УДК 004.31

EDN FDNUCD

Фундаментальные основы и перспективы квантовых вычислений

Н.А. Днепровский[1*], П.М. Урвачев[2]

[1]Студент, ФГБОУ ВО «Кубанский Государственный Технологический Университет», Краснодар, Россия
[2]Старший преподаватель кафедры информационных систем и программирования ФГБОУ ВО «Кубанский Государственный Технологический Университет», Краснодар, Россия

*E-mail: dneprowsky2021@yandex.com

Аннотация. Статья посвящена исследованию фундаментальных принципов квантовых вычислений и их практического потенциала. В первом разделе рассматривается природа кубита как базового элемента квантовых систем и его принципиальные отличия от классического бита. Во втором разделе анализируется феномен суперпозиции как ключевой ресурс квантового превосходства. Третий раздел освещает явление квантовой запутанности и его роль в создании квантовых систем. Четвертый раздел посвящен перспективам практического применения квантовых вычислений в криптографии, материаловедении и искусственном интеллекте. Статья подчеркивает трансформационный потенциал квантовых технологий для решения вычислительных задач, недоступных классическим компьютерам.

Ключевые слова: квантовые вычисления, кубит, суперпозиция, квантовая запутанность, квантовые алгоритмы.

Fundamental principles and prospects of quantum computing

N.A. Dneprovsky[1*], P.M. Urvachev[2]

[1]Student of Kuban State Technological University, Russia, Krasnodar
[2]Senior Lecturer of the Department of Information Systems and Programming Kuban State Technological University, Russia, Krasnodar

[*]E-mail: .dneprowsky2021@yandex.com

Abstract. This article explores the fundamental principles of quantum computing and its practical applications. The first section focuses on the nature of the qubit as the basic unit of quantum systems and its key differences from classical bits. The second section analyzes the phenomenon of superposition as a key resource for quantum supremacy. The third section highlights the concept of quantum entanglement and its role in creating quantum systems. The fourth section focuses on the practical applications of quantum computing in cryptography, materials science, and artificial intelligence. The article highlights the transformative potential of quantum technologies for solving computational problems that are beyond the capabilities of classical computers.

Keywords: quantum computing, qubit, superposition, quantum entanglement, quantum algorithms.

1. Введение

Квантовые вычисления представляют собой одну из наиболее перспективных технологий XXI века, способную кардинально изменить подходы к обработке информации [1-2]. В отличие от классических компьютеров, основанных на архитектуре фон Неймана, квантовые вычислительные системы используют фундаментальные принципы квантовой механики для решения задач, недоступных даже самым мощным современным суперкомпьютерам [3-4].

Основная цель данной работы - систематизировать знания о фундаментальных принципах квантовых вычислений и проанализировать их практический потенциал. В рамках исследования рассматриваются такие ключевые аспекты, как природа кубита, явления суперпозиции и квантовой запутанности, а также перспективные направления практического применения квантовых технологий [5-6].

2. Материалы и методы

Исследование проводилось на основе анализа научной литературы и публикаций в рецензируемых журналах за период 2022-2025 годов. Для систематизации информации использовались методы сравнительного анализа и синтеза данных из различных источников, включая российские научные журналы "Успехи физических наук", "Квантовая электроника" и "Автоматика, связь, информатика" [7-9].

Методология исследования включала изучение математических моделей квантовых систем, анализ экспериментальных данных по созданию и управлению кубитами, а также оценку перспектив практической реализации квантовых алгоритмов. Особое внимание уделялось работам российских исследователей в области сверхпроводящих кубитов и квантовой запутанности [10].

3. Результаты и обсуждение

3.1. Кубит: фундаментальный элемент квантовых вычислений

Кубит представляет собой квантовый аналог классического бита, однако обладает принципиально иными свойствами [3]. В отличие от классического бита, который может находиться строго в состоянии 0 или 1, кубит может существовать в суперпозиции этих

состояний. Это означает, что до момента измерения кубит одновременно содержит в себе оба базисных состояния с определенными вероятностями [5].

Математически состояние кубита описывается вектором в гильбертовом пространстве: $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, где α и β - комплексные амплитуды вероятности, удовлетворяющие условию нормировки $|\alpha|^2 + |\beta|^2 = 1$ [7]. Для визуализации состояния кубита используется сфера Блоха (Рисунок 1), где каждая точка на поверхности сферы соответствует определенному квантовому состоянию.

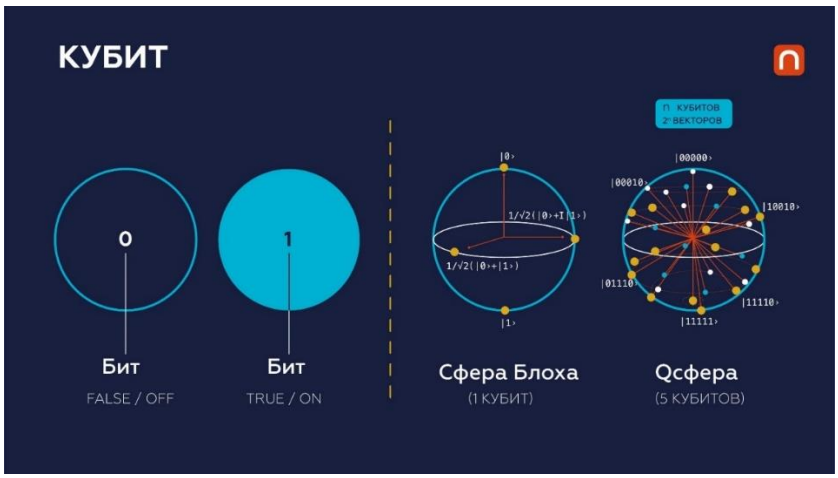

Рисунок 1. Сфера Блоха - геометрическое представление состояния кубита.

3.2. Суперпозиция как основа квантового превосходства

Суперпозиция является краеугольным камнем квантовых вычислений [5-7]. Это фундаментальное свойство, которое кардинально меняет классические представления об обработке информации.

Классический бит, аналогичный выключателю, может находиться только в одном из двух четко определенных состояний: 0 или 1 [1]. Система из N бит может хранить лишь одну из 2^N возможных комбинаций в любой момент времени. Вычисления осуществляются путем последовательного перебора и изменения этих состояний.

Вероятностная природа кубитов. Состояние кубита математически описывается вектором: $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, где $|0\rangle$ и $|1\rangle$ — ортонормированные базисные состояния, а α и β — комплексные амплитуды вероятности, удовлетворяющие условию нормировки $|\alpha|^2 + |\beta|^2 = 1$. Вероятность получения соответствующего базисного состояния при измерении равна квадрату модуля его амплитуды [6].

Ключевое преимущество проявляется при рассмотрении многокубитных систем. Система из N кубитов существует в суперпозиции всех 2^N возможных классических состояний: $|\Psi\rangle = \Sigma\ \alpha_i\ |i\rangle$, где $|i\rangle$ обозначает i-е базисное состояние (например, $|00...0\rangle$, $|00...1\rangle$, ..., $|11...1\rangle$) [7].

Это означает, что квантовая операция, применяемая к такой системе, действует на все 2^N состояний одновременно. Данный феномен известен как квантовый параллелизм. Его вычислительная мощность растет экспоненциально с ростом числа кубитов:

- 3 кубита — суперпозиция 8 состояний
- 10 кубитов — суперпозиция 1024 состояний
- 300 кубитов — суперпозиция ~2^{300} состояний, что превышает количество атомов в наблюдаемой Вселенной

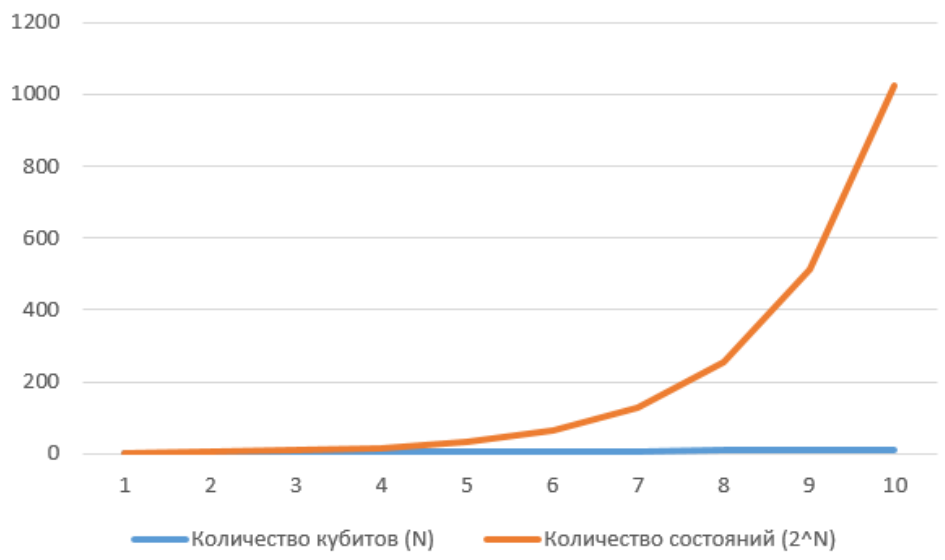

Рисунок 2. Экспоненциальный рост количества состояний.

Таким образом, квантовый процессор, манипулируя системой из сотен кубитов, оперирует с пространством состояний, не поддающимся классическому моделированию в силу его экспоненциальной размерности.

Рисунок 3. Квантовый процессор от IBM.

Важнейшее ограничение: Проблема измерения. Непосредственный доступ ко всем результатам суперпозиции невозможен. При измерении система коллапсирует в одно случайное классическое состояние с вероятностью, определяемой квадратами амплитуд [8]. Следовательно, стратегия квантовых алгоритмов заключается не в простом получении всех ответов, а в когерентном управлении амплитудами вероятностей таким образом, чтобы амплитуды неверных решений подавлялись за счет деструктивной интерференции; амплитуда верного решения усиливалась за счет конструктивной интерференции.

В результате при измерении система с высокой вероятностью оказывается в состоянии, соответствующем верному результату [9].

Суперпозиция является не абстрактной концепцией, а конкретным вычислительным ресурсом. Это способность квантовой системы осуществлять параллельные вычисления в экспоненциально большом пространстве состояний в рамках одного физического процесса. Применение этого ресурса открывает путь к решению задач, недоступных для классических суперкомпьютеров [10].

3.3. Квантовая запутанность: принцип нелокальной связи

Квантовая запутанность представляет собой фундаментальное физическое явление, при котором квантовые состояния двух или более частиц образуют единую связанную систему [6-8]. Это свойство лежит в основе современных квантовых технологий и кардинально отличает квантовые системы от классических.

Физические основы явления. Возникновение запутанности связано с особенностями описания составных квантовых систем в формализме квантовой механики. Состояние такой системы описывается неделимым вектором в тензорном произведении гильбертовых пространств подсистем. Одним из канонических примеров запутанного состояния является состояние Белла: $|\Phi^+\rangle = 1/\sqrt{2}\,(|00\rangle + |11\rangle)$ [7].

Экспериментальное подтверждение. Существование квантовой запутанности подтверждено многочисленными экспериментами по проверке неравенств Белла. Нарушение этих неравенств в экспериментах с фотонными парами, ионами и сверхпроводящими кубитами доказывает неклассический характер корреляций в квантовых системах [9-10].

Прикладные аспекты:

- Квантовые вычисления - запутанность является необходимым ресурсом для реализации квантовых алгоритмов, включая алгоритм Шора и алгоритм Гровера [8]
- Квантовая криптография - протоколы квантового распределения ключей используют свойства запутанных состояний для обеспечения безопасности передачи информации [9]
- Квантовая метрология - использование запутанных состояний позволяет преодолеть стандартный квантовый предел точности измерений [10]
- Квантовые сети - создание распределённых запутанных состояний является основой для разработки квантового интернета [10]

Основные проблемы в исследовании и использовании запутанности включают: борьбу с декогеренцией и шумами в квантовых системах; разработку эффективных методов генерации и распределения запутанных состояний; создание методов верификации и квантовой томографии для многокубитных систем; масштабирование квантовых систем с сохранением качества запутанности [9-10].

3.4. Практическое применение квантовых технологий

Теоретическая мощь квантовых вычислений обретает реальную значимость только в контексте конкретных приложений, способных коренным образом изменить наши технологические возможности [7-9].

Криптография: угроза и смена парадигмы безопасности

Проблема: Уязвимость современных стандартов шифрования. Вся современная цифровая экономика — от банковских транзакций до защищённых мессенджеров — основана на криптографических системах с открытым ключом, таких как RSA и ECC (Elliptic Curve Cryptography) [2]. Их стойкость зиждется на вычислительной сложности определённых математических задач. Для RSA, например, это задача разложения очень большого числа на простые множители. Классическому компьютеру для решения этой задачи при длине ключа в 2048 бит потребуется время, превышающее возраст Вселенной [6].

Квантовая угроза: Алгоритм Шора. В 1994 году Питер Шор разработал квантовый алгоритм, который позволяет эффективно решать задачу факторизации и дискретного логарифмирования (основу ECC) [8]. На достаточно мощном квантовом компьютере (оценки говорят о нескольких тысячах устойчивых к ошибкам кубитов) взлом ключа RSA из 2048 бит из задачи космического масштаба превратится в операцию, занимающую часы или дни. Это создаёт так называемую «квантовую угрозу» для всей существующей инфраструктуры цифровой безопасности [9].

Решение: Постквантовая и квантовая криптография. В ответ на эту угрозу развиваются два направления: постквантовая криптография - разработка новых классических алгоритмов шифрования, основанных на математических задачах, устойчивых к атакам как классических, так и квантовых компьютеров; квантовая криптография (QKD - Quantum Key Distribution) - использование фундаментальных принципов квантовой механики для безопасного распределения ключей [10].

Разработка лекарств и материалов: прямое моделирование природы

Проблема: Сложность точного квантового моделирования. Химия и наука о материалах по своей сути являются квантовыми [7]. Чтобы предсказать свойства новой молекулы (скажем, лекарственного препарата), её реакционную способность или прочность нового материала, необходимо смоделировать поведение её электронов. Точное решение уравнений квантовой механики для систем, состоящих всего из нескольких десятков частиц, требует от классического суперкомпьютера астрономических вычислительных ресурсов из-за экспоненциального роста сложности [8].

Квантовое решение: Естественное моделирование. Квантовый компьютер, будучи сам квантовой системой, способен естественным образом моделировать другие квантовые системы [9]. Кубиты могут быть настроены так, чтобы представлять электроны в молекуле. В

этом случае эволюция квантового процессора будет напрямую отражать поведение моделируемой молекулы. Это позволит: ускорить разработку лекарств - точное моделирование взаимодействия молекул-кандидатов с белками организма, что сократит время и стоимость доклинических испытаний; создать новые материалы - расчёт свойств сверхпроводников, работающих при комнатной температуре, высокоэффективных катализаторов для снижения энергозатрат в промышленности или новых поколений аккумуляторов [10].

Искусственный интеллект и оптимизация: ускорение поиска решений

Проблема: Перебор в сложных системах. Многие практические задачи в машинном обучении, логистике и финансах сводятся к поиску оптимального решения среди огромного числа вариантов (так называемые NP-трудные задачи) [7]. Примеры: задача коммивояжёра - найти кратчайший маршрут через десятки тысяч городов; оптимизация портфеля - выбрать наилучшее распределение активов на финансовом рынке с учётом тысяч параметров и рисков; обучение сложных моделей ИИ - подбор оптимальных параметров для глубоких нейронных сетей [8].

Квантовое решение: Структурный поиск с помощью интерференции. Квантовые алгоритмы, такие как алгоритм Гровера, предлагают принципиально иной подход [9]. Вместо последовательного перебора они используют интерференцию амплитуд вероятности. Алгоритм Гровера позволяет квадратично ускорить поиск в неструктурированной базе данных. Это означает, что для поиска среди N элементов вместо N попыток потребуется порядка $\sqrt{N}$ квантовых операций. Хотя ускорение не экспоненциальное, как у алгоритма Шора, оно критически важно для огромных массивов данных [10].

Перспективы: логистика - оптимизация глобальных цепочек поставок и маршрутов транспорта; финансы - более точное и быстрое оценка рисков, выявление мошеннических схем; искусственный интеллект - ускорение обучения машин и открытие новых, более эффективных архитектур нейронных сетей [9-10].

4. Заключение

Проведенный анализ позволяет выделить три фундаментальных принципа, составляющих основу квантовых вычислений [7-9]. Кубит, обладающий свойством суперпозиции, представляет собой базовый элемент квантовой информации. Суперпозиция состояний обеспечивает квантовый параллелизм, позволяя одновременно обрабатывать экспоненциально большое пространство решений. Квантовая запутанность создает сильные корреляции между кубитами, формируя единую систему с неклассическими свойствами [10].

Перспективы развития связаны с созданием гибридных вычислительных систем, где квантовые и классические процессоры решают задачи в соответствии с их преимуществами [8-9]. Квантовые устройства предполагается использовать для задач молекулярного моделирования и оптимизации, в то время как классические компьютеры обеспечивают управление и обработку данных.

Список литературы

1. Архитектура фон Неймана [Электронный ресурс] // Википедия. – URL: https://ru.wikipedia.org/wiki/Архитектура_фон_Неймана (дата обращения: 20.09.2025).
2. Как работают квантовые компьютеры. [Электронный ресурс] // Habr. – URL: https://habr.com/ru/articles/480480/ (дата обращения: 20.09.2025).
3. Что такое кубит? [Электронный ресурс] // ПостНаука. – URL: https://postnauka.org/questions/157303 (дата обращения: 21.09.2025).
4. Краткая история электроники: от лампочки к квантовому компьютеру [Электронный ресурс] // ПостНаука. – URL: https://postnauka.org/longreads/103187 (дата обращения: 21.09.2025).
5. Основы квантовых вычислений [Электронный ресурс] – URL: https://qtcenter.tsu.ru/data/uploads/posobie.pdf (дата обращения: 21.09.2025).
6. Устойчивая к потерям технология для квантовой метрологии с использованием обратного эффекта Хонга — Оу — Манделя [Электронный ресурс] // Nature Communications. – URL: https://www.nature.com/articles/ncomms11925 (дата обращения: 21.09.2025).
7. Квантовые вычисления: принципы и перспективы [Электронный ресурс] // Автоматика, связь, информатика. – 2025. – № 9. – С. 25–27. – URL: https://asi-journal-rzd.ru/photoelectric-infrared-device-pmt-ir-for-marshaling-humps-1 (дата обращения: 21.09.2025).

8. Семенов А.Г., Заикин А.Д. Сверхпроводящие квантовые флуктуации в одном измерении [Электронный ресурс] // Успехи физических наук (УФН). – 2022. – URL: https://ufn.ru/en/articles/2022/9/a/ (дата обращения: 21.09.2025).
9. Квантовые вычисления: прогнозы и препятствия [Электронный ресурс] // Квантовая электроника. – 2023. – Т.53, № 8. – С. 622-630. – URL: https://journals.rcsi.science/0368-7147 (дата обращения: 21.09.2025).
10. Квантовую запутанность предложили генерировать в сверхпроводнике [Электронный ресурс] // CoLab. – 2023. – URL: https://colab.ws/news/691 (дата обращения: 21.09.2025)