

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ КВАНТОВЫХ КОМПЬЮТЕРОВ

Кабарухин А.П.¹, Камалиденов К.Ш.², Култазин Н.М.³, Ангапов В.Д.⁴

¹Кабарухин Алексей Павлович - старший инженер сопровождения разработки,
Акционерное общество "Нэксайн", г. Москва;

²Камалиденов Куаныш Шарипханович - ведущий системный архитектор,
Digital IQ;

³Култазин Нурлан Муратович - инженер инфраструктуры,
Astana International Exchange,
г. Нур-Султан, Республика Казахстан;

⁴Ангапов Василий Данилович - старший системный архитектор,
Digital IQ, г. Улан-Удэ

Аннотация: в статье рассматриваются перспективы использования квантовых компьютеров в современном мире. Особое внимание уделяется развитию истории применения квантового компьютера, определению его понятия и сущности. Отмечено, что несмотря на потрясающие возможности, которые квантовые компьютеры предоставляют сегодня, квантовые технологии формируют и ряд проблем, которые в основном вызваны принципиально другими законами природы и трудностями перехода к квантовой механике. На фоне этого в работе приведены аргументы перспектив и возникающих рисков использования квантовых компьютеров.

Ключевые слова: квантовый компьютер, вычислительное устройство, перспективы.

УДК 004.386

Современные электронные технологии развиваются стремительно. То, что было фантазией несколько лет назад, становится реальностью на наших глазах. Информация стала неотъемлемой частью нашей жизни. Человеческое общество все активнее ищет способы и механизмы ее обработки и передачи. Сегодня человечество сталкивается с задачами, которые не может решить даже самые мощные суперкомпьютеры, занимающие площадь целого дата-центра. Квантовые компьютеры, которые могут решать задачи любой сложности, приходят на помощь обычным.

Рассматривая определения «квантовый компьютер», отметим, что по мнению Альшина С.К. и Селюкова С.А., это — принципиально новая система. Она отличается от обычных компьютеров в самом фундаменте, в физических основах, на которых работает. Их даже нельзя сравнивать — это все равно что поставить рядом счеты и современный многозадачный компьютер [1]. Как считают Ягодкин Д.А. Герасимова Ю.Я. и Кузнеченкова Е.С. квантовый компьютер – это такое электронно-вычислительное устройство, которое применяет квантовую природу микрообъектов: их умение находиться для передачи и обработки данных в положении «суперпозиции» и хранить не «0» или «1», а сразу некоторое количество состояний одновременно [2]. В то же время Попова И.Г., Грицай И.П. и Скворцова Н.С. утверждают, что квантовый компьютер — вычислительное устройство, которое использует квантовую природу микрообъектов: их способность находиться для передачи и обработки данных в состоянии «суперпозиции» и хранить не «0» или «1», а сразу несколько состояний одновременно [3]. Таким образом дадим краткое определение: Квантовый компьютер — это тип вычислительной машины, которая использует эффекты квантовой механики для выполнения определенных операций более эффективно, чем обычный компьютер.

Идея технологии квантового компьютера зародилась еще в 1980-х годах, благодаря работе ученого Ричарда Фейнмана – лауреата Нобелевской премии. Рассматривая историю возникновения квантового компьютера обозначим значимые этапы развития [4]:

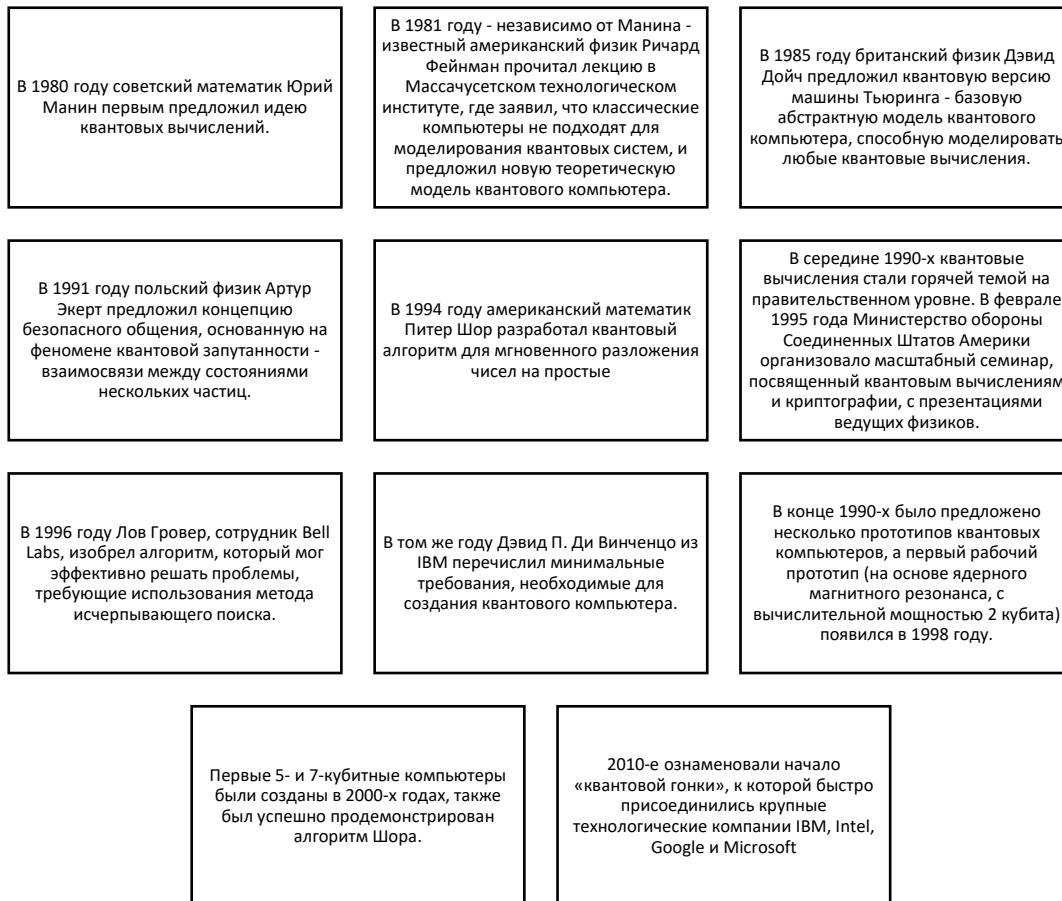


Рис. 1. История возникновения квантового компьютера

Квантовые компьютеры способны открыть для человечества новые горизонты. Развитие квантовой технологии коснется многих сфер жизни. Рассмотрим перспективы использования квантовых компьютеров.

Одно из самых важных применений квантового компьютера — разложение на простые числа. Вся современная криптография основана на том, что никто не сможет быстро разложить число из 30–40 знаков (или больше) на простые множители. На обычном компьютере на это уйдёт миллиарды лет. Квантовый компьютер сможет это сделать примерно за 18 секунд. Идея квантового компьютера заключалась в том, чтобы обратить недостаток в достоинство: использовать для вычислений саму неопределенность, которая так затрудняет обычные расчеты. Представим, что нужно подобрать пароль, у которого неизвестны последние два бита. Тут возможны четыре комбинации: 00, 01, 10 и 11. В классическом случае каждый из них необходимо считать отдельно: подставить его в нужное место и проверить результат. Однако если носителем информации станет квантовый объект – например, два кубита с суперпозицией поляризации, – то все четыре комбинации можно будет проверить одновременно [5]. Это означает, что тайн больше не будет, потому что любые алгоритмы шифрования можно будет сразу взломать и получить доступ к чему угодно. Это касается всего — от банковских переводов до сообщений в мессенджере. Возможно, наступит интересный момент, когда обычное шифрование перестанет работать, а квантовое шифрование ещё не изобретут [6].

Квантовые компьютеры могут быть интегрированы в квантовый Интернет, который будет более безопасным, чем тот, который существует сегодня. «Квантовые компьютеры и квантовая связь позволяют вам делать что-то гораздо более конфиденциальным», - говорит физик Сет Ллойд из Массачусетского технологического института, который предполагает поиск в Интернете, за которым не сможет шпионить даже поисковая машина [7].

В целом потенциал квантовых технологий и квантовых компьютеров в частности пока до конца не раскрыт, но уже сегодня можно однозначно утверждать, что они находят свое применение и в медицине. Квантовая медицина является сейчас одним из самых модных и многообещающих направлений. И здесь в будущем следует ожидать многих прорывных решений. Важные подвижки могут быть достигнуты в поиске новых медицинских препаратов. На рынке уже и без того много хороших лекарств, однако скорость, с которой они производятся, а также их эффективность крайне ограничены. Даже с новейшим приростом скорости и точности, обеспечиваемыми классическими компьютерами, последние весьма незначительны из-

за ограничений, предъявляемых к существующим вычислительным системам. Существует бесчисленное множество способов, с которыми человеческий организм может реагировать на лекарства, плюс безграничность генетического разнообразия на молекулярном уровне и потенциальные исходы для неспецифических лекарственных средств, все это в совокупности достигает миллиардных чисел. Справиться с этим классические компьютеры не в состоянии. И только у квантовых компьютеров будет возможность изучить каждый возможный сценарий взаимодействия организма с препаратом и представить не только наилучший возможный план действий, но и шансы человека на успешный прием препарата – за счет комбинации более точного и ускоренного секвенирования ДНК и более точного понимания фолдинга белка. Квантовые расчеты позволят моделировать сложные молекулярные взаимодействия на атомном уровне, что станет бесценным, если говорить о разработке новых методов медицинской фармацевтики. Доступной станет возможность смоделировать 20 000 белков и их взаимодействие с мириадами новых разных препаратов (даже тех, что еще не изобретены) с безукоризненной точностью. Анализ этих взаимодействий (опять же при помощи квантовых вычислений) приведет к созданию новых методов лечения пока неизлечимых заболеваний.

Нововведения, которые будут открыты с помощью квантовых компьютеров, неизбежно приведут к лучшему пониманию того, как функционирует жизнь в целом, что впоследствии приведет к гораздо более точной ее трактовке, улучшению медицинских препаратов и результатов их действия. Квантовые компьютеры помогут полностью понять мозг и вылечить нейродегенеративные болезни Паркинсона и Альцгеймера, которые сегодня излечить невозможно, поскольку невозможно просчитать всю последовательность активации нейронов – не хватает мощностей обычных компьютеров. Квантовые компьютеры помогут перепрограммировать мозг, чтобы повысить уровень счастья и уменьшить страдания. Одновременно с этим квантовые датчики позволят регистрировать нейронную активность головного мозга, фактически делая возможным даже считывание мыслей [8].

Квантовые вычисления могут упростить управление воздушным и наземным движением, поскольку они так хороши в быстром вычислении оптимального маршрута. Сложный анализ схем воздушного движения с использованием квантового компьютера означал бы более эффективное планирование полетов и сократит время в пути, поскольку мы сможем лучше избегать узких мест при взлетах и посадках в аэропортах [9].

Работа с квантовыми компьютерами требует специальных знаний и методологических навыков. В проекте управления дорожным движением в Лиссабоне уже используются квантовые компьютеры. Не суперкомпьютеры, а именно квантовые системы лучше всего подходят для прогнозирования автомобильного трафика, спроса на транспорт в определенный момент и времени пребывания в пути, утверждают в Volkswagen. Алгоритм Volkswagen сначала анализирует анонимные данные о движении автомобилистов при помощи обычных компьютеров, а затем обращается к квантовым системам для оптимизации трафика, используя предиктивную аналитику. Созданные с использованием квантовых технологий дорожные модели помогают сократить простой общественного транспорта, разгрузить дороги в часы пик и адаптировать работу светофоров под текущую дорожную ситуацию. Кроме того, в будущем на дорогах появится большое количество беспилотных транспортных средств, от которых квантовый компьютер будет собирать данные и одновременно управлять ими. Для реализации такого проекта Volkswagen воспользовалась мощностями квантовых компьютеров компании D-Wave. Использовать систему управления дорожным трафиком сначала решили в Барселоне, где развернута большая база данных, в которую стекается информация о ситуации на дорогах [10]. Интеллектуальное управление движением, использующее производительность квантового компьютера, может обеспечить значительную поддержку для городов и жителей пригородов.

Еще одна область, в которой квантовые компьютеры могут помочь автомобильной промышленности добиться значительных успехов — это аккумуляторные технологии. Понимание того, что именно происходит с батареями на атомном уровне, может открыть путь к более легким и даже более мощным батареям для электромобилей. Эти данные будут непосредственно использованы, например, в недавно начатом производстве аккумуляторных элементов в Центре передового опыта Volkswagen в области исследований аккумуляторов в Зальцгиттере. Тогда каждый водитель электромобиля получит конкретную пользу от этого исследования в своей повседневной жизни [11].

Квантовыми компьютерами уже заинтересовались военные и оборонная промышленность. Компания ColdQuanta недавно подписала соглашение с Министерством обороны США, о создании квантового компьютера, который сможет определять, с какой скоростью компьютер может дать команду радарам обнулить свое местоположение [12].

Компания Lockheed Martin уже несколько лет занимается темой квантовых вычислений. На официальных ресурсах компании упоминается использование компьютеров от D-Wave Systems в качестве средства проверки программного обеспечения. При написании ПО возможны те или иные ошибки, поиск и исправление которых отнимают массу времени и ресурсов разработчика. Быстродействующий квантовый компьютер может провести тестирование программы в минимальное время и выявить все имеющиеся проблемы. В ряде случаев квантовые вычисления способны справиться с задачами, которые практически неразрешимы для систем с другими архитектурами. Проверка кода может использоваться в разных сферах. В качестве примера приводится разработка ПО для авиационной техники. Квантовый компьютер ускорит процесс тестирования и усовершенствования программ, и на испытания выйдут готовый и безопасный

самолет. Быстродействующие компьютеры пригодны и для расчетов в космической отрасли. В течение нескольких миллисекунд квантовый компьютер D-Wave Two способен рассчитать множество траекторий корабля и выбрать оптимальную.

Быстрая обработка крупных массивов данных или выполнение сложных расчетов необходимы в разных областях оборонной промышленности. Внедрение квантовых компьютеров упростит разработку программного обеспечения, ускорит проектирование различных конструкций, а также позволит сократить необходимое число натурных испытаний. Высокая производительность может быть полезна при создании систем с искусственным интеллектом разного назначения – это направление тоже интересует военных и оборонные предприятия [13].

Рэй Джонсон, член совета директоров стартапа компании QxBranсh по квантовым вычислениям, сказал, что даже при наличии самых современных инструментов, которые анализируют температуру и давление, существует слишком много возможных способов проявления данной погодной модели, а текущие прогнозы погоды - это в лучшем случае обоснованное предположение. Квантовые вычисления могут проанализировать все эти данные сразу и дать лучшее представление о том, когда и где ударит плохая погода. Специальные службы заблаговременно уведомляли бы о сильных штормах, таких как ураганы, и дополнительное время на подготовку могло бы помочь спасти жизни.

Интересно применение квантового компьютера и в сельском хозяйстве. Процесс Габера-Боша, который используется для создания богатых азотом удобрений, очень энергоемкий, требует высоких температур и давления. Этот процесс, необходимый для современного сельского хозяйства, потребляет около одного процента мировых запасов энергии. Но есть и лучший способ. Азотфиксирующие бактерии легко извлекают азот из воздуха благодаря ферменту нитрогеназе. Квантовые компьютеры могут помочь смоделировать этот фермент и раскрыть его свойства, что, возможно, позволит ученым «разработать катализатор для улучшения реакции азотфиксации, повышения ее эффективности и экономии энергии в мире», - говорит Своре из Microsoft. «Это то, что мы хотим делать на квантовом компьютере» [14].

Благодаря своей способности анализировать большие объемы данных за короткий период времени квантовые компьютеры также становятся интересными для финансового сектора. Например, игроки финансового рынка с квантовыми компьютерами будут иметь преимущество перед игроками с классическими компьютерами в высокочастотной торговле ценными бумагами. Банки также могут использовать квантовые компьютеры для профилирования своих клиентов с целью выявления мошенничества или оптимизации инвестиционных портфелей [15].

Тем не менее, несмотря на потрясающие возможности, которые квантовые компьютеры предоставляют, квантовые технологии представляют ряд проблем, которые в основном вызваны принципиально другими законами природы и трудностями перехода к квантовой механике.

По сути, квантовые компьютеры делают устаревшими почти все современные подходы к программированию, обработке и защите данных. Человечеству придется не только использовать новую технологию, но и сосредоточиться на создании совершенно новых протоколов передачи данных и инфраструктуры.

Для крупных игроков ИТ-рынка квантовые компьютеры представляют как потрясающий потенциал, так и огромные риски. Поскольку современные корпорации, такие как Google или Facebook, получают большую часть своего дохода от рекламы и продажи пользовательских данных, они будут вынуждены полностью перестроить свои бизнес-модели, потому что их существующие технологии просто перестанут работать.

Квантовые вычисления также вызывают значительный интерес на правительственном уровне. Новая компьютерная революция резко снизит влияние отдельных политиков, поскольку решения большинства правительственных проблем будет легко вычислить. При этом вопросы регулирования квантовых технологий также будут решаться на политическом уровне.

Проблемы, связанные с координацией и законодательством о квантовых компьютерах, могут возникнуть в ближайшем будущем - как только мы увидим первую машину с достаточной вычислительной мощностью, чтобы угрожать конфиденциальности личных, корпоративных или государственных данных или нарушить финансовые системы. Классические системы шифрования общедоступны, они посильны для квантового компьютера — это означает не только возможность украсть деньги, но в будущем и украсть, например, здоровье: взломать управление кардиостимулятором или иными приборами, которых будет только больше. Как у любой медали, у квантового компьютера две стороны: это не только преимущество новых материалов, логистики, оптимизации, но и риск.

Современные квантовые вычислительные системы — это огромные и сложные машины, разработка и обслуживание которых чрезвычайно дороги. Их могут себе позволить только корпорации или университеты. Но то же самое произошло и с обычными компьютерами, которые вместо того, чтобы занимать целые комнаты, поместились на наших столах - и даже в наших карманах. Полноценные квантовые компьютеры, вероятно, появятся в ближайшие несколько десятилетий, но из-за их высокой стоимости пользователи смогут лишь арендовать вычислительные мощности и облачные сервисы, как это сейчас предлагает IBM. Станет ли сегодняшнее общество свидетелем творения крошечных квантовых смартфонов, которые будут иметь большую мощность, чем любой современный компьютер, и смогут передавать любую информацию в любую точку Вселенной? Трудно сказать наверняка. Но практическое применение законов, действующих на

квантовом уровне - совершенно отличных от тех, которые используются в нашем макром мире, управляемом законами механики Ньютона, - уже кажется вполне достижимым.

Список литературы

1. Альшин С.К., Селюкова С.А. Квантовый компьютер в сборнике: Актуальные вопросы науки и хозяйства: Новые вызовы и решения. Сборник материалов LV Студенческой научно-практической конференции, 2021. С. 380-383.
2. Ягодкин Д.А., Герасимова Ю.Я., Кузнеценкова Е.С. Компьютеры Бедующего. Перспективы Развития. В сборнике: Цифровизация образования: теоретические и прикладные исследования современной науки. Материалы XXVII Всероссийской научно-практической конференции. В 2-х частях, 2021. С. 75-79.
3. Попова И.Г., Грицай И.П., Скворцова Н.С. Перспективы создания квантовых компьютеров // Молодой исследователь Дона, 2019. № 6 (21). [Электронный ресурс]. Режим доступа: <https://cyberleninka.ru/article/n/perspektivy-sozdaniya-kvantovyh-kompyutero v/> (дата обращения: 24.12.2021).
4. Evan McBride Quantum computer: a panacea for computing technology? [Электронный ресурс]. Режим доступа: <https://hitecher.com/articles/quantum-computers/> (дата обращения: 24.12.2021).
5. Еришов Александр. Квантовое превосходство // Популярная механика, 2018. № 5. С. 54—59.
6. Валиев К.А., Кокин А.А. Квантовые компьютеры: надежды и реальность. 350 стр. Регулярная и хаотическая динамика (РХД) М.-Ижевск, 2004.
7. Emily Conover Quantum computers are about to get real [Электронный ресурс]. Режим доступа: <https://www.sciencenews.org/article/quantum-computers-are-about-get-real/> (дата обращения: 21.12.2021).
8. Борисевич М.Н. О КВАНТОВОМ КОМПЬЮТЕРЕ И КВАНТОВОЙ МЕДИЦИНЕ // Вестник ВГМУ, 2021. № 2. [Электронный ресурс]. Режим доступа: <https://cyberleninka.ru/article/n/o-kvantovom-kompyutere-i-kvantovoy-meditsine/> (дата обращения: 23.12.2021).
9. Kelly Dickerson 7 awesome ways quantum computers will change the world. [Электронный ресурс]. Режим доступа: <https://www.businessinsider.com/quantum-computers-will-change-the-world-2015-4/> (дата обращения: 23.12.2021).
10. Volkswagen начала использовать квантовый компьютер для управления трафиком на дорогах. [Электронный ресурс]. Режим доступа: <https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82:Volkswagen/> (дата обращения: 26.01.2022).
11. Quantum computers work in a completely different way from conventional computers. [Электронный ресурс]. Режим доступа: <https://www.volkswagenag.com/en/news/stories/2019/11/where-is-the-electron-and-how-many-of-them.html/> (дата обращения: 23.12.2021).
12. Rumeel Hussain Quantum Computing: The World's Coldest Computer That Will Surpass Conventional Computers. [Электронный ресурс]. Режим доступа: <https://www.c-sharpcorner.com/article/quantum-computing-the-worlds-coldest-computer-that-will-surpass-conventional-co/> (дата обращения: 24.12.2021).
13. Квантовые вычисления для оборонной промышленности. [Электронный ресурс]. Режим доступа: <https://topwar.ru/174044-kvantovye-vychislenija-dlja-oboronnoj-promyshlennosti.html/> (дата обращения: 20.12.2021).
14. Инженер Microsoft Криста Свор: Почему мы хотим квантовый компьютер? [Электронный ресурс]. Режим доступа: <https://ftimes.ru/313872-inzhener-microsoft-krista-svor-pochemu-my-xotim-kvantovyy-kompyuter.html/> (дата обращения: 25.12.2021).
15. Julian Eberling Quantum computers: state of development and areas of application. [Электронный ресурс]. Режим доступа: <https://www.lead-innovation.com/english-blog/quantum-computers-state-of-development/> (дата обращения: 25.12.2021).