

Л.В. Козиенко, К.Е. Землянова

Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ КВАНТОВЫХ КОММУНИКАЦИЙ В КОМПАНИИ ОАО «РЖД»

Аннотация. В статье рассматривается технология квантовой коммуникации, её разновидности и области применения. Особое внимание уделено процессу внедрения данной технологии компанией ОАО «РЖД», начиная с соглашения между Правительством Российской Федерации и ОАО «РЖД», закрепившего статус компании, как ответственной за развитие высокотехнологичной области «Квантовые коммуникации».

Основная деятельность компании направлена на создание экосистемы и координация работ всех участников рынка квантовых коммуникаций, институтов развития, ВУЗов, разработчиков, производителей и конечных потребителей в целях обеспечения технологической безопасности и суверенитета страны, а также стимулирования развития цифровой экономики.

Ключевые слова: квантовые коммуникации, квантовое распределение ключей, квантовая криптография, квантовая сеть связи, дорожная карта, передача зашифрованной информации.

L.V. Kozienko, K.E. Zemlyanova

Irkutsk State Transport University, Irkutsk, the Russian Federation

APPLICATION OF QUANTUM COMMUNICATIONS AT JSC «RUSSIAN RAILWAYS»

Abstract. The article examines quantum communication technology, its varieties and areas of application. Particular attention is paid to the process of implementing this technology by JSC «Russian Railways», starting with the agreement between the Government of the Russian Federation and JSC «Russian Railways», which secured the company's status as responsible for the development of the high-tech field of Quantum Communications.

The company's main activity is aimed at creating an ecosystem and coordinating the work of all participants in the quantum communications market, development institutions, universities, developers, manufacturers and end consumers to ensure technological security and sovereignty of the country, as well as stimulating the development of the digital economy.

Keywords: quantum communications, quantum key distribution, quantum cryptography, quantum communication network, roadmap, transmission of encrypted information.

Введение

Квантовые коммуникации представляют собой метод защиты коммуникаций, основанный на принципах квантовой физики. В отличие от традиционной криптографии, которая использует математические методы, чтобы обеспечить секретность информации, квантовая криптография сосредоточена на физике, рассматривая случаи, когда информация переносится с помощью объектов квантовой механики. Она основана на принципиальной неопределенности поведения квантовой системы, выраженной в принципе неопределенности Гейзенберга [1]. Это позволяет создавать каналы связи, которые обеспечивают высокую степень безопасности за счёт невозможности подслушивания без изменения определенных параметров физических объектов-переносчиков информации. Одним из основных достижений в этой области является возможность передачи данных по квантовому каналу со скоростью до нескольких Мбит/с.

Квантовые сети являются практическим применением квантовой криптографии и позволяют передавать квантовую информацию между физически разделёнными квантовыми системами. Они играют ключевую роль в развитии квантовых вычислений и систем криптографии. Специалисты отмечают, что через 10–15 лет квантовая связь станет таким же обязательным элементом цифровой инфраструктуры, как защита от вредоносных программ, установленная на каждом компьютере.

Разновидности квантовых коммуникаций

Квантовые коммуникации включают различные подходы и технологии, каждая из которых имеет свои особенности и преимущества. Можно выделить следующие ключевые направления квантовых коммуникаций:

Квантовое распределение ключей (КРК) является наиболее известным видом квантовых коммуникационных технологий. КРК используется для безопасного обмена ключами шифрования между двумя сторонами. Основная идея заключается в том, что любая попытка прослушивания канала связи приведет к изменению состояния передаваемых фотонов, что будет обнаружено получателем. Примеры протоколов КРК включают:

– BB84 (Bennett-Brassard 1984): Один из первых и наиболее известных протоколов квантового распределения ключей, основанный на использовании двух ортогональных базисов поляризации фотонов [2].

– E91 (Ekert 1991): Протокол, использующий запутанные пары частиц для генерации ключа [3].

– B92: Упрощенная версия BB84, требующая только одного базиса поляризации [4].

Распределение запутанных состояний предполагает передачу запутанных пар частиц между двумя удалёнными точками. Запутанность позволяет осуществлять мгновенную корреляцию измерений даже на больших расстояниях. Распределение таких состояний может использоваться для реализации квантовой телепортации и других приложений.

Протоколы квантовой аутентификации основаны на использовании квантовых свойств для проверки подлинности отправителя сообщения. Аутентификация может осуществляться с использованием квантовых состояний, которые невозможно подделать или изменить без обнаружения.

Многопользовательские квантовые сети предполагают наличие нескольких узлов, связанных квантовым каналом. Такие сети могут использоваться для безопасного распределения ключей среди множества участников или для выполнения распределённых квантовых вычислений.

Долговременное хранение квантовой информации связано с возможностью хранения квантовой информации в течение длительного времени. Такая способность важна для построения устойчивых квантовых сетей и обеспечения непрерывного функционирования квантовых вычислительных систем.

Указанные разновидности квантовых коммуникаций охватывают широкий спектр задач, начиная от простого шифрования данных и заканчивая сложными многоуровневыми сетевыми структурами. Каждый из подходов имеет свою нишу и область применения, а их развитие продолжается благодаря активным научным исследованиям и технологическому прогрессу.

Применение квантовых коммуникаций

Квантовые коммуникации находят применение в различных областях, где требуется высокая безопасность передачи данных:

Финансовые учреждения нуждаются в защите финансовых транзакций и конфиденциальной информации клиентов. Квантовые ключи могут использоваться для шифрования банковских операций, обеспечивая высокий уровень безопасности при передаче данных о платежах, кредитах и других операциях.

Государственные структуры, такие как военные ведомства, разведывательные службы и дипломатические миссии, требуют высокой степени конфиденциальности при обмене информацией. Квантовая криптография поможет обеспечить защиту каналов связи, предотвращая несанкционированный доступ к стратегически важной информации.

Медицинские учреждения хранят и передают большие объёмы персональных данных пациентов, включая медицинские карты, результаты анализов и другую чувствительную информацию. Квантово-защищенные каналы связи помогут защитить эти данные от утечек и атак хакеров.

Операторы телекоммуникационных сетей могут использовать квантовые технологии для обеспечения безопасной передачи данных через волоконно-оптические линии связи. Это особенно важно для защиты крупных корпоративных сетей и интернет-трафика.

Крупные компании часто сталкиваются с необходимостью защищать свои коммерческие тайны, патенты, финансовые отчёты и другие важные документы. Квантовый канал связи может стать эффективным инструментом для предотвращения промышленного шпионажа и кибератак.

С развитием *Интернета вещей (IoT)* растёт потребность в обеспечении безопасности устройств, подключенных к интернету. Квантовые технологии могут предложить решения для защиты этих устройств от взлома и перехвата данных.

При проведении *научных исследований* учёные могут использовать квантовые коммуникации для обмена данными между лабораториями и исследовательскими центрами. Например, передача результатов экспериментов или обсуждение теоретических моделей требует высокого уровня безопасности.

Системы космической связи представляют собой распределённый комплекс приёмо-передающих устройств, функционирующих в сложных условиях, где традиционные методы шифрования могут оказаться уязвимыми. Квантовое распределение ключей сможет повысить надёжность связи между спутниками и наземными станциями.

Таким образом, квантовые коммуникации открывают новые горизонты в сфере информационной безопасности, предлагая уникальные возможности для защиты данных в различных отраслях. Развитие технологий квантового распределения ключей и создание глобальных квантовых сетей открывает перспективы для создания новых стандартов безопасности в будущем [5].

Применение квантовых коммуникаций в ОАО «РЖД»

В июле 2019 года были подписаны соглашения о намерениях между Правительством Российской Федерации и ПАО «Сбербанк» (направление «Искусственный интеллект»), ОАО «РЖД» (направление «Квантовые коммуникации»), госкорпорацией по атомной энергии «Росатом» (направления «Квантовые вычисления» и «Технологии создания новых материалов и веществ»), госкорпорацией «Ростех» (направления «Квантовые сенсоры», «Технологии распределенного реестра», «Новые поколения узкополосной беспроводной связи для интернета вещей и связи ближнего и среднего радиусов действия»), а также трёхстороннее соглашение с госкорпорацией «Ростех» и ПАО «Ростелеком» по направлению «Беспроводная связь нового поколения» [6].

Предметом соглашения является объединение и координация совместных действий правительства и ОАО «РЖД» для ускорения технологического развития и достижения РФ позиции одного из лидеров на глобальных технологических рынках в области квантовых коммуникаций. В соответствии с соглашением была разработана дорожная карта развития высокотехнологичной области «Квантовые коммуникации». Дорожная карта определяет три ключевые задачи:

- достижение технологического лидерства (сетевые технологии, абонентские устройства, спутниковая и атмосферная связь, интернет вещей и др.);
- формирование инфраструктуры (магистральные сети, локальные сети, центры управления и мониторинга и др.);
- развитие экосистемы и формирование рынков товаров и услуг (подготовка кадров, национальная и международная стандартизация, информационное продвижение и профессиональные сообщества, развитие рынка, нормативное регулирование и др.).

Таким образом, ОАО «РЖД» определена правительством РФ как компания, ответственная за развитие высокотехнологичной области «Квантовые коммуникации». Это новое направление сформировалось на стыке технологий фотоники (работа с оптическими сигналами и создание устройств на их основе) и квантовых технологий.

В 2020 году был сделан ряд практических шагов по реализации положений дорожной карты. Компания ОАО «РЖД» приступила к реализации проекта по созданию магистральной квантовой сети связи Москва – Санкт-Петербург. Строительство квантовой сети позволило апробировать новые технологические решения и внедрить важные сервисы. При этом новая инфраструктура позволяет передавать большие массивы данных с высочайшим уровнем надежности. Позже по квантовой сети состоялся сеанс видеоконференцсвязи между Москвой и Санкт-Петербургом [7].

В 2021 году компания «Ростелеком» и ОАО «РЖД» подписали соглашение о сотрудничестве в развитии квантовых коммуникаций. В этом же году был заключен договор о сотрудничестве между ОАО «РЖД», Госкорпорацией «Роскосмос» и ПАО «Ростелеком» в области развития квантовых коммуникаций. Данные соглашения способствовали развитию высокотехнологичных областей квантовых коммуникаций и космических систем, а также позволили координировать проекты развития наземного и космического сегментов квантовой связи. Объединение усилий с ПАО «Ростелеком» способствовало развитию рынка квантовых коммуникаций и внедрению этих технологий в сфере услуг, а также на объектах критической информационной инфраструктуры.

В августе 2021 года ОАО «РЖД», аэропорт Шереметьево и «Компания ТрансТелеКом» провели тестовый запуск квантовой линии связи на полигоне Международного аэропорта Шереметьево. Квантовая линия, протяженностью 5,5 км связала Терминал F и здание Центра обработки данных, расположенное за пределами территории аэропорта. Квантовая сеть продемонстрировала устойчивую работу канала квантовой коммуникации. Тестирование проводилось на оборудовании отечественных компаний Qrate и «Код безопасности». Данный опыт использования квантового оборудования на инфраструктуре ОАО «РЖД» показал перспективы проведения дальнейших работ по внедрению данной прогрессивной технологии в транспортную отрасль.

В начале 2022 года ОАО «РЖД» и Центр компетенций НТИ «Квантовые коммуникации» НИТУ «МИСиС» заключили договор на создание инновационного устройства для квантово-защищённых сетей связи. Целью проекта является разработка экспериментального образца устройства квантового распределения ключей шифрования с использованием технологии для «недоверенного» центрального узла. Такой узел не накапливает квантовые ключи шифрования в сети типа «звезда» (с центральным узлом и несколькими подключенными периферийными устройствами связи). Ключ распределяется сразу между периферийными устройствами, что позволяет снизить возможность несанкционированного доступа. В апреле этого же года, в рамках дорожной карты, предполагалось проведение эксперимента по созданию оптического канала связи между космическими аппаратами и наземными терминалами. С помощью тестируемой системы связи можно передавать, в том числе, и квантовые ключи шифрования, обеспечивающие максимальный уровень защиты информации.

В течение 2022 года ОАО «РЖД» была запущена первая линия квантовой связи в России Москва – Санкт-Петербург, протяженностью около 700 км, соединившая два крупнейших мегаполиса страны. Также был построен участок квантовой сети связи между Москвой и Нижним Новгородом. Новая инфраструктура позволила с высоким уровнем защиты передавать большие объёмы данных. Информация шифруется алгоритмом квантового распределения ключей, что гарантирует ее сохранность. При попытке получить несанкционированный доступ без ключа данные искажаются.

В 2022 году была так же актуализирована дорожная карта «Квантовые коммуникации», рассчитанная до 2030 года. Для достижения Россией лидирующих позиций в данной области ведутся работы по ключевым направлениям: научно-техническое развитие, формирование инфраструктуры и экосистемы квантовых коммуникаций.

В конце 2022 года кабмин и ОАО «РЖД» подписали соглашение для реализации обновленной дорожной карты по развитию квантовых коммуникаций. Она предполагает достижение к концу 2024 года протяженности квантовых сетей свыше 7 000 км, а к 2030 году – более 15 000 км [8]. Документ так же определяет 17 ключевых групп продуктов и показатели,

которые характеризуют их готовность к выходу на рынок. В соответствии с соглашением ОАО «РЖД» определена ключевая роль в развитии квантовых коммуникаций, поскольку компания дальше всех в стране продвинулась в этом направлении.

Таким образом, за период 2021–2022 г.г. в ходе реализации проектов ОАО «РЖД» были построены и введены в эксплуатацию участки между Москвой и Санкт-Петербургом, Москвой и Нижним Новгородом. Общая протяженность квантовой сети связи составила 1147 км. При этом, по оценкам специалистов затраты на строительство еще 1400 км новых участков квантовых сетей могут обойтись в сумму от 1,5 млрд до 3 млрд руб. Дополнительно были завершены мероприятия по организации Центра управления и мониторинга квантовой сети ОАО «РЖД».

В апреле 2023 года было подписано соглашение между ОАО «РЖД» и ФГУП «Космическая связь» об объединении усилий в области развития технологий квантовых коммуникаций. Компании договорились о сотрудничестве в сфере развития сетей и экосистемы квантовых коммуникаций на базе спутниковых технологий. Также, Минюстом России, был утвержден новый профессиональный стандарт «Специалист по исследованиям и разработкам в области квантовых коммуникаций», который вступил в силу с 1 сентября 2023 года.

В 2023 году на базе инфраструктуры ОАО «РЖД» создаётся межвузовская квантовая сеть. Во время «Форума будущих технологий» (9–14 июля 2023, г. Москва, ЦМТ) состоялся пилотный сеанс в формате видеоконференцсвязи по квантовому защищённому каналу между МГУ и Университетом Лобачевского в Нижнем Новгороде. К проекту присоединятся также МГУСИ, МИСИС, ИТМО, а в перспективе – университеты и научные центры Казани, Самары, Челябинска и других регионов.

В сентябре 2023 года ОАО «РЖД» представила карту проекта магистральной квантовой сети связи в рамках VIII Восточного экономического форума. Она включает в себя такие города, как Москва, Санкт-Петербург, Тула, Воронеж, Сочи, Краснодар, Лихая, Ростов-на-Дону, Арзамас, Нижний Новгород, Саратов, Ульяновск, Волгоград, Казань, Ижевск, Самара, Уфа, Пермь, Екатеринбург и Челябинск.

В этом же году компания ОАО «РЖД» увеличила протяженность магистральной квантовой сети в России в 2,9 раза по сравнению с предыдущим годом – до 3 295 км. К квантовой сети были подсоединены Санкт-Петербург, Москва, Нижний Новгород, Ростов-на-Дону и Казань.

В апреле 2024 года ПАО «Ростелеком» и ОАО «РЖД» построили опытную линию связи с использованием квантовых технологий между Москвой и центрами обработки данных (ЦОД) «Ростелеком» в Удомле (Тверская область), рядом с Калининской АЭС.

Планируется продлить участки магистральной квантовой сети до Сочи, Екатеринбурга и Челябинска. Также ожидается, что квантовые сети соединят Москву, Воронеж и Ростов-на-Дону, а также Нижний Новгород, Арзамас и Казань. Согласно данным ОАО «РЖД» в текущем 2024 году протяжённость квантовых сетей связи увеличится до 7 700 км [9].

Заключение

В ОАО «РЖД» отмечают, что кадровые потребности в квантовых коммуникациях до 2030 года составят свыше 1 000 специалистов с профильным высшим образованием, и более 7 000 специалистов со средним профессиональным образованием. В настоящее время в России более 30 вузов реализуют образовательные программы по подготовке специалистов в области квантовых коммуникаций. В 2020–2023 годах уже подготовлено более 400 специалистов по направлениям, связанным с квантовыми коммуникациями. При этом исторически вузы готовили по направлению квантовых коммуникаций исследователей и разработчиков. А в настоящее время отрасли уже требуются проектировщики, инженеры и эксплуатанты.

В рамках дорожной карты компания ОАО «РЖД» ведёт работу по созданию национальных стандартов технологий квантовых коммуникаций и квантового интернета вещей. Также разработкой стандартов занимается консорциум, в который, кроме ОАО «РЖД»,

входят Центры компетенций Национальной технологической инициативы (НТИ) на базе Сколтеха, Технический комитет 194 «Киберфизические системы» (ТК 194) и Технический комитет 26 «Криптографическая защита информации». Консорциум принимает активное участие в продвижении постквантовой криптографии, предлагая созданные решения коммерческим организациям и государственным структурам и проводя пилотные проекты для демонстрации возможных решений.

Основной целью мероприятий, проводимых ОАО «РЖД» является достижение технологического лидерства в области квантовых коммуникаций, создание конкурентоспособной отечественной индустрии в этой сфере, обеспечение технологической безопасности и суверенитета страны, стимулирование развития цифровой экономики и повышение качества жизни населения. ОАО «РЖД» взаимодействует с научными сообществами и технологическими компаниями в области внедрения квантовой технологии передачи и защиты данных, которые способствуют повышению эффективности бизнес-процессов компании, использования инфраструктуры, а также укреплению безопасности функционирования железнодорожного транспорта.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Heisenberg W. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. — Zeitschrift für Physik. — 1927. — Vol. 43. — P. 172–198. (Англ. перевод в кн.: Wheeler J. A., Zurek H. Quantum Theory and Measurement. — Princeton Univ. Press. — 1983. — P. 62–84).

2. Bennett C. H. Quantum cryptography: public key distribution and coin tossing / C. H. Bennett, G. Brassard // International Conference on Computers, Systems, and Signal Processing, Bangalore, 10–12 December 1984. — 1984. — Vol. 1. — P. 175–179.

3. Artur K. Ekert. Quantum Cryptography Based on Bell's Theorem // Physical Review Letters. — 1991. — Т. 67. — С. 661–663

4. Bennett C. H. Quantum cryptography using any two nonorthogonal states / C. H. Bennett // Physical review letters. — 1992. — Vol. 68, № 21. — P. 3121–3124.

5. Роенков, Д. Н. Применение квантовых линий связи / Д. Н. Роенков // Автоматика, связь, информатика. — 2019. — № 12. — С. 2–7. — DOI 10.34649/AT.2019.12.12.001.

6. Подписаны соглашения о намерениях между Правительством и крупнейшими компаниями о развитии отдельных высокотехнологичных направлений // Президент России: сайт. Москва. URL: <http://kremlin.ru/events/president/news/60971> (дата обращения: 10.09.2024).

7. Состоялся первый «квантовый звонок» между Москвой и Санкт-Петербургом // Пресс-центр ОАО «РЖД»: сайт. Москва. URL: <https://company.rzd.ru/ru/9397/page/104069?id=263377> (дата обращения: 10.09.2024).

8. Магистральная квантовая сеть РЖД: к 2030 году будет построено 15 тысяч км // РЖД цифровой: сайт. Москва. URL: <https://rzddigital.ru/events/k-2030-godu-rzhd-postroit-15-tys-km-kvantovoykh-setey/> (дата обращения: 10.09.2024).

9. РЖД к концу года удвоят протяженность магистральной квантовой сети. // ТАСС: информ. агентство России : сайт. Москва. Обновляется в течение суток. URL: <https://tass.ru/ekonomika/21962089> (дата обращения: 15.09.2024).

REFERENCES

1. Heisenberg W. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. — Zeitschrift für Physik. — 1927. — Vol. 43. — P. 172–198. (Wheeler J. A., Zurek H. Quantum Theory and Measurement. — Princeton Univ. Press. — 1983. — P. 62–84).

2. Bennett C. H. Quantum cryptography: public key distribution and coin tossing / C. H. Bennett, G. Brassard // International Conference on Computers, Systems, and Signal Processing, Bangalore, 10–12 December 1984. — 1984. — Vol. 1. — P. 175–179.

3. Artur K. Ekert. Quantum Cryptography Based on Bell's Theorem // Physical Review Letters. — 1991. — Т. 67. — С. 661–663

4. Bennett C. H. Quantum cryptography using any two nonorthogonal states / C. H. Bennett // Physical review letters. – 1992. – Vol. 68, № 21. – P. 3121–3124.

5. Roenkov, D. N. Application of quantum communication lines / D. N. Roenkov // Automation, communication, informatics. – 2019. – No. 12. – P. 2–7. – DOI 10.34649 / AT.2019.12.12.001.

6. Agreements of intent between the Government and the largest companies on the development of individual high-tech areas were signed // President of Russia: website. Moscow. URL: <http://kremlin.ru/events/president/news/60971>

7. The first «quantum call» took place between Moscow and St. Petersburg // Press center of JSC «Russian Railways»: website. Moscow. URL: <https://company.rzd.ru/ru/9397/page/104069?id=263377>

8. Russian Railways quantum backbone network: 15 thousand km will be built by 2030 // Russian Railways digital: website. Moscow. URL: <https://rzddigital.ru/events/k-2030-godu-rzhd-postroit-15-tys-km-kvantovykh-setey/>

9. Russian Railways to double the length of the quantum main network by the end of the year. // TASS: Information Agency of Russia: website. Moscow. Updated within 24 hours. URL: <https://tass.ru/ekonomika/21962089>

Информация об авторах

Козиевко Леонид Владимирович – к.т.н., доцент, доцент кафедры «Автоматика, телемеханика и связь», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: leo.kozienko@gmail.ru

Землянова Кристина Евгеньевна – студентка группы СОД.3–19–1, факультет «Системы обеспечения транспорта», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: zemlyanova.kristina103@mail.ru

Authors

Kozienko Leonid Vladimirovich – Ph.D. of Technical Sciences, Associate Professor of the Department of Automation, Telemechanics and Communications, Irkutsk State Transport University, Irkutsk, e-mail: leo.kozienko@gmail.ru

Zemlyanova Kristina Evgenievna – student of the group SOD.3–19–1, Department of Transport Support Systems, Irkutsk State Transport University, Irkutsk Irkutsk, e-mail: zemlyanova.kristina103@mail.ru