

# УНИВЕРСАЛЬНЫЙ КВАНТОВЫЙ КОМПЬЮТЕР — ВПЕРЕДИ ВРЕМЕНИ И ТЕХНОЛОГИЙ

Мнений о квантовых компьютерах (КК) в настоящее время очень много, причем часто весьма противоречивых, что связано с тем уровнем потенциальных возможностей, которыми могут обладать эти устройства, а также выходом ряда первых продуктов квантовых технологий на рынок. Данный материал — попытка краткого анализа изменений, происходящих в рассматриваемой области. 24 года назад вышел первый русскоязычный обзор по квантовой информации, опубликованный в журнале «Успехи физических наук» [1]. Это было время ожиданий быстрой реализации квантовых компьютеров и тех возможностей, которые они могут принести в связи со сделанными накануне предсказаниями. Что изменилось за прошедшие годы? Какие рубежи достигнуты?



**Сергей Килин,**  
заведующий  
Центром «Квантовая  
оптика и квантовая  
информатика»  
Института физики  
им. Б. А. Степанова  
НАН Беларуси, академик

Простая оценка показывает: объем памяти классических устройств ограничен. Используя все частицы Вселенной, т.е.  $2^{200}$ , мы можем создать память ограниченного размера, в которую реально записать все 200-разрядные бинарные числа, но не более. Квантовая память такого же объема реализуется на основе всего 200 кубитов (квантовых частиц с двумя состояниями). Другой пример — химическая реакция образования из относительно простых молекул новой. Природа находит глобальный минимум энергии взаимодействующих частиц, при котором они соединяются и образуют устойчивое состояние новой молекулы, за фемтосекунды. Человек, используя современные суперкомпьютеры, не решит эту задачу за разумное время. На основе какого принципа Природа решает данную задачу — открытый вопрос, который активно стал обсуждаться в последнее время в связи с КК. Но то, что он связан с эффективным управлением системой квантовых частиц, — очевидно. В конце прошлого века было показано, что человек, научившись управлять системой кубит, сохраняя их когерентность, получит способ реализовывать экспоненциальное число возможностей  $2^K$ , выполнив  $K$  операций

над кубитами (*квантовый параллелизм*). Именно это обеспечивает основное преимущество квантовых компьютеров над традиционными, работающими с классическими носителями информации – битами. В 1994 г. американский физик Б. Шор доказал, что универсальный квантовый компьютер может факторизовать большое число  $N$  за полиномиальное время  $\log N$ . Это показало, что квантовый компьютер представит реальную угрозу информационной безопасности, построенной на различной сложности прямых и обратных задач (например, нахождения произведения простых чисел и факторизации числа, составленного из произведения простых чисел). Последовавшее через 2 года открытие Л. Гровером квантового алгоритма, ускоряющего поиск в неструктурированной базе данных с  $O(N)$  операций до  $O(\sqrt{N})$ , показало, что квантовый компьютер может быть полезным и для задач такого класса.

### ПРИМЕР УНИВЕРСАЛЬНОГО НАБОРА ГЕЙТОВ

Один из универсальных наборов гейтов Адамара  $\{U\} = \{X, Z, Y, H, CNOT, T\}$  представлен пятью однокубитными операциями, описываемыми тремя операторами Паули  $X, Z, Y$  оператором Адамара  $H$ , диагональным оператором  $T = \text{diag}(1, e^{i\pi/4})$  сдвига фазы на  $\pi/4$ , и одной двухкубитной операцией УСЛОВНОГО НЕТ ( $CNOT$ ).

Абстрактно универсальный квантовый компьютер (УКК) определяется как устройство, которое может выполнять любую унитарную операцию  $U$ , переводя регистр кубитов из одного состояния в другое в гильбертовом пространстве  $U|\psi\rangle = |\psi'\rangle$ , при этом  $U$  эффективно компилируются из конечного набора элементарных гейтов (*универсальный набор гейтов*). Именно для УКК в такой формулировке и проводились математические доказательства эффективности первых квантовых алгоритмов. Проще говоря, унитарные преобразования некоторого количества кубитов и есть квантовый компьютер. Однако любая его реализация будет сопряжена с ошибками, которые нарушают необходимое условие унитарности операций квантовых вычислений.

### КВАНТОВЫЙ ПАРАЛЛЕЛИЗМ

Квантовый параллелизм можно проиллюстрировать на примере операции записи числа в регистр из  $N$  битов в классическом и  $N$  кубитов в квантовом компьютере. Произведя  $N$  операций в классическом регистре, мы запишем только одно число длиной  $N$  бит. В квантовом случае, выполнив над каждым из кубитов, первоначально находящемся в состоянии  $|0\rangle$ , операцию Адамара  $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ , мы в результате  $N$  операций получим все  $2^N$  числа длиной  $N$  в виде суперпозиции:

$$|x\rangle = H^{\otimes N} |0\rangle_1 |0\rangle_2 \dots |0\rangle_N = 2^{-N/2} (|0\rangle + |1\rangle)_1 (|0\rangle + |1\rangle)_2 \dots (|0\rangle + |1\rangle)_N = 2^{-N/2} \sum_n |n\rangle, \text{ где } n \in \{0, 2^N - 1\}.$$

Это центральный момент в возможности создания *полезного квантового компьютера* (табл. 1), и он связан с разработкой эффективных кодов, исправляющих ошибки, и достижением очень низкого порогового значения скорости генерации ошибок. Использование таких кодов с неизбежностью приводит к увеличению количества кубитов для исправления ошибок и сохранения унитарности для кубитов, выполняющих основные преобразования (*логических кубитов*).

Взаимодействие кубитов в УКК, то есть его *архитектура*, – принципиальный вопрос эффективности квантового компьютера. Крупномасштабный УКК должен связать воедино миллионы или даже миллиарды кубитов. Есть два подхода к построению таких устройств. Первый, подразумевающий использование *однородной архитектуры*, где каждый кубит напрямую соединен со своими соседями, технически привлекателен, но плохо масштабируется. В зависимости

ПОЛЕЗНЫЙ КВАНТОВЫЙ КОМПЬЮТЕР	
Универсальный	Не ограничивается одним классом задач
Точный	Вероятность ошибки на выходе может быть сколь угодно малой
Масштабируемый	Требования к ресурсам не растут экспоненциально с уменьшением целевой вероятности ошибки

Таблица 1. Необходимые свойства УКК при наличии ошибок


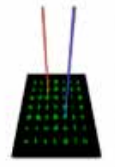
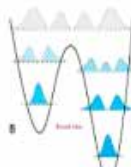


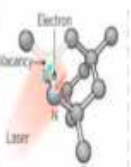
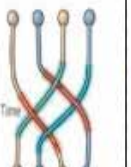
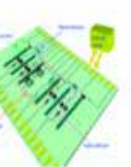














АТОМЫ		ЭЛЕКТРОНЫ СВЕРХПРОВОДНИКОВЫЕ КОНТУРЫ И УПРАВЛЯЕМЫЕ СПИНЫ					ФОТОНЫ
 ионы в ловушках	 холодные атомы	 квантовый отжиг	 сверхпроводники	 кремний	 NV-центры	 топологические	 фотоны
ПРОИЗВОДИТЕЛИ							
							

Таблица 2. Платформы, производители и исследователи (адаптировано из Olivier Ezratty (2021), arXiv:2111.15352 [quant-ph])

от платформы (ионы, сверхпроводящие устройства, фотоны, твердотельные системы и др.) может потребоваться множество управляющих лазеров или микроволн, направленных на одну физическую область, или очень большой криостат, вмещающий все кубиты. Альтернативный подход – модулярная архитектура, где квантовый компьютер формируется из множества небольших модулей (каждый состоит только из (относительно) небольшого числа кубит), которые необходимо связать вместе и выполнять межмодульные шлюзы между удаленными кубитами с помощью (А) их физического перемещения (*shuttling* для ионных платформ) или (В) *телепортации*.

Если на первых этапах количество квантовых алгоритмов практически ограничива-

лось алгоритмами Шора и Гровера и упоминанием идеи Фейнмана о симуляции квантовых процессов на квантовых компьютерах, то сейчас их количество растет [2, 3], включая в себя все новые по областям применения алгоритмы. Математически алгоритмы подразделяются на 4 группы: алгебраические и относящиеся к теории чисел (1); основанные на использовании процедуры так называемого оракула (2); симуляции и аппроксимации (3); оптимизации, численные методы и машинное обучение (4). По ускорению времени выполнения квантового алгоритма по сравнению с классическим выделяются суперполиномиальные (например, алгоритм Шора) и полиномиальные (алгоритм Гро-

вера). Для некоторых алгоритмов, например квантового отжига, ускорение неизвестно.

Наблюдается рост интереса к квантовым компьютерам для прикладных задач симуляции химических [4] и биомедицинских процессов [5], к задачам оптимизации, машинного обучения. Использование небольших квантовых специализированных вычислителей в качестве параллельных или последовательных сопроцессоров совместно с классическими суперкомпьютерами позволит добиться преимуществ в выяснении особенностей химических процессов. Так, имея всего 200 безошибочных идеальных кубитов, квантовый компьютер может разгадать биологическую фиксацию азота. Отметим, что в настоящее время процесс Гебера-Боша (получения аммиака) потребляет 2% мирового годового запаса энергии. С помощью квантового процессора IBM Q Valencia был вычислен дипольный момент молекулы LiH – одного из элементов литий-серных батарей [6].

Создание универсальных квантовых компьютеров – сложная, многоаспектная задача. Первые попытки добиться успехов в данной области показали отсутствие у исследователей необходимого опыта изоляции, управления и измерений одиночных квантовых объектов. Так, работы по флуоресценции одиночных молекул появились только в 1990-х гг., и потребовалось достаточно много времени и усилий для разработки новых методов и технологий для наблюдения и управления в лабораторных условиях не только одиночными молекулами, но и атомами, ионами, примесными центрами в твердых телах, электронами, одиночными электронными и ядерными спинами, а также фотонами с целью их использования в качестве кубитов для УКК на соответствующих платформах. Плодами этих достижений уже пользуются в многочисленных приложениях, в том числе и технологиях, которые относят к квантовым. Это квантовые сенсоры с повышенной чувствительностью, устройства для квантовой криптографии, квантовые генераторы случайных чисел и др.

Над решением задачи создания устройств квантовых вычислений работают не только в лабораториях университетов и научных центров, но и в корпорациях (Google, IBM, Intel, NEC, Honeywell и др.) (см. табл. 2, на которой представлены как производители, так и исследователи, разнесенные по соответствующим платформам используемых физических кубитов).

Однако несмотря на усилия, УКК продолжает оставаться технологическим вызовом. Причина этого – «хрупкость» квантовой информации и факт, что КК – принципиально вероятностные устройства. Растущая с увеличением числа перепутанных кубитов *декогеренция* вынуждает предпринимать специальные меры по изоляции КК и сети кубитов от внешних возмущений, а также разработке специальных квантовых кодов, исправляющих ошибки. Ответы на технологический вызов ищут физики и математики совместно с инженерами. На этом пути в качестве реперных требований для разработчиков выступают *критерии Ди Винченцо* (табл. 3). С другой стороны, физики хотели бы получить от квантовой индустрии ответы на вопросы, которые формулируются как *опросник Скотта Аэронсона* (табл. 4). Ответы на данные вопросы формируют уровень доверия к выпускаемой аппаратуре.

#### КРИТЕРИИ ДИ ВИНЧЕНЦО

- 1 Масштабируемость
- 2 Надежная инициализация кубитов
- 3 Большие времена декогеренции по сравнению с временем срабатывания отдельных гейтов
- 4 Возможность реализации универсального набора гейтов
- 5 Индивидуальное считывание состояний кубитов

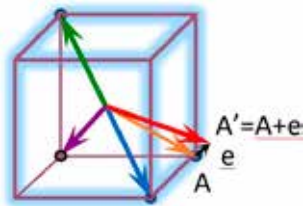
Таблица 3. Чек-лист для разработчиков КК

#### ОПРОСНИК СКОТТА АЭРОНСОНА

- 1 Сколько используется кубитов?
- 2 С какими временами когерентности?
- 3 С какой архитектурой связей?
- 4 Какова точность (фиделити) одно- и двухкубитных гейтов, а также вывода данных (измерений)?
- 5 Какова глубина схемы?
- 6 Какие ресурсы необходимы стандартным классическим алгоритмам для моделирования системы?  
В чем заключается главный недостаток используемой системы, какие ее характеристики хуже всего, и что прежде всего надо улучшить?
- 7
- 8 Что мешает компании иметь масштабируемый квантовый компьютер прямо сейчас?

Таблица 4. Что хотят узнать исследователи у производителей КК

## КЛАССИЧЕСКИЕ КОДЫ, ИСПРАВЛЯЮЩИЕ ОШИБКИ



Измененный за счет ошибки  $e$  кодовый символ  $A$  (коричневый вектор) превращается в символ  $A' = A + e$  (красный вектор), который отличается от других кодовых символов (вектора разных цветов) при условии, что минимально расстояние между ними (кодовое расстояние  $d$ ) больше  $2e$ . Т.е.  $d = 2t + 1$ , где  $t$  – количество исправляемых бит кода.

Возвращаясь к основной проблеме создания УКК (ошибкам при выполнении гейтов), отметим, что основная идея ее решения совпадает с методом борьбы с ошибками в обычных компьютерах (использование классических кодов, исправляющих ошибки). Путем добавления к битам данных избыточных битов растет расстояние между кодовыми символами, тем самым увеличивается их различимость даже при возникновении ошибки в одном или нескольких битах символа.

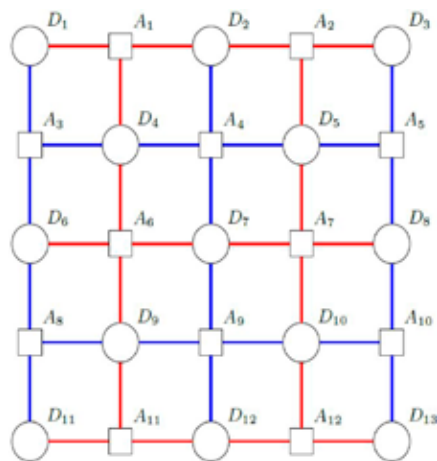
Квантовые коды, исправляющие ошибки, сложнее классических, так как они должны исправлять не только перевороты кубита ( $Z$ ), но и изменение относительной фазы кубита ( $X$ ). Как следствие, увеличивается число избыточных кубитов для обеспечения исправления ошибок логических кубитов. Например, для квантового кода Шора [9, 1, 3] с кодовым расстоянием 3, исправляющего любую ошибку в одном логическом кубите, требуется 9 физических кубитов. Разработаны различные квантовые коды: Шора, Стина, CSS (Калдербанк, Шор и Стин), стабилизационные коды, топологические (Китаев), поверхностные и др.

Однако даже их использование не избавляет от неконтролируемого распространения ошибки при выполнении логических операций (гейтов): возникнув в одном логическом кубите, она переносится при выполнении гейта на другой и так далее лавинообразно.

Существуют некоторые устойчивые к ошибкам гейты (трансверсальные). Например, трансверсальная CNOT-операция над двумя логическими кубитами в 7-кубитном коде Стина. Было показано, что некоторые подмножества универсального набора гейтов  $\{U\}$  являются трансверсальными. Однако в 2009 г. доказана no-go-теорема, согласно которой полный универсальный набор гейтов  $\{U\}$  не является трансверсальным [8]. Поэтому единственное, что «спасает»

идею универсального квантового компьютера, оставляя надежду на его реализацию, – это **квантовая пороговая теорема** (Аронов Д., Бен-Ор М.; Китаев А.; Книлл Е., Лафлам Р., Журеку В.). Согласно ей, квантовый компьютер с коэффициентом физических ошибок  $p$  ниже определенного порога  $p_{th}$  может, применяя схемы квантовой коррекции ошибок, подавить коэффициент логических ошибок до сколь угодно низкого уровня. Для поверхностного кода текущие оценки устанавливают порог порядка 1%, хотя они сильно различаются и трудновычислимы из-за экспоненциальной сложности моделирования больших квантовых систем. При вероятности деполяризационной ошибки 0,1% поверхностный код потребует приблизительно 1000–10 000 физических кубитов на 1 логический кубит данных (~166 млн физиче-

## КВАНТОВЫЕ ПОВЕРХНОСТНЫЕ КОДЫ



Код  $[[13, 1, 3]]$  – наименьший поверхностный код, способный обнаруживать и исправлять ошибки за один прогон. Кружки – кубиты данных, квадраты – вспомогательные кубиты. Красными линиями обозначены гейты КОНТРОЛИРУЕМОЕ  $X$ , синим – КОНТРОЛИРУЕМОЕ  $Z$ . Архитектура – однородная: связь между соседними кубитами.



Рис. 1. Прогнозируемая эволюция создания УКК как функция достигаемой пороговой вероятности ошибки гейта

## НАХОЖДЕНИЕ КВАНТОВОГО ОБЪЕМА

Протокол квантового объема определяет самую большую квадратную квантовую цепь, в которой ширина и глубина равны и которая может быть запущена на КК. Протокол состоит в многократном запуске случайной 2-кубитной схемы глубины два, с проверкой теста – наиболее вероятные строки возникают с вероятностью  $> 2/3$  и с уровнем доверительного интервала более 97,725% и последующем повторе с тремя кубитами на третьей глубине, четырьмя кубитами на четвертой глубине, и т.д. до невыполнения теста.

ских кубитов для факторизации числа в 1000 бит). Исходя из данной теоремы, прогнозируется эволюция создания УКК как функция достигаемой пороговой вероятности ошибки гейта  $p_{th}$  (рис. 1).

Сегодняшняя точность (фиделити) однокубитных гейтов достигает 99,9X%, двухкубитных – 99, X% в зависимости от типа кубитов (платформы). Эти показатели очевидным образом демонстрируют, что пока УКК можно рассматривать в лучшем случае как отдаленную перспективу. Так, запланированный к выпуску в 2023 г. IBM квантовый компьютер «Condor» на сверхпроводниках, содержащий 1121 физический кубит, сможет реализовать *только* 1 логический кубит поверхностного кода с коррекцией ошибок. В ближайшей перспективе, по мере решения проблемы уменьшения вероятности ошибки гейта  $p_{th}$ , на первый план выходят задачи создания КК *небольших масштабов* (NISQ) – квантовых ускорителей вычислений, решающих *специализированные*

задачи и работающих совместно с суперкомпьютерами [9].

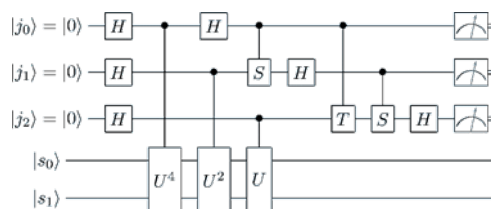
Чтобы показать имеющиеся практические преимущества в вычислениях квантовых машин (даже на уровне NISQ) по сравнению с обычными компьютерами, производителями был введен специальный термин – «квантовое превосходство». Термин, имеющий и рекламный характер, основан на том, что квантовый компьютер можно эмулировать на обычном. Однако количество кубитов для такой эмуляции ограничено памятью компьютера, а не его вычислительной мощностью. Самый большой суперкомпьютер сегодня имеет ~ 10 петабайт памяти, что позволяет имитировать операции с ~ 48 кубитами.

Любой квантовый компьютер с более чем примерно 50 кубит невозможно смоделировать

Любой квантовый компьютер с более чем примерно 50 кубит невозможно смоделировать

## ШИРИНА И ГЛУБИНА КВАНТОВОЙ ЦЕПИ

Ширина квантовой цепи – количество используемых кубитов, глубина – максимальное число операций.



Глубина данной цепи равна 7. Регистр 3 имеет 5 гейтов, но 2-й (КОНТРОЛИРУЕМОЕ-U) не может быть выполнен, пока не будут исполнены КОНТРОЛИРУЕМЫЕ -  $U^4$  и  $U^2$ , что добавляет 2 шага. Гейт КОНТРОЛИРУЕМОЕ-T может быть реализован одновременно с H. Следовательно, глубина цепи равна 7.

## ЗАДАЧИ ДЛЯ NISQ

Квантовая оптимизация

Цифровая/аналоговая квантовая симуляция

Квантовое вычисление/симуляция промежуточного масштаба

Квантовая химия

Квантовое глубокое машинное обучение

Вариационное квантовое вычисление

Квантовые стохастические процессы, игры

Квантовые адиабатические вычисления (отжиг)

Таблица 5. Где будет полезен NISQ?

на обычном компьютере. Причем эти кубиты не обязательно должны быть корректируемыми. Можно использовать физические кубиты, которые достаточно хороши для выполнения тысяч операций раньше, чем возникает ошибка. Данная машина не масштабируется и может выполнять только относительно *короткие алгоритмы*. Тем не менее даже такой не универсальный квантовый компьютер нельзя эмулировать на обычном, поэтому он может показать квантовое превосходство и оказаться полезным для некоторых приложений (табл. 5).

Гонка за большим числом кубитов в квантовом компьютере не должна являться самоцелью. Недавно введенный еще один термин «квантовый объем» (КО) определяет величину пространства состояний, доступное конкретному КК. Увеличение числа кубитов в компьютере с высоким уровнем ошибок не увеличивает его квантовый объем. В то время как десятикратное снижение уровня ошибок при заданном числе кубитов повышает КО в 24 раза.

Задачи для КК типа NISQ, которые будут определять перспективы квантовой индустрии вычислений в обозримом будущем, весьма многообразны, и многие из них, как и сама индустрия, находятся только на пороге своего развития. Для каждой из специализированных задач будет использоваться наиболее подходящий тип платформы (кубитов). Наряду при-

кладными элементами (оптимизация, квантовая химия, квантовая симуляция, глубокое обучение) NISQ будут применять как инструменты характеристики и калибровки создаваемых устройств, что невозможно сделать с помощью классических вычислительных средств. Примером может служить недавняя работа [10], в которой для этих целей использовался 127-кубитный процессор с высоким уровнем ошибок.

Особняком в списке задач для NISQ стоят *адиабатические квантовые вычисления* (квантовый отжиг). В отличие от квантового компьютера на основе цепей (ЦКК), адиабатические квантовые компьютеры (АКК) выполняют очень специфический вид вычислений, но чрезвычайно полезный: оптимизацию. АКК используется для поиска набора переменных, который минимизирует некоторые функции с несколькими переменными, и *считается*, что он может делать это быстрее, чем обычный компьютер, хотя математика, лежащая в основе этого, на данный момент не совсем ясна. Любое стандартное квантовое вычисление в принципе может быть выполнено с помощью АКК и наоборот, но доказательство не показывает простого пути перехода от одной системы к другой.

В зависимости от вида используемых кубитов существует несколько основных *платформ*, реализующих КК типа NISQ: сверхпроводники (IBM, Google, D-Wave); ионы в ловушках (IONQ, Honeywell); нейтральные атомы (Pascal, QuERA); фотоны (PsiQuantum, Xanadu); NV-центры в алмазе (эта платформа [11] была впервые

## АКК: ОТКРЫТЫЕ ВОПРОСЫ

Исправление ошибок. В отличие от ЦКК неизвестно, как исправлять ошибки в АКК.

Проблема энергетической щели. Суть работы АКК: при медленном изменении параметров система остается в основном состоянии, но уже в новой конфигурации. Количественная оценка «насколько медленно» обратно пропорциональна «энергетической щели между основным и первым возбужденным состоянием». Величина энергетической щели не совсем понятна теоретически и зависит от конкретной проблемы.

Щель уменьшается с увеличением размера системы. Вследствие этого время вычислений увеличивается. Таким образом, АКК ограничен размером задач, которые он может решить.

Идеальный АКК должен работать при чрезвычайно низкой температуре, чтобы тепловые флуктуации не могли перекрыть энергетическую щель. АКК, работающий при конечной температуре, коммерчески доступен сегодня (D-Wave).

предложена в работе 2001 г. [12]; продемонстрирована система из 27 ядерных спинов  $^{13}\text{C}$  [13] в окружении NV-центра); электронные и дырочные спины в полупроводниках, а также ядерные спины в молекулах и топологические КК. Один из последних обзоров платформ представлен в [14].

Если оглянуться на пройденный путь – от появления яркой идеи использования квантовых систем для ускорения вычислений до первых реализаций простейших квантовых процессоров, – ясно видно, что ученые в результате многочисленных исследований в течение четверти века (серия 17 международных конференций по квантовой оптике и квантовой информатике ICQOQI, организованных белорусскими физиками, в определенной мере отражает этот путь [15]) научились *манипулировать и измерять* различные квантовые системы на *одиночном уровне*, включая электроны, фотоны, ядерные спины молекул и примесных центров. При этом получены новые знания о функционировании таких систем и попутно предложен ряд методов прецизионных измерений и уникальных сенсоров. Столкнувшись с явлением декогеренции, ученые разработали квантовые коды, исправляющие ошибки. Осознав, что УКК составит угрозу для современной системы защиты информации, исследователи создали противодействие в виде квантовой криптографии (квантового распределения ключа) [16]. Все эти достижения подтверждают широкие возможности квантового мира, который, будучи контринтуитивным, слегка приоткрыл перед нами свои тайны. Его особенности требуют для освоения и соответствующей подготовки тех, кто будет использовать уже полученные результаты, и дальнейшего развития изысканий.

Только сейчас КК начинают входить в наш мир. Общество заинтересовано в новых ярких возможностях. Необычные квантовые технологии вряд ли оставят в стороне инвесторов «всех мастей». Идея невероятного прогресса с помощью КК в бизнесе, совмещенная с «легкой» популяризацией КК (на многих сайтах и в выступлениях описывают данную технологию как достижимую и прорывную для всех сфер), может привести к эффекту доткомов. Как слово *blockchain* в названии компании в 2016–2018 гг. провоцировало панически скупки, так и слово *quantum* будет заставлять трейдеров покупать акции. В итоге – возможный очередной финансовый пузырь.

Создание универсального КК – слишком сложная задача, чтобы увидеть план ее реа-

лизации с точными датами. На первый план выходит получение КК небольших масштабов (NISQ) – ускорителей вычислений, работающих совместно с суперкомпьютерами. Получаемые при этом результаты следует анализировать и рассматривать в контексте их важности для реализации УКК. Стоимость современного КК запредельно велика даже для очень крупных компаний. Естественной бизнес-моделью использования таких компьютеров является облачная модель. Задача создания УКК – исключительно наукоемкая и решается по законам науки. Рыночными инструментами ускорить этот процесс невозможно. Прогресс технологий на этом пути – пожалуй, самый важный результат, полученный за последние 25 лет истории освоения квантового мира. ■

#### СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. С. Я. Килин. Квантовая информация // Успехи физических наук. 1999. Т. 169. №5. С. 507–527. // <https://doi.org/10.1070/PU1999v042n05ABEH000542>.
2. S. Jordan. Quantum Algorithm Zoo // <https://quantumalgorithmzoo.org/>.
3. J. Abhijith [et al]. Quantum Algorithm Implementations for Beginners // ACM Transactions on Quantum Computing. 2022. №3, 4. Article 18. P. 92. // <https://doi.org/10.1145/3517340>.
4. R. Jarrod [et al]. What the foundations of quantum computer science teach us about chemistry. // J. Chem. Phys. 2021. Vol. 155. №15. P. 150901. // <https://doi.org/10.1063/5.0060367>.
5. B. A. Cordier [et al]. Biology and medicine in the landscape of quantum advantages. // J. R. Soc. Interface. 2022. Vol. 19. P. 20220541. // <https://doi.org/10.1098/rsif.2022.0541>.
6. M. Reiher [et al]. Elucidating reaction mechanisms on quantum computers. // PNAS. 2017. Vol. 114. №29. P. 7555. // <https://doi.org/10.1073/pnas.1619152114>.
7. J. E. Rice [et al]. Quantum computation of dominant products in lithium–sulfur batteries. // J. Chem. Phys. 2021. Vol. 154. №13. P. 134115. // <https://doi.org/10.1063/5.0044068>.
8. B. Eastin, E. Knill. Restrictions on Transversal Encoded Quantum Gate Sets. // Phys. Rev. Lett. 2009. Vol. 102. P. 110502. // <https://link.aps.org/doi/10.1103/PhysRevLett.102.110502>.
9. J. Preskill. Quantum computing in the NISQ era and beyond. // Quantum. 2018. Vol. 2. P. 79. // <https://doi.org/10.22331/q-2018-08-06-79>.
10. Y. Kim [et al]. Evidence for the utility of quantum computing before fault tolerance. // Nature. 2023. Vol. 618. P. 500. // <https://doi.org/10.1038/s41586-023-06096-3>.
11. S. Pezzagna, J. Meijer. Quantum computer based on color centers in diamond // Applied Physics Reviews. 2021. Vol. 8. №1. P. 011308. // <https://doi.org/10.1063/5.0007444>.
12. J. Wrachtrup, S. Y. Kilin, A. P. Nizovtsev. Quantum computation using the  $^{13}\text{C}$  nuclear spins nearby the single NV defect center in diamond. // Оптика и Спектроскопия. 2001. Т. 91. №3. С. 460–467 // <https://doi.org/10.1134/1.1405224>.
13. M. H. Abobeih [et al]. Atomic scale imaging of a 27 nuclear spin cluster using a single spin quantum sensor // Nature. 2019. Vol. 576. P. 411. // <https://doi.org/10.1038/s41586-019-1834-7>.
14. B. Cheng [et al]. Noisy intermediate-scale quantum computers. // Front. Phys. 2023. Vol. 18. P. 21308. // <https://doi.org/10.1007/s11467-022-1249-z>.
15. History of ICQOQI. // <https://master.basnet.by/icqoi2019/>.
16. Килин С. Я. Квантовая криптография: идеи и практика / С. Я. Килин [и др.]; под ред. С. Я. Килина, Д. Б. Хорошко, А. П. Низовцева. – Минск, 2007.