УДК 621.391.6:530.145

Романов Роман Романович студент
5 курс, Российский государственный университет нефти и газа
(НИУ) имени И.М. Губкина
Россия, г. Москва

КВАНТОВЫЙ ИНТЕРНЕТ: КОНЦЕПЦИЯ, ПРИНЦИПЫ РАБОТЫ И ПЕРСПЕКТИВЫ

Аннотация: В статье рассматриваются концептуальные основы квантового интернета — перспективной телекоммуникационной инфраструктуры, функционирующей на принципах квантовой механики. Проанализированы фундаментальные физические ограничения квантовых коммуникаций: теорема о запрете клонирования и принцип неопределённости Гейзенберга. Описана шестиуровневая дорожная карта эволюции квантовых сетей (Wehner et al.). Рассмотрены ключевые протоколы квантового распределения ключей (BB84, COW, MDI-QKD, DI-QKD), архитектура квантовых повторителей, физические платформы квантовой памяти, протоколы слепых квантовых вычислений, а также действующие экспериментальные системы, включая спутник «Micius».

Ключевые слова: квантовый интернет, квантовая запутанность, квантовое распределение ключей, BB84, MDI-QKD, квантовые повторители, квантовая память, слепые квантовые вычисления.

Romanov Roman Romanovich, student
5th year, Gubkin Russian State University of Oil and Gas (National Research University)
Russia, Moscow

QUANTUM INTERNET: CONCEPT, OPERATING PRINCIPLES AND PROSPECTS

Annotation: The article examines the conceptual foundations of the quantum internet — a prospective telecommunications infrastructure based on quantum mechanical principles. The no-cloning theorem and the Heisenberg uncertainty principle are discussed as the key physical constraints of quantum communications. The six-stage roadmap proposed by Wehner et al. is outlined. Key QKD protocols (BB84, COW, MDI-QKD, DI-QKD), quantum repeater architectures, physical quantum memory platforms, and blind quantum computing protocols are reviewed, alongside operational implementations including the Micius satellite.

Key words: quantum internet, quantum entanglement, quantum key distribution, BB84, MDI-QKD, quantum repeaters, quantum memory, blind quantum computing.

1. Введение

Развитие квантовых технологий открывает перспективу создания принципиально новой телекоммуникационной инфраструктуры — квантового интернета. Его концепция не предполагает замены существующего интернета: речь идёт о параллельной сети, способной передавать квантовые состояния между удалёнными узлами и реализовывать протоколы, недостижимые в рамках классической теории информации [1]. Ведущие исследовательские группы соотносят текущее состояние отрасли с периодом конца 1960-х годов в истории ARPANET, подчёркивая, что речь идёт не о гипотетической концепции, а об инженерной задаче с конкретными промежуточными этапами и измеримыми параметрами прогресса [2].

2. Физические основы квантовых коммуникаций

2.1. Теорема о запрете клонирования. Классические оптические сети усиливают сигнал, считывая и копируя входящий световой импульс на промежуточных узлах. В квантовых сетях такой подход неприменим: теорема о запрете клонирования доказывает, что невозможно создать

идеальную копию произвольного, заранее неизвестного квантового состояния [3]. Это следует из линейности квантовой механики: унитарный оператор копирования не может дублировать суперпозицию кубита без её разрушения. Следовательно, для дальней квантовой передачи необходимы принципиально иные методы.

2.2. Принцип неопределённости Гейзенберга и обнаружение перехвата. Принцип неопределённости Гейзенберга означает, что любое измерение квантового состояния фотона необратимо нарушает это состояние. Попытка злоумышленника перехватить квантовый канал приводит к коллапсу волновой функции передаваемых фотонов — возмущению, которое обнаруживается при сверке контрольной части ключа [4]. Данное свойство формирует физическую основу абсолютно безопасной криптографии: защита гарантируется законами природы, а не вычислительной сложностью алгоритмов.

2.3. Квантовая запутанность. Основным ресурсом квантового интернета является квантовая запутанность — состояние многочастичной системы, при котором квантовые характеристики отдельных частиц остаются коррелированными независимо от расстояния между ними [1]. Для двухкубитной системы максимально запутанные состояния образуют базис Белла:

$$|\Phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = (1/\sqrt{2})(|00\rangle - |11\rangle)$$
$$|\Psi^+\rangle = (1/\sqrt{2})(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)$$

Надёжное распределение состояний Белла между удалёнными узлами открывает возможность квантовой телепортации, защищённого распределения ключей и высокоточной синхронизации времени [1].

3. Стадии эволюции квантового интернета

Комплексная дорожная карта развития квантового интернета предложена Стефани Венер и соавторами в журнале Science в 2018 году [2]. Авторы выделяют шесть последовательных стадий (таблица 1), каждая из

которых расширяет функционал сети и предъявляет более высокие требования к аппаратному обеспечению.

Таблица 1. Стадии эволюции квантового интернета (по Wehner et al. [2])

Ст.	Название	Технологические требования	Доступный функционал
0	Доверенные узлы	Оптические каналы; доверие к промежуточным узлам; нет сквозной квантовой передачи	Базовые QKD-сети; объединение локальных сетей через защищённые ЦОД
1	Подготовка и измерение	Конечные узлы подготавливают и измеряют одиночные кубиты; прямая сквозная передача фотонов	Защищённая идентификация; QKD без доверенных узлов
2	Распределение запутанности	Генерация и распределение запутанных пар между любыми двумя узлами; долговременная память не требуется	DI-QKD; синхронизация атомных часов
3	Квантовая память	Локальная квантовая память в узлах; хранение состояний; локальные унитарные операции	Слепые квантовые вычисления (BQC); квантовая телепортация по запросу
4	Малокубитные отказоустойчивые сети	Малые квантовые процессоры с коррекцией ошибок (QEC)	Квантовая метрология; маломасштабные распределённые вычисления
5	Полноценные квантовые вычисления	Полномасштабные QC с неограниченными ресурсами коррекции ошибок	Алгоритмы Шора и Гровера в распределённом формате; глобальный квантовый консенсус

Большинство действующих коммерческих систем находится на стадии 0. Переход к стадиям 3–5 требует внедрения квантовых повторителей и когерентной памяти — компонентов, находящихся в стадии активных исследований.

4. Квантовое распределение ключей (QKD)

Квантовое распределение ключей (QKD) — наиболее практически отработанное приложение ранних стадий квантового интернета. Оно обеспечивает генерацию симметричного криптографического ключа между абонентами, связанными квантовым и классическим каналами.

4.1. Протоколы BB84 и COW. Первый протокол QKD — BB84 — разработан Беннеттом и Брассаром в 1984 году [4]. Алиса кодирует случайные биты в поляризацию одиночных фотонов, случайно выбирая один из двух неортогональных базисов ({0°, 90°} или {45°, 135°}). Боб независимо

выбирает базис для каждого измерения. После передачи стороны сопоставляют только использованные базисы по открытому каналу; совпавшие биты образуют «просеянный ключ». Любой перехват повышает уровень квантовых ошибок (QBER), сигнализируя о прослушивании.

Протокол COW (Coherent One-Way) адаптирован для существующих оптоволоконных сетей: вместо поляризации используются временны́е слоты, а безопасность контролируется через специальные «состояния-ловушки», проверяющие фазовую когерентность канала.

4.2. MDI-QKD и DI-QKD: защита от аппаратных атак. Физические реализации BB84 уязвимы к атакам на детекторы: злоумышленник может «ослепить» фотодетекторы Боба мощными импульсами. Протокол MDI-QKD (Lo, Curty, Qi, 2012) устраняет эту угрозу: оба абонента выступают только отправителями и направляют состояния транзитному узлу Чарли, который выполняет интерференционное измерение состояния Белла (BSM) и публично объявляет результат. Детекторы вынесены за периметр доверенной зоны, что делает систему невосприимчивой к любым атакам на детекторы [5].

Наиболее высокий уровень защиты обеспечивает DI-QKD: безопасность обосновывается исключительно нарушением неравенств Белла, а квантовые устройства рассматриваются как «чёрные ящики», не требующие доверия ни к источникам, ни к детекторам [2]. Для реализации DI-QKD суммарная ошибка при подготовке и измерении состояний не должна превышать 0,057 — условие, соответствующее переходу к стадии 2.

5. Квантовые повторители

Затухание в оптоволокне (~0,2 дБ/км) ограничивает прямую квантовую передачу расстояниями в 100–200 км. Квантовый повторитель передаёт запутанность без проективных измерений, разрушающих суперпозицию [3]. Два принципиальных подхода: повторители на базе квантовой памяти (дистанция разбивается на сегменты, в каждом генерируется локальная

запутанность, затем выполняется обмен запутанностью) и всецело фотонные повторители, использующие избыточные кластерные состояния — Repeater Graph States (RGS) — для устойчивости к потерям фотонов в канале [6].

5.1. Протокол обмена запутанностью. Обмен запутанностью позволяет установить квантовую корреляцию между частицами, никогда не взаимодействовавшими напрямую [3]. В базовой схеме: Алиса и Чарли совместно удерживают запутанную пару (1,2), Боб и Чарли — независимую пару (3,4). Чарли проводит BSM над частицами 2 и 3 и передаёт результат (два классических бита) Алисе и Бобу. Применив локальные унитарные преобразования (вентили Паули), они получают запутанную пару (1,4) — при том что каждая частица преодолела лишь половину общего расстояния.

5.2. Эффект Хонга–Оу–Манделя (HOM). Физическая реализация BSM опирается на HOM-эффект: два неразличимых фотона, попадая на разные входные порты симметричного светоделителя (50:50), вследствие деструктивной интерференции всегда выходят через один и тот же порт [7]. Вероятность одновременного срабатывания детекторов на разных выходах:

$$Pc = ½(1 - |\langle\psi_1|\psi_2\rangle|^2)$$

Для полностью неразличимых фотонов Pc = 0 («HOM-провал»). Наблюдение этого эффекта подтверждает неразличимость фотонов — необходимое условие работы повторителя.

6. Физические платформы квантовой памяти

Ключевая метрика квантовой памяти — время когерентности, определяющее максимальную длительность хранения квантового состояния до его декогеренции [8]. В таблице 2 приведено сравнение основных физических платформ.

Таблица 2. Сравнение платформ квантовой памяти

Платформа	Время когерентности	Ключевое преимущество	Основная сложность
Ионные	>30 мин	Точность операций $<10^{-3}$; зрелая	Несоответствие длин волн (~400–

ловушки		технология	800 нм) телекоммуникационному диапазону (~1550 нм)
Нейтральные атомы (EIT)	мс–с	Хорошая совместимость с одиночными фотонами	Шум управляющего лазерного луча при считывании
Кристаллы с РЗЭ ($Eu:Y_2SiO_5$)	до 6 ч [9]	Мультиплексирование по времени и частоте; «квантовая почта»	Необходимость динамического развязывания
NV/SiV-центры в алмазах	мс–с (ядра)	Оптическое управление; совместимость с ядерными спинами ^{13}C	Низкий КПД оптической эмиссии

Рисунок 1 наглядно иллюстрирует диапазон времён когерентности: он охватывает шесть порядков — от миллисекунд до нескольких часов. Редкоземельные кристаллы ($Eu:Y_2SiO_5$), где методы динамического развязывания позволили достичь шести часов [9], открывают возможность физической транспортировки памяти («квантовая почта») и использования на спутниковых ретрансляторах.

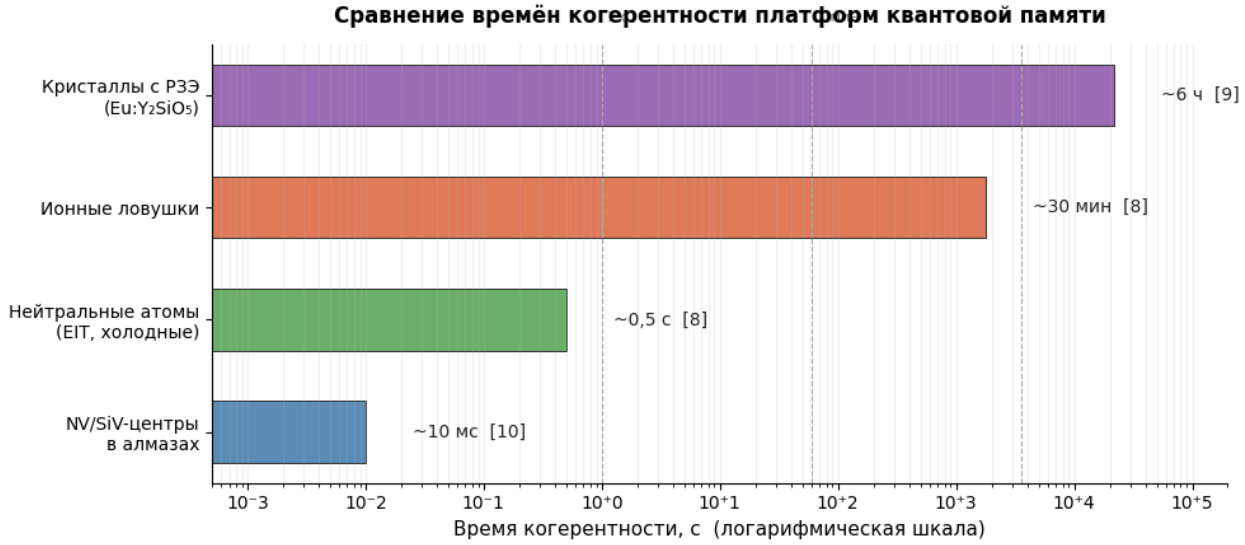

Рисунок 1. Сравнение времён когерентности платформ квантовой памяти (логарифмическая шкала)

7. Слепые квантовые вычисления (BQC)

По мере продвижения к стадиям 3–5 квантовый интернет откроет доступ к облачным квантовым вычислениям по модели «клиент–сервер». Задача доверия решается протоколами слепых квантовых вычислений (BQC): клиент направляет случайно подготовленные фотоны на сервер, который

формирует запутанное кластерное состояние и выполняет измерения в базисах, задаваемых клиентом. Параметры остаются скрытыми — сервер видит лишь усреднённую матрицу плотности, не содержащую информации о данных [10]. Экспериментальные реализации BQC на SiV-центрах в алмазах демонстрируют точность однокубитных вентилей на уровне 94,8% [11]. Параллельно разрабатываются схемы для полностью классического клиента, опирающиеся на постквантовую криптографию и доказательства с нулевым разглашением (zk-SNARKs).

8. Практические реализации

8.1. Спутниковые квантовые каналы. Оптоволоконные каналы, ограниченные затуханием ~0,2 дБ/км, практически непригодны для межконтинентальных квантовых магистралей. В 2016 году Китайская академия наук запустила спутник QUESS («Micius»). Под руководством профессора Цзянь-Вэй Паня были реализованы распределение запутанности, QKD и квантовая телепортация на расстоянии 1200 км [12]. Спутник обеспечил генерацию секретного ключа со скоростью ~1,1 кбит/с — результат, принципиально недостижимый для оптоволоконных систем на той же дистанции.

Рисунок 2 иллюстрирует разрыв между эффективностью волоконных и спутниковых каналов по мере роста расстояния: скорость генерации ключа для волокна убывает экспоненциально, тогда как спутниковый сегмент сохраняет работоспособность на масштабах свыше 1000 км.

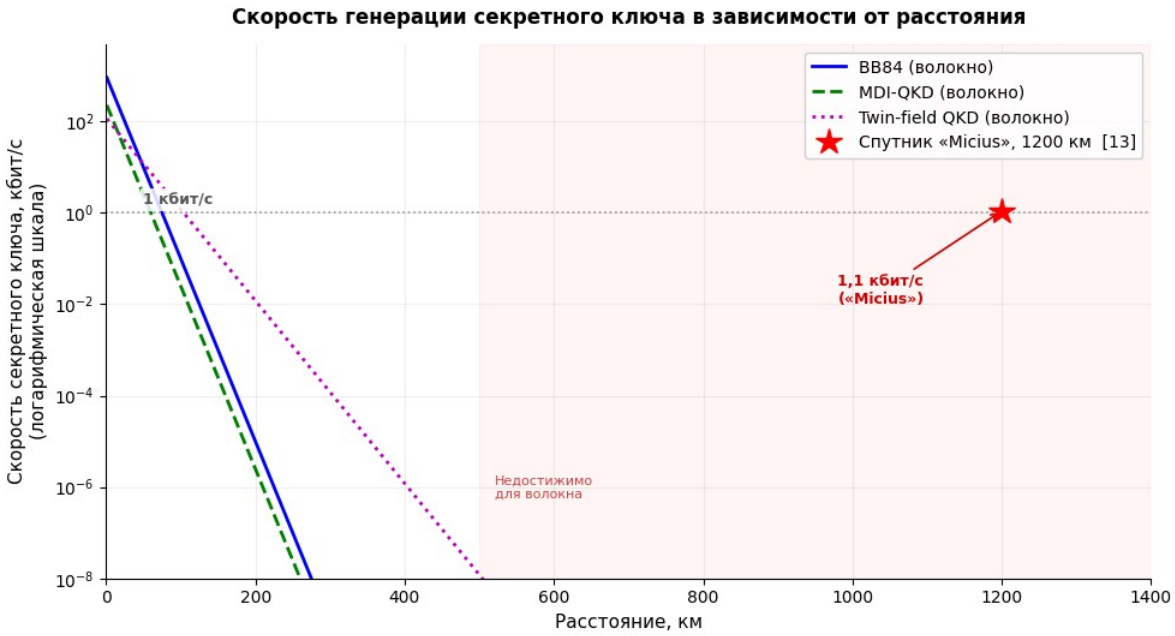

Рисунок 2. Скорость генерации секретного ключа как функция расстояния: волоконный канал vs спутниковый канал (по данным [12])

8.2. Наземные квантовые сети. В Европе альянс Quantum Internet Alliance (в том числе институт QuTech) реализует проект по созданию квантовой сети, связывающей четыре города Нидерландов — концептуальный аналог ранней ARPANET [2]. В России ОАО «РЖД» к 2025 году, по данным компании, развернуло волоконно-оптическую квантовую сеть протяжённостью около 8 тысяч километров, используя существующую железнодорожную инфраструктуру. Большинство действующих сетей функционируют на стадии 0; внедрение MDI-QKD и квантовых повторителей позволит перевести их на стандарты стадий 2–3.

Заключение

Квантовый интернет представляет собой технологическую задачу с конкретными промежуточными этапами и измеримыми параметрами прогресса, а не абстрактную концепцию. Теорема о запрете клонирования и принцип неопределённости Гейзенберга диктуют отказ от классических методов усиления в пользу обмена запутанностью и квантовой телепортации

— протоколов, математически обоснованных и экспериментально продемонстрированных.

Экспериментальный прогресс охватывает все ключевые направления: спутник «Micius» подтвердил работоспособность космического сегмента на 1200 км; редкоземельные кристаллы достигли шестичасового времени когерентности; протоколы BQC вплотную приблизились к практически значимым уровням точности. Успешное развёртывание глобального квантового интернета окажет определяющее влияние на криптографию, распределённые вычисления и фундаментальную науку.

Использованные источники:

1. Kimble H. J. The quantum internet // Nature. — 2008. — Vol. 453. — P. 1023–1030.
2. Wehner S., Elkouss D., Hanson R. Quantum internet: A vision for the road ahead // Science. — 2018. — Vol. 362, No. 6412. — eaam9288.
3. Wootters W. K., Zurek W. H. A single quantum cannot be cloned // Nature. — 1982. — Vol. 299. — P. 802–803.
4. Bennett C. H., Brassard G. Quantum cryptography: public key distribution and coin tossing // Theoretical Computer Science. — 2014. — Vol. 560. — P. 7–11.
5. Lo H.-K., Curty M., Qi B. Measurement-device-independent quantum key distribution // Physical Review Letters. — 2012. — Vol. 108. — 130503.
6. Azuma K., Tamaki K., Lo H.-K. All-photonic quantum repeaters // Nature Communications. — 2015. — Vol. 6. — 6787.
7. Hong C. K., Ou Z. Y., Mandel L. Measurement of subpicosecond time intervals between two photons by interference // Physical Review Letters. — 1987. — Vol. 59. — P. 2044–2046.
8. Duan L.-M., Lukin M. D., Cirac J. I., Zoller P. Long-distance quantum communication with atomic ensembles and linear optics // Nature. — 2001. — Vol. 414. — P. 413–418.

9. Zhong M., Hedges M. P., Ahlefeldt R. L. et al. Optically addressable nuclear spins in a solid with a six-hour coherence time // Nature. — 2015. — Vol. 517. — P. 177–180.

10. Broadbent A., Fitzsimons J., Kashefi E. Universal blind quantum computation // Proc. 50th Annual IEEE FOCS. — 2009. — P. 517–526.

11. Gritsch A. et al. Universal distributed blind quantum computing with solid-state qubits // Science. — 2025. — eadu6894.

12. Yin J., Cao Y., Li Y.-H. et al. Satellite-based entanglement distribution over 1200 kilometers // Science. — 2017. — Vol. 356, No. 6343. — P. 1140–1144.