УДК 004.7

# КВАНТОВЫЕ ТЕХНОЛОГИИ В СФЕРЕ БЕЗОПАСНОСТИ

Дубинкин С. Д., студент гр. ЦСб-231, II курс, Кирин Н. А., студент гр. ЦСб-231, II курс, Александрович Е. А., студент гр. ЦСб-231, II курс, Иванов Г. Р., студент гр. ЦСб-231, II курс
Научный руководитель: Елкин И.С., к.т.н., доцент

Кузбасский государственный технический университет
имени Т. Ф. Горбачёва
Россия, г. Кемерово

Аннотация. Обсуждается значимость применения методов квантового шифрования в современном мире для повышения безопасности передачи данных в развитии информационных технологий. Рассматривается структура и основные принципы технологии квантовой криптографии на основе свойств квантовых систем, физические принципы квантового шифрования и передачи данных, проблемы, перспективы развития глобальных квантовых систем связи, передачи информации.

Ключевые слова: квантовый компьютер, информационная безопасность, информационные технологии, квантовая сеть, кубит.

Квантовые технологии в сфере информационной безопасности наиболее актуальны на сегодняшний день во всем мире, а в особой степени – в России. По данным аналитиков Surfshark в 2022 году Российская Федерация стала самой взламываемой страной в мире. В III квартале 2022 года хакеры взломали 22,3 миллиона аккаунтов россиян, для сравнения: во Франции, которая заняла 2 место рейтинга, взломали 13,8 миллионов аккаунтов. Ттаким образом, здесь мы видим практически двукратную разницу [1]. В то же время квантовые технологии позволяют решать данную проблему с максимальной безопасностью, хранить и передавать данные пользователям. Это позволит минимизировать количество взломов аккаунтов, тем самым повысит уровень информационной безопасности в целом. В настоящее время системы квантовой связи не только существуют, но и имеют коммерческую реализацию, создавая и решая новые задачи по повышению безопасности, в основном в сфере кодирования и передачи данных – криптографии [2].

Квантовые связь и шифрование с использованием квантовых технологий уже не являются лабораторной инновацией на сегодня. Первые научные работы на эту тему появились уже в 70–80-х годов XX века, а первые лабораторные тесты прошли в 1989 году. В конце 90-х функционировали коммерческие системы квантовой передачи ключей на расстояние от 20 до 50 км. Такие компании, как id Quantique и MagiQ

Technologies, продают готовые системы передачи криптоключей по оптоволоконному кабелю. Эти системы достаточно просты для установки и кроме разного рода военных и правительственных организаций их взяли на вооружение крупные коммерческие организации и банки [3].

В 2021 году РЖД и “Ростелеком” начали совместно развивать квантовые технологии, а уже в 2023 на базе кластера “Ломоносов” в Москве создается площадка для тестирования квантовой связи [4].

Целью данной работы является выявить преимущества и недостатки квантовой связи, объективно оценить возможность фактической реализации квантовых сетей.

Основные задачи исследования:

1. Подробно изучить основные принципы работы квантовой связи, понять её фундаментальные особенности и возможности и выявить преимущества квантовой связи в сфере информационной безопасности;
2. Проанализировать недостатки квантовой связи и исследовать существующие проекты по созданию квантовых сетей в России и мире;
3. Оценить возможность реализации квантовых сетей в современных условиях.

Основные принципы работы квантовой связи. Квантовая связь основана на принципах квантовой механики, которые обеспечивают высокий уровень безопасности. В отличие от классических битов, квантовый бит (кубит) может находиться в суперпозиции состояний 0 и 1, что позволяет передавать данные с большей эффективностью и безопасностью. Одним из ключевых явлений является квантовая запутанность, при которой две частицы взаимосвязаны, и изменение состояния одной влияет на другую, даже на расстоянии (рис.1). Это свойство используется для создания защищённых каналов связи, так как любое вмешательство изменяет состояние системы и может быть легко обнаружено.

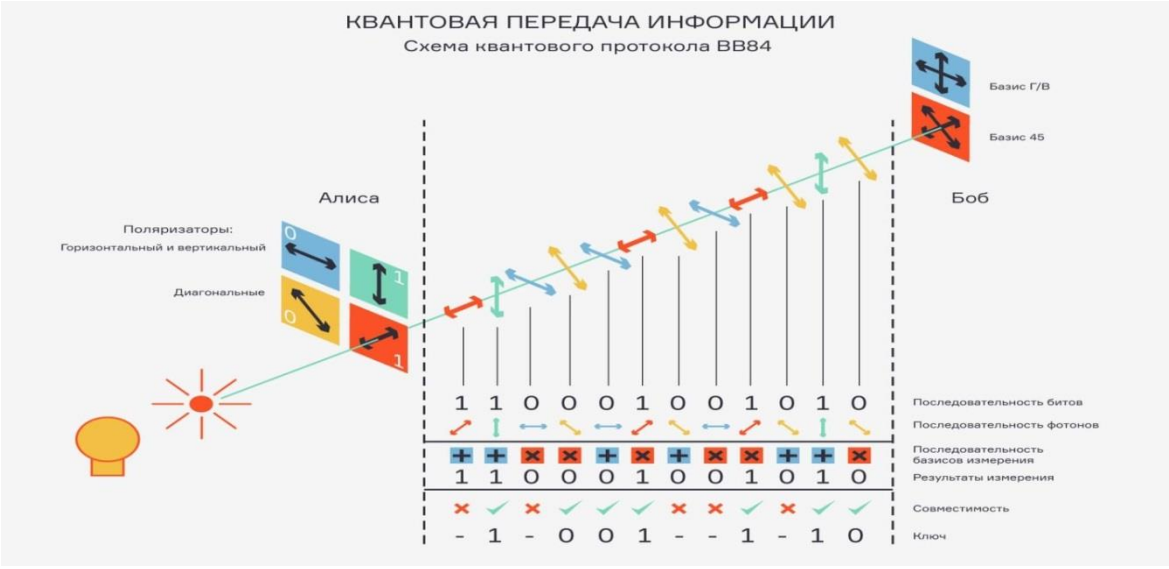


Рис. 1. Схема квантовой передачи информации

Кроме того, принцип неопределённости Гейзенберга ограничивает точность измерений в квантовых системах, что делает невозможным скрытное прослушивание передаваемых данных: вмешательство в систему приводит к изменению её состояния, и это сразу обнаруживается. В квантовой криптографии применяется технология распределения квантовых ключей (QKD), которая позволяет безопасно обмениваться секретными криптографическими ключами. Протокол BB84 использует свойства квантовых состояний, чтобы любая попытка перехвата ключа была обнаружена, обеспечивая, таким образом, абсолютную защиту данных [5].

Основная проблема квантовых коммуникационных систем заключается в ограниченном радиусе действия, который составляет около 100 км. Это объясняется тем, что одиночные фотоны подвержены изменению своих состояний под воздействием внешних факторов. Кроме того, они могут быть полностью поглощены средой из-за помех. В настоящее время для построения оптических квантовых сетей применяются ретрансляторы. Эти устройства расшифровывают полученную информацию, затем заново её кодируют и передают дальше по цепи узлов. Однако такой подход имеет недостаток: промежуточные узлы получают доступ к содержимому сообщений, что создаёт риск утечки данных при взломе любого из них. Также массово создавать подобные линии передач данных мешает слишком высокая стоимость материалов. В конструкции данных устройств используются дорогие в производстве магниты и редкие минералы [5].

Существуют и другие варианты решения этой проблемы. Вместо кодирования информации в поляризации фотона, которая подвержена влиянию внешних факторов, можно использовать другие степени свободы, такие как орбитальный угловой момент (OAM от англ. orbital angular momentum). OAM кодирование менее чувствительно к внешним воздействиям и позволяет передавать больше информации за счет увеличения количества возможных состояний. Этот вариант, как и другие, имеет свой недостаток – турбулентность, которая может отрицательно влиять на оптические волны, несущие OAM в виде спирального фазового фронта, что приводит к искажениям [5].

Для изучения основных принципов работы квантовой связи, включая квантовую криптографию и передачу квантовых ключей, необходимо обратиться к фундаментальным концепциям квантовой механики, лежащим в основе этих технологий. Квантовая связь использует особые свойства квантовых объектов, такие как суперпозиция, квантовая запутанность и принцип неопределённости Гейзенберга, для обеспечения надежности и безопасности передачи данных, попытка прослушивания или вмешательства в систему изменяет её состояние, что может быть немедленно обнаружено.

Квантовый бит (кубит), являющийся основой квантовой информации, отличается от классического бита тем, что может находиться не только в состояниях 0 или 1, но и в их суперпозиции. Это свойство позволяет квантовой системе одновременно обрабатывать и передавать большое

количество информации, что значительно повышает её вычислительные и информационные возможности. Квантовая связь использует кубиты для передачи данных, что обеспечит более высокую безопасность по сравнению с классическими системами [6].

Квантовая криптография – это технология кодирования и передачи данных в квантовых состояниях фотонов. В ней используются вышеописанные принципы для создания защищённых каналов связи и безопасной передачи данных. Один из основных протоколов квантовой криптографии – BB84, предложенный Чарльзом Беннетом и Жилем Брассаром в 1984 году, используется для обмена секретными ключами, которые обеспечивают шифрование данных. Любая попытка перехвата этих ключей немедленно приводит к обнаружению вмешательства, что делает возможным создание абсолютно защищённых каналов для передачи данных [5], [7].

Квантовая связь, благодаря своим фундаментальным особенностям, значительно повышает уровень безопасности передачи данных по сравнению с классическими методами. Это преимущество квантовой связи тесно связано с принципом квантовой неопределенности и квантовой запутанности. В отличие от классических систем, где возможно перехватить данные без их изменения, в квантовой связи невозможно перехватить данные без их модификации. Это связано с тем, что в квантовых системах любые попытки измерить или «копировать» квантовые состояния нарушают их характеристики. Например, в случае с квантовыми битами (кубитами) любое измерение суперпозиции состояний изменяет саму квантовую систему.

Квантовая криптография является неотъемлемой частью системы квантовой связи, и её возможности активно используются для защиты данных. Одним из главных преимуществ квантовой криптографии является использование квантового распределения ключей (QKD), которое предоставляет методы для создания и обмена секретными ключами через квантовые каналы, при этом любое вмешательство в процесс передачи немедленно выявляется. Благодаря использованию квантовых свойств, таких как суперпозиция и запутанность, информация может быть передана с гарантированной защитой от подслушивания.

Одним из основных ограничений квантовой связи является не большая дальность передачи данных. Потери в оптоволоконных кабелях увеличиваются экспоненциально с увеличением длины канала (рис. 2) [8]. В классических системах связи эти потери компенсируются с помощью повторителей и маршрутизаторов, которые усиливают сигнал. Однако для квантовых систем это невозможно, так как любое вмешательство, включая попытки измерения состояния фотонов, разрушает их квантовое состояние. Это делает невозможным восстановление переданного фотона, если он был изменён в процессе передачи.

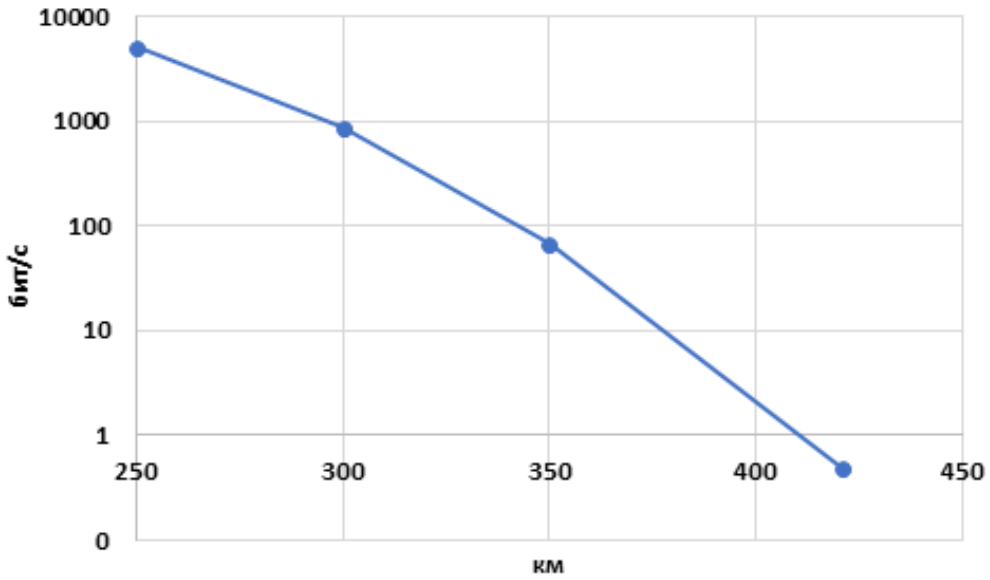


Рис.2. Зависимость скорости передачи данных с помощью квантовых сетей связи от расстояния [8]

На данный момент квантовая связь ограничена небольшими расстояниями, и наибольшее расстояние для эффективной передачи квантовых данных составляет 421 километров (рис. 2). При этом скорость передачи данных остаётся крайне низкой – около 0,49 бита в секунду. Но уже на расстоянии в 250 километров скорость передачи данных возрастает до 4,9 бита в секунду. Такие характеристики позволяют использовать квантовые сети для защищённой связи на коротких расстояниях, например, в пределах города, для таких нужд, как передача данных между офисами банков. На большие расстояния можно передавать лишь ключи шифрования, а сами пакеты данных отправлять, используя оптоволокно. Однако, безопасность данного способа оставляет желать лучшего [8].

Для преодоления ограничений по дальности передачи данных исследователи работают над созданием квантовых повторителей, которые могут усиливать квантовые сигналы на больших расстояниях. Однако на сегодняшний день эта технология находится на стадии экспериментов, и ещё не разработаны решения, которые обеспечивали бы стабильную работу таких устройств на практике.

Одним из способов решения проблемы дальности передачи является использование космических технологий. Потери фотонов в атмосфере и космосе значительно ниже, чем в оптоволокне, что позволяет использовать спутники для ретрансляции квантовых сигналов на расстояния в тысячи километров. В 2017 году китайский спутник «Мо-Цзы» продемонстрировал успешное распределение запутанных фотонов на рекордное расстояние более 1200 километров, а позже с его помощью была организована квантовая линия связи между Веной и Пекином [5].

Космическая квантовая связь открывает новые возможности для создания глобальных квантовых сетей, однако эта технология ещё находится в стадии разработки и требует дальнейших исследований и улучшений.

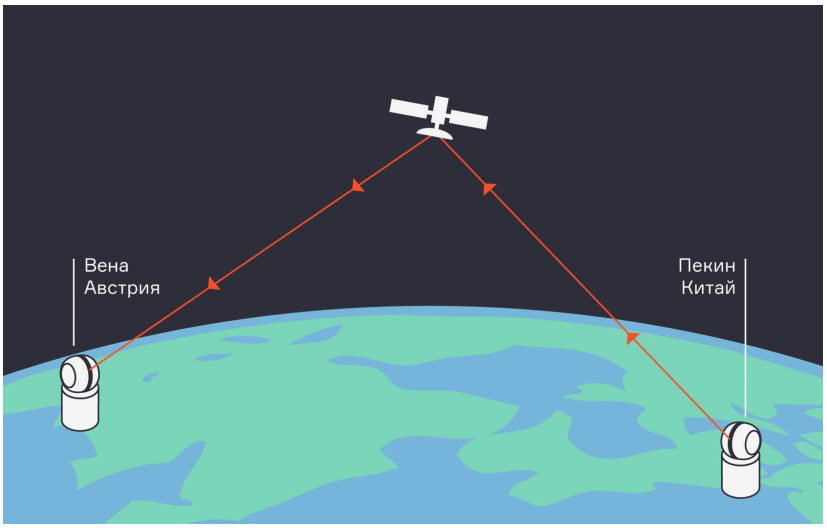


Рис.3. Схема использования космической связи

Несмотря на высокую степень безопасности, квантовые системы могут быть уязвимы для определённых типов атак, особенно в реальных условиях эксплуатации. Квантовые устройства могут иметь слабые места в своей физической реализации, которые можно использовать для воздействия на систему.

В России на данный момент существует несколько крупных проектов, направленных на создание квантовых сетей. Одним из них является проект, реализуемый в рамках РЖД и Ростелекома. В 2021 году эти компании начали сотрудничество для разработки квантовых технологий с целью создания защищённых квантовых каналов для передачи данных. В результате этого сотрудничества в 2023 году был создан квантовый канал для тестирования и разработки квантовых систем связи на базе московского кластера "Ломоносов" [9].

Одним из самых известных проектов является Quantum Internet Alliance в Европе, который включает в себя исследовательские центры из различных стран ЕС. Этот проект направлен на создание квантового интернета с использованием квантовых повторителей, которые позволят передавать квантовые данные на большие расстояния. В рамках проекта также разрабатываются стандарты для интеграции квантовых технологий в существующие телекоммуникационные сети [9].

Кроме того, на базе Московского физико-технического института (МФТИ) и других научных организаций России ведутся исследования по разработке квантовых повторителей и других компонентов квантовых сетей. Эти устройства помогут преодолеть ограничения по дальности передачи квантовых сигналов, создавая более масштабируемые и доступные сети [2].

В области квантовых вычислений наблюдаются значительные достижения, однако полноценная реализация таких систем ещё не достигнута. Например, компания IBM недавно продемонстрировала квантовый процессор с 433 сверхпроводниковыми кубитами, а также решение конкретной задачи на процессоре с 127 кубитами [9].

Что касается квантового интернета, то, несмотря на отсутствие его работающих физически реализованных систем на данный момент, эта концепция остаётся перспективной для безопасной передачи данных. Совсем недавно IBM объявила о планах к 2033 году объединить четыре квантовых процессора по 25 000 кубитов в единую сеть. Важно отметить, что для успешного применения квантовых вычислительных устройств необходимо правильно выбрать задачу, подходящую для квантовых технологий [6].

Квантовая связь, основанная на принципах квантовой механики, представляет собой перспективную технологию, которая может значительно улучшить информационную безопасность. Изучение основ квантовой криптографии, квантовых ключей и других фундаментальных понятий, таких как кубиты, суперпозиция и квантовая запутанность, показывает, что квантовые системы обеспечивают высокую степень защиты от перехвата данных. Одним из главных преимуществ является невозможность получения информации из квантового канала без её изменения, что обеспечивает защиту от подслушивания и атак.

Однако, несмотря на многочисленные преимущества, квантовые сети сталкиваются с рядом серьёзных технических ограничений. Проблемы с масштабируемостью, стоимостью и дальностью передачи сигналов остаются важными барьерами. Квантовая связь, несмотря на свою теоретическую безопасность, всё ещё уязвима для некоторых типов атак, и существующие технологии требуют значительных доработок. Ограничение по дальности передачи фотонов и необходимость в квантовых повторителях также сдерживают массовое внедрение этой технологии.

Что касается глобальной реализации квантовых сетей, то в России и мире активно развиваются проекты, направленные на создание и тестирование квантовых каналов связи. На данный момент они обеспечивают защищённые каналы связи на ограниченные расстояния, например, в рамках городских сетей. Ведущие страны, такие как Китай, активно работают над созданием спутниковых квантовых систем, что позволяет расширить возможности передачи данных на тысячи километров. Несмотря на эти достижения, полноценное создание глобальной квантовой сети требует значительных усилий и инвестиций.

Таким образом, квантовая связь обещает революцию в области информационной безопасности, но для её широкого применения необходимо решить ряд технических и экономических проблем, связанных с масштабируемостью и внедрением инфраструктуры.

**Список литературы:**

1. http://safe.cnews.ru/news/top/2022-10-27_rossiya_obognala_ssha_i_stala.
2. Что такое квантовые коммуникации и их развитие в РФ. URL: http://telecomtimes.ru/2018/12/kvantoviye-kommunications-tehnologii.
3. Квантовые компьютеры и конец безопасности. URL: http://www.kaspersky.ru/blog/kvantovye-kompyutery-i-konec-bezopasnosti/1989/
4. Россия в «квантовом мире»: прогресс несмотря на санкции. URL: http://www.cnews.ru/articles/2023-07-13_rossiya_v_kvantovom_mire_progress
5. Квантовые технологии. URL: http://nplus1.ru/material/2020/02/06/course-quantum-technology-chapter5
6. Квантовые сети: перспективы и сложности реализации. URL: https://habr.com/ru/companies/vasexperts/articles/428740/
7. Актаева А. У., Баймуратов О. А., Галиева Н. Г., Байкенов А. С. Безопасность информации: применение квантовых технологий. International Journal of Open Information Technologies. 2016. Т. 4. № 4. С. 40-48. URL: https://cyberleninka.ru/article/n/bezopasnost-informatsii-primenenie-kvantovyh-tehnologiy/viewer
8. Физики обновили рекорд дальности квантовой связи по оптоволоконному кабелю. URL: https://nplus1.ru/news/2018/11/07/QKD-fiber.
9. https://rg.ru/2023/07/13/kvantovaia-kriptografiia-protiv-kvantovyh-kompiuterov-kto-silnee.html