УДК 004.056.5

Киселева Александра Игоревна, студент, РГУ нефти и газа (НИУ) имени И.М. Губкин, г. Москва

КВАНТОВЫЙ ИНТЕРНЕТ: КОНЦЕПЦИЯ, ПРИНЦИПЫ РАБОТЫ И ПЕРСПЕКТИВЫ

Аннотация

В статье рассматривается концепция квантового интернета как следующего поколения сетевых технологий, основанных на принципах квантовой механики. Проведен сравнительный анализ классического и квантового подходов к передаче данных, описаны ключевые компоненты архитектуры и фундаментальные принципы работы. Особое внимание уделено протоколу квантового распределения ключей BB84 как основе сверхзащищенных коммуникаций. В практической части работы выполнена симуляция данного протокола на языке Python в среде Google Colab. Моделирование позволило исследовать зависимость квантового уровня ошибок (QBER) от доли перехвата данных и уровня шума в канале, наглядно продемонстрировав способность квантовой криптографии обнаруживать попытки несанкционированного доступа. На основе полученных результатов и анализа современных тенденций определены перспективы развития глобальной квантовой сети до 2030 года.

Annotation

The article examines the concept of the quantum internet as the next generation of network technologies based on the principles of quantum mechanics. A comparative analysis of classical and quantum approaches to data transmission is carried out, the key components of the architecture and fundamental operating principles are described. Particular attention is paid to the BB84 quantum key distribution protocol

as the basis for ultra-secure communications. In the practical part of the work, a simulation of this protocol was performed in Python within the Google Colab. The modeling made it possible to investigate the dependence of the Quantum Bit Error Rate (QBER) on the fraction of intercepted data and the noise level in the channel, clearly demonstrating the ability of quantum cryptography to detect unauthorized access attempts. Based on the obtained results and analysis of current trends, the prospects for the development of a global quantum network up to 2030 are determined.

Ключевые слова: квантовый интернет, квантовая запутанность, квантовая криптография, протокол BB84, квантовое распределение ключей (QKD), уровень ошибок (QBER).
Keywords: quantum internet, quantum entanglement, quantum cryptography, BB84 protocol, quantum key distribution (QKD), quantum bit error rate (QBER),.

Квантовый интернет представляет собой следующее поколение сетевых технологий, которое использует принципы квантовой механики для передачи, обработки и хранения информации. В отличие от классического интернета, где данные передаются в виде битов (0 или 1), квантовый интернет опирается на кубиты, способные находиться в состоянии суперпозиции и запутанности. Это позволяет достигать беспрецедентного уровня безопасности и скорости в коммуникациях. Концепция квантового интернета возникла в начале 2000-х годов и активно развивается в последние годы благодаря прогрессу в квантовых вычислениях.

Квантовый интернет — это сеть квантовых устройств, соединенных каналами для передачи квантовых состояний, таких как запутанные фотоны. В отличие от классического интернета, он фокусируется на распределении запутанности для безопасной передачи данных, а не на прямой передаче битов. Ключевые компоненты: квантовые узлы (процессоры), повторяющие устройства (репитеры) и протоколы вроде QKD. По состоянию на 2026 год, разработки

включают интеграцию с существующими оптоволоконными сетями для гибридных систем. В таблице 1 проведен сравнительный анализ классического и квантового интернета.

Таблица 1 – Сравнительный анализ видов интернета

Аспект	Классический интернет	Квантовый интернет
Единица информации	Бит (0 или 1)	Кубит (суперпозиция состояний)
Передача данных	Электромагнитные сигналы (пакеты данных)	Квантовые состояния (фотоны, запутанность)
Безопасность	Шифрование на основе математики (RSA, AES)	Квантовая криптография (QKD, устойчивая к eavesdropping)
Скорость	Ограничена скоростью света	Потенциально мгновенная корреляция через запутанность, но с классическими ограничениями на сигнал
Основные проблемы	Уязвимость к хакерским атакам, потеря пакетов	Декогеренция, потери сигнала в каналах, необходимость в криогенных условиях
Масштабируемость	Легко масштабируется с помощью роутеров	Требует квантовых репитеров и entanglement swapping для дальних расстояний
Применения	Веб-серфинг, стриминг, облачные сервисы	Распределенные квантовые вычисления, сверхзащищенные коммуникации, квантовые сенсоры
Энергоэффективность	Относительно низкое потребление	Высокое потребление из-за охлаждения и лазеров, но потенциал оптимизации
Технологии передачи	Оптоволокно, беспроводные сети	Оптоволокно с низкими потерями, спутники для глобального покрытия
Устойчивость к ошибкам	Коррекция ошибок на основе повторов	Квантовая коррекция ошибок (QEC), устойчивость к шумам через purification

Принципы работы квантового интернета основаны на фундаментальных свойствах квантовой механики. К 2026 году эти принципы реализуются в реальных системах, включая интеграцию с классическим интернетом для гибридных сетей. Основные принципы квантовой механики в сети.

1. Суперпозиция: кубиты могут существовать в множестве состояний одновременно, позволяя параллельную обработку. В сети это используется для кодирования информации в поляризации фотонов.

2. Запутанность (entanglement): частицы связаны так, что измерение одной мгновенно определяет состояние другой. Это ключ к безопасной передаче без физического перемещения данных.

3. Теорема о нет-клонировании: невозможно скопировать неизвестное квантовое состояние, что предотвращает перехват данных.

4. Неопределенность Гейзенберга: ограничивает точность измерений, усиливая безопасность, но усложняя передачу.

Архитектура квантового интернета многоуровневая: физический слой (передача фотонов), квантовый слой (управление запутанностью), сетевой слой (маршрутизация). Ключевой протокол – Quantum Key Distribution (QKD), например BB84, где отправитель (Алиса) посылает поляризованные фотоны получателю (Бобу), а затем они сравнивают базы для генерации ключа. Любая попытка перехвата разрушает состояние, обнаруживая подслушивающее устройство (рисунок 1).

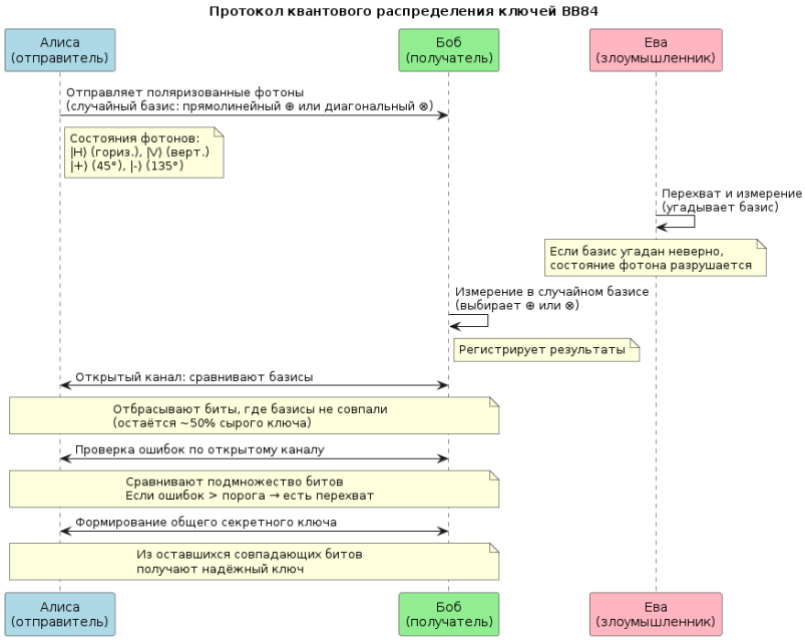

Рисунок 1 – Протокол квантового распределения ключей BB84

На схеме представлена последовательность действий при реализации протокола квантового распределения ключей BB84. Алиса отправляет Бобу фотоны, поляризованные в случайно выбранных базисах. Потенциальный перехватчик Ева пытается измерить фотоны, угадывая базис, что неизбежно вносит искажения. Боб также измеряет полученные фотоны в случайном базисе. После передачи по открытому классическому каналу Алиса и Боб сравнивают использованные базисы, отбрасывая события с несовпадением. Затем они выборочно проверяют уровень ошибок: если он превышает

пороговое значение, присутствие Евы обнаружено. В противном случае оставшиеся совпадающие биты формируют секретный ключ.

Для преодоления потерь в каналах используются квантовые репитеры. Они не усиливают сигнал (из-за нет-клонирования), а создают цепочку запутанных пар с последующим обменом: запутанность между A-B и B-C становится A-C (рисунок 2). К 2026 году репитеры интегрируются в сети, позволяя расстояния до тысяч км через спутники.

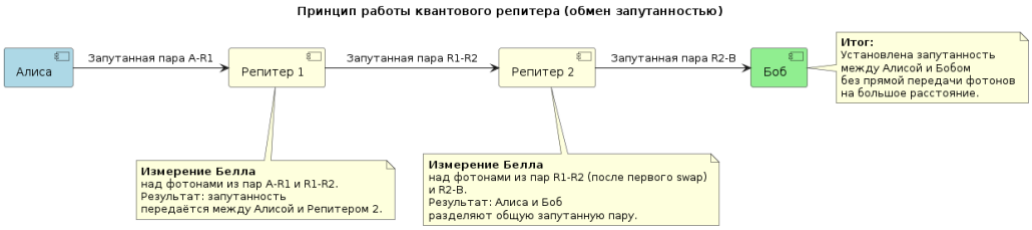

Рисунок 2 – Принцип работы квантовго репитера

Схема иллюстрирует принцип работы квантового репитера на основе обмена запутанностью для увеличения дальности передачи квантового состояния. Между Алисой и первым репитером, первым и вторым репитерами, вторым репитером и Бобом создаются три независимые запутанные пары фотонов. В каждом репитере выполняется измерение Белла над фотонами, принадлежащими соседним парам. В результате этих измерений запутанность «телепортируется»: Алиса и Боб оказываются обладателями общей запутанной пары, хотя непосредственно друг с другом фотоны не взаимодействовали.

Объектом исследования является процесс реализации квантового распределения ключей (QKD) как базового элемента архитектуры квантового интернета. Предметом – методы и средства симуляции протокола BB84 на классических вычислительных системах, включая вероятностное моделирование квантовых эффектов и анализ влияния внешних факторов на уровень ошибок (QBER).

Целью является исследование принципов работы квантового интернета и демонстрация фундаментальных свойств квантовой криптографии путем

разработки интерактивной симуляции протокола BB84 с визуализацией ключевых метрик.

Современные исследования в области квантовых коммуникаций фокусируются на переходе от теоретических моделей к практическим сетевым реализациям. В работах [1,2,3] описываются базовые принципы квантового распределения ключей и протокол BB84, заложивший основы криптографической защиты. Некоторые исследования посвящены проблеме декогеренции и потерь в оптоволоконных каналах, а также методам их компенсации с помощью квантовых репитеров и коррекции ошибок (QEC) [4,5]. Ряд авторов [6,7] рассматривают интеграцию QKD-систем в существующую оптоволоконную инфраструктуру для создания гибридных сетей, а также прогнозируют развитие глобальных квантовых сетей к 2030 году [8].

Данная статья выделяется практическим акцентом на создании интерактивной симуляции протокола BB84 в среде Google Colab. Для реализации симуляции использовались библиотеки: NumPy (для вероятностных расчетов и генерации случайных последовательностей), Matplotlib (для визуализации зависимостей QBER от параметров модели) и ipywidgets (для создания интерактивных элементов управления – слайдеров, кнопок). Проведем практическую симуляцию протокола BB84. Разработка кода проводилась поэтапно, с фокусом на ключевые компоненты протокола. Ниже описаны основные фрагменты кода и их функции.

1. Подготовка состояний Алисой. Этот блок генерирует случайные биты и базисы (0 для прямолинейного – горизонтальная/вертикальная поляризация; 1 для диагонального +/- 45°) для n фотонов. Ключевой расчет: случайная генерация с помощью np.random.randint, имитирующая подготовку квантовых состояний.

```
def alice_prepare_full(n):
    bits = np.random.randint(0, 2, n)
    bases = np.random.randint(0, 2, n)
    return bits, bases
```

2. Ева перехватывает долю фотонов (fraction), измеряет их в случайном базисе и пересылает измененные состояния. Ключевой расчет: если базис Евы совпадает с исходным, бит сохраняется; иначе – случайный бит. Это демонстрирует теорему о нет-клонировании: попытка копирования разрушает состояние, вводя ошибки.

```
def eve_intercept_full(bits, bases, fraction):
    n = len(bits)
    new_bits = bits.copy()
    new_bases = bases.copy()
    eve_indices = np.random.choice(n, size=int(fraction * n), replace=False)
    for i in eve_indices:
        eve_basis = np.random.randint(0, 2)
        eve_result = bits[i] if eve_basis == bases[i] else np.random.randint(0, 2)
        new_bits[i] = eve_result
        new_bases[i] = eve_basis
    return new_bits, new_bases
```

3. Измерение Бобом. Боб измеряет фотоны в случайных базисах. Ключевой расчет: если базис совпадает с текущим состоянием фотона, бит правильный, иначе – случайный.

```
def bob_measure_full(bits_sent, bases_sent, bases_bob):
    n = len(bits_sent)
    results = np.zeros(n, dtype=int)
    for i in range(n):
        results[i] = bits_sent[i] if bases_bob[i] == bases_sent[i] else np.random.randint(0, 2)
    return results
```

4. Просеивание ключей и расчет QBER. Сравниваются базисы, оставляются совпадающие позиции. QBER рассчитывается как доля ошибок в просеянном ключе.

```
def sift_keys(bases_alice, bases_bob, bits_alice, bits_bob):
    match = (bases_alice == bases_bob)
    return bits_alice[match], bits_bob[match]


def estimate_qber(sifted_alice, sifted_bob, sample_size=None):
```

```
    if sample_size and sample_size < len(sifted_alice):
        indices = np.random.choice(len(sifted_alice), sample_size, replace=False)
        errors = np.sum(sifted_alice[indices] != sifted_bob[indices])
        return errors / sample_size
    errors = np.sum(sifted_alice != sifted_bob)
    return errors / len(sifted_alice)
```

5. Интеграция шума и запуск симуляции . Добавляется шум как случайная инверсия битов (имитируя декогеренцию в каналах). Полная симуляция объединяет этапы и возвращает QBER и длину ключа.

```
def run_bb84_simulation(n_bits=1000, eve_fraction=0.0, noise_level=0.0, sample_size=100):
    # ... (вызов предыдущих функций)
    # Добавление шума:
    noise_mask = np.random.random(n_bits) < noise_level
    bits_bob[noise_mask] = 1 - bits_bob[noise_mask]
    sifted_alice, sifted_bob = sift_keys(...)
    qber = estimate_qber(sifted_alice, sifted_bob, sample_size)
    return qber, len(sifted_alice)
```

Для демонстрации перспектив квантового интернета, симуляция подчеркивает, как QKD может интегрироваться в будущие сети: низкий QBER обеспечивает безопасность, но шум и атаки требуют продвинутых решений, таких как квантовые репитеры и коррекция ошибок.

Ниже показаны результаты для различных настроек, иллюстрирующие переход от идеальных условий к реальным вызовам, что указывает на необходимость развития технологий для глобального квантового интернета.

Зададим начальные параметры, смоделируем лабораторные условия без внешних помех. На рисунке 3 видно, что QBER ≈0%, а длина ключа примерно 506 (примерно половина исходных бит из-за случайного совпадения базисов). График зависимости QBER от активности Евы начинается строго с нуля и плавно растёт до 0.26 при полной активности Евы. Красная линия 10 % пересекается примерно при доле 0.35–0.4.

Это «эталонный» случай, когда протокол работает идеально. Отсутствие ошибок подтверждает фундаментальный принцип: без подслушивания и шума

ключ генерируется без потерь. В будущем квантовом интернете такие условия будут достигаться с помощью современных QKD-систем.

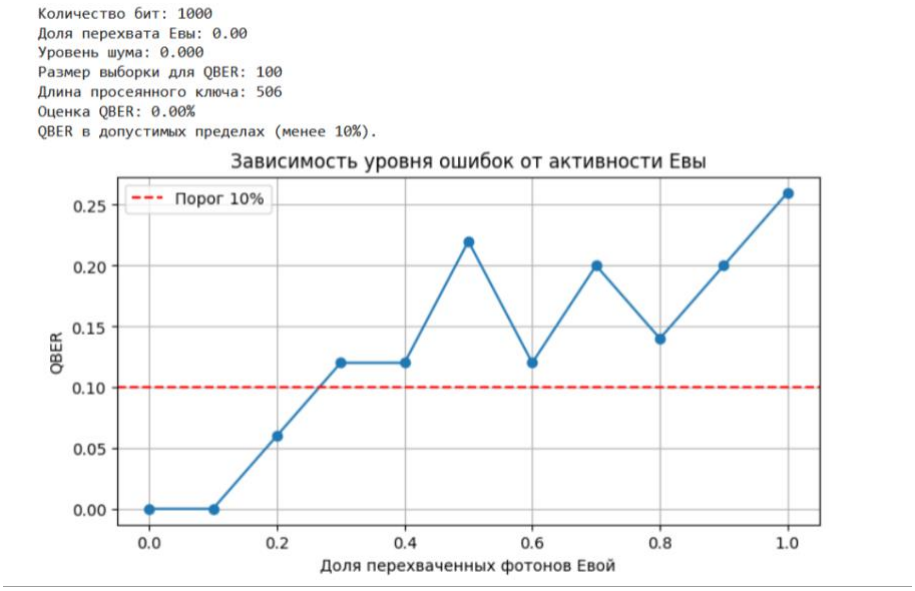

Рисунок 3 - Зависимость QBER от доли перехвата Евы в идеальном канале

Изменим параметры, увеличив активность Евы до 40 % (умеренная атака, имитирующая реальную угрозу), сохранив noise_level=0.0. На рисунке 4 видно, что QBER возрастает до 7%, длина ключа равная 523. График теперь стартует с чуть более высокого, но уже при 0.4 достигает 0.10–0.11 и дальше резко растёт до 0.32. Порог 10 % пересекается раньше – около 0.35–0.4.

Это указывает, что даже умеренная атака (всего 40 % фотонов) поднимает QBER почти до критического уровня. Это наглядно демонстрирует «встроенную сигнализацию» протокола BB84: Ева не может подслушать незаметно. Это означает, что любая попытка перехвата в глобальной сети будет мгновенно обнаружена, что делает QKD принципиально устойчивее классического шифрования.

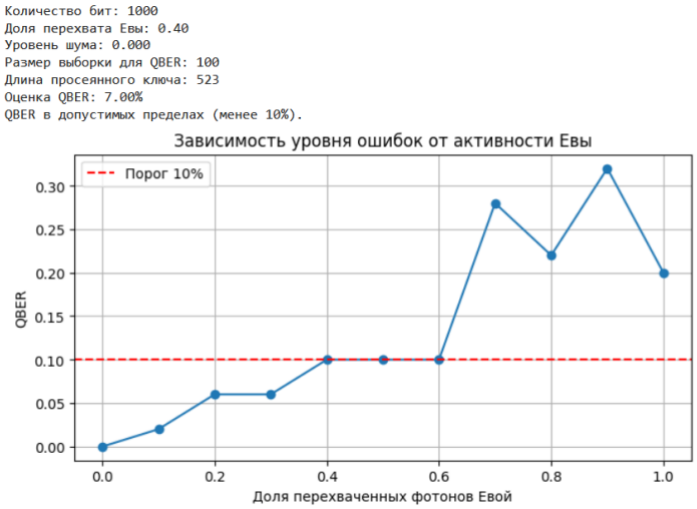

Рисунок 4 - Зависимость QBER от доли перехвата Евы при умеренной атаке.

Далее уберем Еву (0 %), но добавим реалистичный шум канала = 5 % (имитация декогеренции и потерь в оптоволокне). На рисунке 5 видно, что QBER 5%, а график смещён вверх: даже при нулевой активности Евы QBER уже ≈ 0.03–0.05, а при полной активности поднимается до 0.28. Порог 10 % пересекается примерно при 0.35.

Это демонстрирует, что шум сам по себе создаёт «фоновые» ошибки. Это главная практическая проблема сегодняшних QKD-систем. Именно поэтому так активно разрабатываются квантовые репитеры и протоколы коррекции ошибок, чтобы снизить влияние шума и достичь тысяч километров.

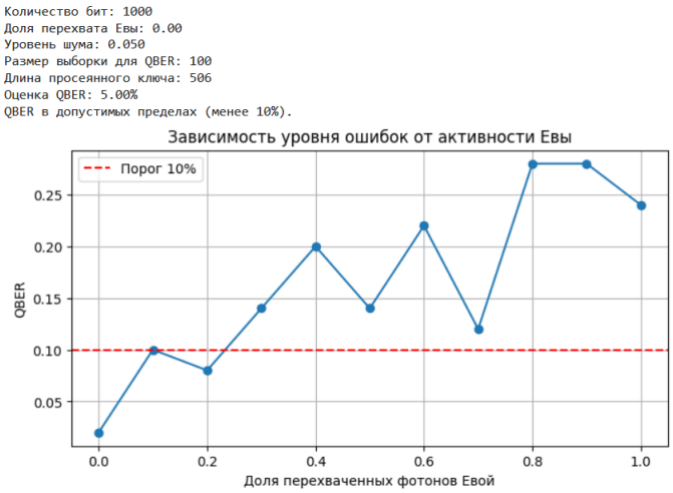

Рисунок 5 - Зависимость QBER от доли перехвата Евы при наличии шума

Наконец, комбинируем eve_fraction=0.5 и noise_level=0.1 (реалистичный сценарий для будущих гибридных сетей). На рисунке 6 видно, что QBER ≈

4.00%, длина ключа = 482. График стартует с низкого уровня, но уже при 0.2–0.3 пересекает 10 % и дальше растёт почти линейно до 0.34.

Из этого можно сделать вывод, что когда атака и шум действуют вместе, их эффекты складываются. Даже очень слабое вмешательство Евы на фоне реального шума канала может приблизить систему к порогу 10%. Это показывает, почему в будущих квантовых сетях потребуется многоуровневая защита: не только QKD, но и квантовые репитеры, пост-квантовые алгоритмы и мониторинг QBER в реальном времени.

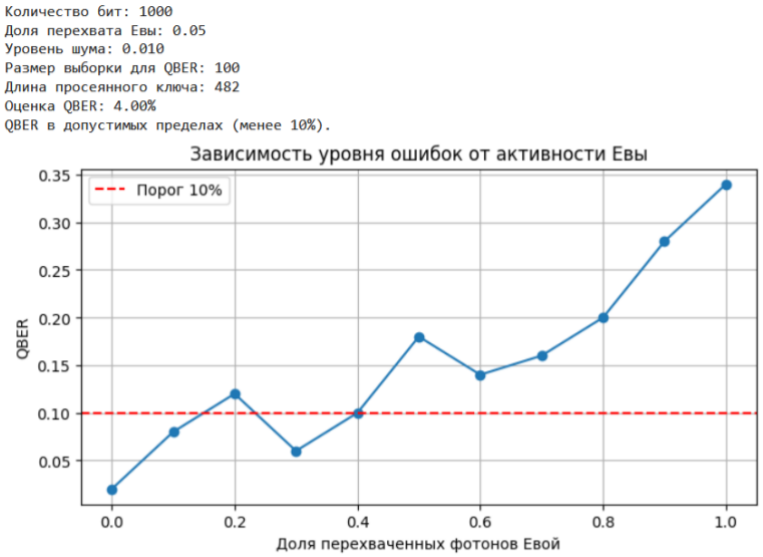

Рисунок 6 - Зависимость QBER от доли перехвата Евы в комбинированном

На основе проведенного в статье исследования продемонрировано, что перспективы квантового интернета выглядят многообещающими, но сопряжены с вызовами. Симуляция показала как квантовая криптография обнаруживает перехват через рост уровня ошибок, подчеркивая фундаментальную безопасность. Это особенно актуально для преодоления уязвимостей классического интернета, таких как кибератаки на шифрование. К 2026 году, согласно экспертным прогнозам, квантовый интернет перейдет от экспериментальных демонстраций к ранним коммерческим приложениям, интегрируясь с существующими инфраструктурами для гибридных систем. Ключевые перспективы включают следующие аспекты.

1. Сверхзащищенные коммуникации: квантовое распределение ключей обеспечит "невзламываемые" каналы к 2035 году, революционизируя

финансы, здравоохранение (безопасная передача геномных данных) и оборону. Симуляция в статье показала, как даже умеренная атака повышает уровень ошибок до 7–8%, позволяя своевременно обнаруживать угрозы.

2. Распределенные квантовые вычисления: к 2030 году сети позволят объединять квантовые компьютеры, обеспечивая масштабируемые вычисления для искусственного интеллекта, материаловедения и фармацевтики. Прогресс в обмене запутанностью и квантовых репитерах решит проблему декогеренции (второй сценарий).

3. Глобальная инфраструктура: к 2030 году ожидаются первые коммерческие услуги в развитых странах, с панъевропейской сетью в ЕС и национальной в Японии. Это интегрируется с сетями 6G для повсеместного квантового взаимодействия, но требует решения вызовов, таких как квантовая память с более длительным временем когерентности и фотонно-интегральные схемы для квантового распределения ключей.

4. Экономическое и социальное влияние: рост квантово-устойчивых блокчейн-систем и защищенных систем голосования к 2032 году. Однако с приближением "дня Q" (когда квантовые компьютеры смогут взломать RSA) срочность перехода на постквантовую криптографию возрастает.

Вызовы включают масштабирование и интеграцию с классическими сетями, но прогресс в фотонных кубитах и гибридных архитектурах ускорит реализацию. Прогнозируется, что квантовый интернет не только усилит безопасность, но и откроет эру распределенных вычислений. Для наглядности представим временную шкалу ключевых вех: прошлые достижения и прогнозируемые (на основе экспертных оценок и рыночных тенденций). Это иллюстрирует эволюцию от теоретических идей к глобальной инфраструктуре (рисунок 7).

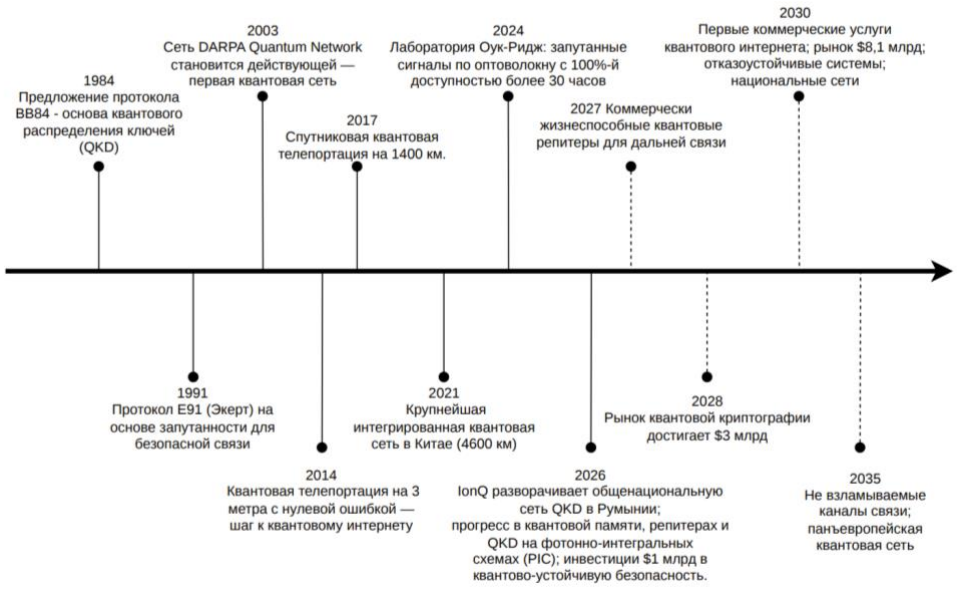

Рисунок 7 – Временная шкала

В ходе выполнения работы была исследована концепция квантового интернета, основанная на фундаментальных принципах квантовой механики – суперпозиции, запутанности и теореме о нет-клонировании. Проведенный сравнительный анализ подтвердил, что квантовый подход к передаче данных обладает принципиальными преимуществами в области безопасности по сравнению с классическими сетями, что обусловлено самой природой квантовых состояний. Полученные результаты подчеркивают, что развитие квантовых сетей открывает перспективы создания глобальной защищенной коммуникационной инфраструктуры к 2030 году.

Список литературы

1. Эттель В.А. Квантовая криптография: квантовое распределение ключей / В.А. Эттель, Т.А. Эм // Международный научно-исследовательский журнал. — 2012. — №5 (5). — URL: https://research-journal.org/archive/6-5-2012-october/kvantovaya-kriptografiya-kvantovoe-raspredelenie-klyuchej (дата обращения 25.02.2026).

2. Данеев О. В. О проблеме квантового распределения ключей: состояние и перспективы // Хроноэкономика. 2020. №2 (23). URL: https://cyberleninka.ru/article/n/o-probleme-kvantovogo-raspredeleniya-klyuchey-sostoyanie-i-perspektivy (дата обращения: 28.02.2026).

3. Бурлаков Е. В., Коробов А. В. Ключевые особенности протоколов квантового распределения ключей на непрерывных переменных //РЭНСИТ: Радиоэлектроника. Наносистемы. Информационные технологии. – 2024. – Т. 16. – №. 2. – С. 255 (дата обращения: 03.03.2026).
4. Goncharenko D.K. Development of methods for increasing the length of a fiber-optical communication channel of a quantum-cryptographic system / D.K. Goncharenko, O.A. Kulish, A.V. Ivakhnenko et al. // International Research Journal. — 2019. — №6 (84). — URL: [object Object] (Accessed date 11.03.2026). — DOI: 10.23670/IRJ.2019.84.6.002 (accessed: 03/05/2026).
5. Гушанский С. М., Потапов В. С. Исследование квантовой вычислительной системы и реализация квантового ядра на ПЛИС //Известия Южного федерального университета. Технические науки. – 2022. – №. 5 (229). – С. 141-151 (дата обращения: 05.03.2026).
6. Muga N. J. et al. Coexistence of classical and quantum signals in hybrid fiber and free-space optics links for qkd integration //2024 24th International Conference on Transparent Optical Networks (ICTON). – IEEE, 2024. – С. 1-5 (дата обращения: 07.03.2026).
7. Xu Y., Chen L., Zhu H. Quantum key distribution scheme with key recycling in integrated optical network //International Journal of Theoretical Physics. – 2023. – Т. 62. – №. 5. – С. 103 (дата обращения: 10.03.2026).
8. Малинецкий Г. Г., Ахромеева Т. С., Торопыгина С. А. Перспективы, проблемы и развитие квантовых технологий //Препринты Института прикладной математики им. МВ Келдыша РАН. – 2025. – №. 0. – С. 66-56 (дата обращения: 13.03.2026).

References

1. Ettel V.A. Quantum cryptography: quantum key distribution / V.A. Ettel, T.A. Em // International Scientific Research Journal. — 2012. — №5 (5). — URL: https://research-journal.org/archive/6-5-2012-october/kvantovaya-kriptografiya-kvantovoe-raspredelenie-klyuchej (accessed 02/25/2026).

2. Daneev O. V. On the problem of quantum key distribution: the state and prospects // Chronoeconomics. 2020. No. 2 (23). URL: https://cyberleninka.ru/article/n/o-probleme-kvantovogo-raspredeleniya-klyuchey-sostoyanie-i-perspektivy (date of request: 02/28/2026).
3. Burlakov E. V., Korobov A.V. Key features of protocols for quantum key distribution on continuous variables //RENSIT: Radioelectronics. Nanosystems. Information technology. – 2024. – Vol. 16. – No. 2. – p. 255 (accessed 03.03.2026).
4. Goncharenko D.K. Development of methods for increasing the length of a fiber-optical communication channel of a quantum-cryptographic system / D.K. Goncharenko, O.A. Kulish, A.V. Ivakhnenko et al. // International Research Journal. — 2019. — №6 (84). — URL: [object Object] (Accessed date 11.03.2026). — DOI: 10.23670/IRJ.2019.84.6.002 (accessed: 03/05/2026).
5. Gushansky S. M., Potapov V. S. Research of a quantum computing system and implementation of a quantum core on FPGAs //Proceedings of the Southern Federal University. Technical sciences. – 2022. – №. 5 (229). – Pp. 141-151 (accessed: 03/05/2026).
6. Muga N. J. et al. Coexistence of classical and quantum signals in hybrid fiber and free-space optics links for qkd integration //2024 24th International Conference on Transparent Optical Networks (ICTON). – IEEE, 2024. – pp. 1-5 (accessed: 03/07/2026).
7. Xu Y., Chen L., Zhu H. Quantum key distribution scheme with key recycling in integrated optical network //International Journal of Theoretical Physics. – 2023. – Vol. 62. – No. 5. – p. 103 (accessed: 03/10/2026).
8. Malinetsky G. G., Akhromeeva T. S. Toropygina S. A. Prospects, problems and development of quantum technologies //Preprints of the Institute of Applied Mathematics named after MV Keldysh RAS. – 2025. – №. 0. – Pp. 66-56 (accessed: 03/13/2026).