Показатель	**Классические криптографические методы (RSA, AES, DES и т.д.)**	**Квантовые криптографические методы**
Безопасность	Основывается на сложности задач, как факторизация больших чисел для RSA и дискретный логарифм	Основана на физических принципах квантовой механики, что делает невозможным перехват ключа без его обнаружения
Уязвимость	Устойчивость к атакам зависит от длины ключа и алгоритма; с развитием квантовых вычислений RSA может стать уязвимым	Квантовые системы могут быть уязвимы к атакам на аппаратном уровне
Скорость обработки данных	Обычно обеспечивают высокую скорость обработки данных, особенно при использовании современных алгоритмов	QKD может иметь более высокую задержку из-за необходимости передачи квантовых состояний и их измерения
Задержка	Задержка может быть минимальной,	Скорость передачи данных с QKD может быть ниже, чем у

	особенно в системах с малой нагрузкой	классических методов, особенно на больших расстояниях
Устойчивость к различным атакам	Устойчивы к атакам «грубой силы» и уязвимостям, но RSA уязвим к квантовым вычислениям	Квантовая криптография защищает от перехвата ключа и атак, используя принцип неопределенности и избегая уязвимостей классических методов
Гибкость и применимость	Классические алгоритмы универсальны и широко применяются в защите информации, аутентификации и шифровании данных	Квантовые протоколы требуют специального оборудования, что ограничивает их применение, но они перспективны для защищенных коммуникаций

Сравнительный анализ показывает, что классические методы криптографии, такие как RSA и AES, уязвимы к атакам, особенно в условиях квантовых вычислений. В отличие от них, квантовые методы, например QKD, обеспечивают более высокий уровень безопасности, предотвращая перехват ключа без обнаружения, хотя могут быть уязвимы на аппаратном уровне. Классические методы обеспечивают высокую скорость обработки и минимальную задержку, тогда как квантовые могут иметь большую задержку из-за сложности передачи квантовых состояний. Классическая криптография остаётся актуальной для большинства задач, но развитие квантовой

криптографии открывает новые горизонты безопасности, несмотря на высокие затраты и сложности внедрения [2, с. 70-75].

Расчеты уровня безопасности и стойкости квантовых протоколов

Для оценки уровня безопасности и стойкости квантовых протоколов, таких как квантовая распределенная ключевая система (QKD), можно рассмотреть несколько математических аспектов. В качестве примера возьмем протокол BB84, который является одним из самых известных квантовых протоколов. «BB84 — первый протокол квантового распределения ключей, который был предложен в 1984 году Чарльзом Беннетом и Жилем Брассаром. Протокол использует для кодирования информации четыре квантовых состояния двухуровневой системы, формирующие два сопряжённых базиса» [1].

Данный протокол использует четыре состояния поляризации:

Обозначение	Поляризация фотонов	Кодируемый бит
↔	Горизонтальная	1
↕	Вертикальная	0
↗	Под углом 45°	0
↖	Под углом 135°	1

Рисунок 1. Условные обозначения

Предположим, что злоумышленник (Ева) перехватывает фотон. Если она делает измерение, она может выбрать неправильный базис. Вероятность того, что Ева выберет правильный базис для измерения, составляет 50%, так как у нее есть два возможных базиса (прямой и диагональный).

Последовательность фотонов Алисы	↕	↗	↗	↔	↖	↕	↕	↔	↔
Последовательность анализаторов Боба	+	x	+	+	x	x	x	+	x
Результаты измерений Боба	0	0	1	1	1	0	1	1	0
Анализаторы выбраны верно	да	да	нет	да	да	нет	нет	да	нет
Ключ	0	0		1	1			1	

Рисунок 2. Процесс распределения ключей

Если Ева измеряет фотон в неправильном базисе, она изменит его состояние. Это приведет к ошибкам в конечном ключе.

Оценка ошибок.

Для оценки вероятности ошибки используем формулу:

$$P_e = {}^{e}/_{n} \quad (1)$$

n – общее количество переданных кубитов, квантовые состояния 1, 0;

e– количество обнаруженных ошибок после передачи.

Если P_e превышает некоторый порог (например, 11% для протокола BB84), это может указывать на присутствие злоумышленника.

Криптографическая стойкость.

Протокол BB84 основывается на теории информации и может быть оценен с точки зрения шенноновской безопасности. Максимальная информация, которую может извлечь Ева при длине ключа L, равной количеству переданных кубитов, определяется неравенством Шеннона:

$$I(A;B) = H(A) - H(A|B) \quad (2)$$

$H(A)$ – энтропия информации о сообщении;

$H(A|B)$ – условная энтропия.

Для оценки эффективности ключа можно использовать следующую формулу:

$$K = n(1 - P_e) \quad (3)$$

K– длина конечного ключа;

n– количество преданных кубитов.

Для оценки безопасности квантовых протоколов используются математические модели и методы криптоанализа. Протокол BB84 демонстрирует применение квантовой механики для защиты передачи данных, при этом важно учитывать угрозы от квантовых вычислений и анализировать вероятность ошибок и шифрования с учетом теории информации.

Пример расчетов в соответствии с представленными выше формулами.

Предположим, что мы предали 1000 кубитов (n = 1000) в квантовой коммуникации. Пусть Ева смогла перехватить и изменить 120 кубитов (e = 120) при измерении в неправильном базисе.

Оценка вероятности ошибок: P_e = e/n = 120/1000 = 0.12 или 12%.

В данном случае вероятность ошибки составляет 10%, что находится выше порога в 11%, это может указывать на присутствие злоумышленника.

Предположим, что энтропия информации о сообщении H(A) = 1 бит (максимальная энтропия для одного кубита). Теперь нужно рассчитать условную энтропию H(A|B). Допустим, что после обнаружения ошибок условная энтропия составляет H(A|B) = 0.8 бит.

Далее произведем расчет информации, которую может извлечь Ева: I (A; B) = H(A)-H(A|B) = 1 – 0.8 = 0.2 бита. Не смотря на наличие ошибок, злоумышленник не может получить значительную информацию о сообщении.

Расчет длины конечного ключа K с учетом вероятности ошибок: K = n (1 - P_e) = 1000(1 – 0.12) = 1000 * 0.88 = 880 бит. Несмотря на потерю части информации из-за ошибок, оставшаяся длина ключа все ещё позволяет обеспечить надежную защиту данных.

Метод BB84 является надежным способом квантового ключевого распределения. Он позволяет обнаруживать вмешательство злоумышленника, сохраняя безопасность передачи информации. Высокая вероятность ошибок может указывать на угрозу, что дает возможность сторонам принять меры для защиты данных.

Заключение

В заключении статьи подчеркивается важность квантовой криптографии для безопасности информации в цифровую эпоху. Квантовое ключевое распределение (QKD) обеспечивает абсолютную конфиденциальность ключей, а квантовая энтропия и случайные ключи гарантируют стойкость передачи данных. Квантовая невозможность клонирования и защита от подслушивания помогают противостоять киберугрозам. Исследования квантовых сетей направлены на создание безопасных коммуникационных

систем, открывая новые перспективы для защиты данных в телекоммуникациях, финансах и медицине. Инновационные методы защиты в квантовых телекоммуникациях значительно способствуют кибербезопасности.

Список использованной литературы

1. BB84 – Wikipedia, 2025. – URL: https://en.wikipedia.org/wiki/BB84 (дата обращения 29.06.25)
2. Никитин В. Н., Ковцур М. М., Юркин Д. В. Повышение защиты протоколов распределения ключей от атак вторжения в середину канала связи //Информационно-управляющие системы. – 2014. – №. 1 (68). – С. 70-75. – URL: https://elibrary.ru/item.asp?id=21303686 (дата обращения 29.06.25)
3. Теорема о запрете клонирования – Wikipedia, 2023. – URL: https://ru.wikipedia.org/wiki/Теорема_о_запрете_клонирования (дата обращения 29.06.25)
4. Квантовая сеть – Wikipedia,2025. – URL: https://ru.wikipedia.org/wiki/Квантовая_сеть (дата обращения 29.06.25)
5. Кяжев Ф.Р. Современные квантовые технологии для безопасного обмена данными, 2023. – URL: https://cyberleninka.ru/article/n/sovremennye-kvantovye-tehnologii-dlya-bezopasnogo-obmena-dannymi/viewer (дата обращения 29.06.25)
6. Кушнир, Д. В. Исследование возможных методов аутентификации согласования данных в классическом канале в протоколах квантовой криптографии / Д. В. Кушнир, С. Н. Шемякин // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2021. – № 4. – С. 63-67. – URL: https://elibrary.ru/qhhwyg?ysclid=mcj95jhctd985840737 (дата обращения 30.06.25)

7. Шемякин С. Н. и др. Выяснение криптографических свойств булевых функций шифра «Магма» //Экономика и качество систем связи. – 2021. – №. 1 (19). – С. 67-73. – URL: https://elibrary.ru/item.asp?id=45574471 (дата обращения 30.06.25)

8. Коржик, В. И. Цифровая стеганография : учебник / В. И. Коржик, А. В. Красов. – Москва : Общество с ограниченной ответственностью "Издательство "КноРус", 2023. – 324 с. – ISBN 978-5-406-10970-0. – EDN KNKBXU.

9. Радынская В. Е., Поляничева А. В., Ахрамеева К. А. Разработка метода защиты ядра программных приложений с применением самомодифицирующегося кода //Региональная информатика и информационная безопасность. – 2019. – С. 136-141. – URL: https://elibrary.ru/ydsulx?ysclid=mcj995h1r284426321 (дата обращения 28.06.25)