КОМПЬЮТЕРНЫЕ ИССЛЕДОВАНИЯ
И МОДЕЛИРОВАНИЕ 2018 Т. 10 № 2 С. 165–179
DOI: 10.20537/2076-7633-2018-10-2-165-179

Ки&М

МАТЕМАТИЧЕСКИЕ ОСНОВЫ И ЧИСЛЕННЫЕ МЕТОДЫ МОДЕЛИРОВАНИЯ

УДК: 530.145

Обзор текущего состояния квантовых технологий

Р. В. Душкин

ООО «ВойсЛинк»,
Россия, 127322, г. Москва, ул. Милашенкова, д. 4а, стр. 1

E-mail: roman.dushkin@gmail.com

Получено 19.02.2018, после доработки — 04.04.2018.
Принято к публикации 11.04.2018.

Сегодня квантовые технологии могут получить новый виток развития, что, наверняка, даст возможность получить решения для многочисленных задач, которые ранее не поддавались решению в рамках традиционных парадигм и вычислительных моделей. Все человечество стоит у порога так называемой второй квантовой революции, и ее краткосрочные и отдаленные последствия затронут практически все сферы жизни глобального общества. Свое непосредственное развитие получат такие направления и отрасли науки и техники, как материаловедение, нанотехнология, фармакология и биохимия вообще, моделирование хаотичных динамических процессов (ядерные взрывы, турбулентные потоки, погода и долгосрочные климатические явления) и т. д., а также решение любых задач, которые сводятся к перемножению матриц больших размеров (в частности, моделирование квантовых систем). Однако вместе с необычайными возможностями квантовые технологии несут с собой и определенные риски и угрозы, в частности слом всех информационных систем, основанных на современных достижениях криптографии, что повлечет за собой практически полное разрушение секретности, глобальный финансовый кризис из-за разрушения банковской сферы и компрометации всех каналов связи. Даже несмотря на то, что уже сегодня разрабатываются методы так называемой постквантовой криптографии, некоторые риски еще необходимо осознать, так как не все долгосрочные последствия могут быть просчитаны. Вместе с тем ко всему перечисленному надо быть готовым, в том числе при помощи подготовки специалистов, работающих в области квантовых технологий и понимающих все их аспекты, новые возможности, риски и угрозы. В связи с этим в настоящей статье приводится краткое описание текущего состояния квантовых технологий, а именно квантовой сенсорики, передачи информации при помощи квантовых протоколов, универсального квантового компьютера (аппаратное обеспечение) и квантовых вычислений, основанных на квантовых алгоритмов (программное обеспечение). Для всего перечисленного приводятся прогнозы развития в части воздействия на различные сферы человеческой цивилизации.

Ключевые слова: квантовые технологии, квантовые сенсоры, квантовая передача информации, универсальный квантовый компьютер, квантовые вычисления, квантовые алгоритмы

COMPUTER RESEARCH AND MODELING
2018 VOL. 10 NO. 2 P. 165–179
DOI: 10.20537/2076-7633-2018-10-2-165-179

Ки&М

MATHEMATICAL MODELING AND NUMERICAL SIMULATION

UDC: 530.145

Review of Modern State of Quantum Technologies

R. V. Dushkin

VoiceLink ltd.,
4a/1 Milashenkova st., Moscow, 127322, Russia

E-mail: roman.dushkin@gmail.com

Received 19.02.2018, after completion — 04.04.2018.
Accepted for publication 11.04.2018.

At present modern quantum technologies can get a new twist of development, which will certainly give an opportunity to obtain solutions for numerous problems that previously could not be solved in the framework of "traditional" paradigms and computational models. All mankind stands at the threshold of the so-called "second quantum revolution", and its short-term and long-term consequences will affect virtually all spheres of life of a global society. Such directions and branches of science and technology as materials science, nanotechnology, pharmacology and biochemistry in general, modeling of chaotic dynamic processes (nuclear explosions, turbulent flows, weather and long-term climatic phenomena), etc. will be directly developed, as well as the solution of any problems, which reduce to the multiplication of matrices of large dimensions (in particular, the modeling of quantum systems). However, along with extraordinary opportunities, quantum technologies carry with them certain risks and threats, in particular, the scrapping of all information systems based on modern achievements in cryptography, which will entail almost complete destruction of secrecy, the global financial crisis due to the destruction of the banking sector and compromise of all communication channels. Even in spite of the fact that methods of so-called "post-quantum" cryptography are already being developed today, some risks still need to be realized, since not all long-term consequences can be calculated. At the same time, one should be prepared to all of the above, including by training specialists working in the field of quantum technologies and understanding all their aspects, new opportunities, risks and threats. In this connection, this article briefly describes the current state of quantum technologies, namely, quantum sensorics, information transfer using quantum protocols, a universal quantum computer (hardware), and quantum computations based on quantum algorithms (software). For all of the above, forecasts are given for the development of the impact on various areas of human civilization.

Keywords: quantum technologies, quantum sensors, quantum information transfer, universal quantum computer, quantum computing, quantum algorithms

Citation: *Computer Research and Modeling*, 2018, vol. 10, no. 2, pp. 165–179 (Russian).

Исследования и разработка квантовых технологий обещают ускорение научно-технического прогресса и, вероятно, появление «настоящего» искусственного интеллекта [Gonçalves, 2014]. Первая квантовая революция привела к появлению лазера и основанных на нем технологий (наиболее широко используемая — компакт-диски), магнитно-резонансной томографии, большого адронного коллайдера, в конце концов [Фёдоров, 2017]. Сегодня человечество стоит на пороге второй квантовой революции, и квантовые технологии, являясь междисциплинарной областью исследований, расширяются и начинают охватывать все большее и большее количество аспектов науки и техники.

Это значит, что современные ученые, исследователи и инженеры должны как минимум ориентироваться в квантовых технологиях, даже если основной областью их исследований является что-то совершенно далекое от квантовой механики. Настоящая статья предлагает краткий обзор квантовых технологий с указанием того, что ждать в будущем. В соответствии с пониманием автора квантовые технологии сегодня можно разделить на следующие направления[1]:

- квантовая передача информации,
- квантовая сенсорика,
- квантовый компьютер (аппаратное обеспечение),
- квантовые вычисления (программное обеспечение).

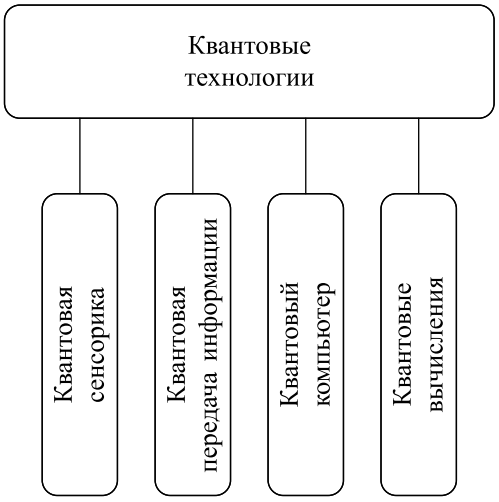

Рис. 1. Классификатор квантовых технологий

Наиболее развитым сегодня является направление квантовой передачи информации, так как уже сегодня существуют так называемые квантовые каналы связи, при помощи которых можно реализовать тот или иной квантовый протокол распределения ключей (первый вариант такого протокола был предложен в 1984 г. Чарльзом Беннетом и Жилем Брассаром — BB84 [Bennet, 1984]), при использовании которого сама квантовая природа реальности защищает передачу от большого количества традиционных атак.

Вместе с тем большая часть квантовых протоколов распределения ключей на практике сталкивается с недостаточностью свойств квантовых каналов. Большинство протоколов требуют однофотонных источников и каналов без затухания, в то время как практические реализации используют лазерные импульсы с когерентными состояниями, число фотонов в которых неопределено, и это позволяет осуществлять некоторые специализированные атаки (например, атака разделения числа фотонов [Янковская, 2013]).

[1] Впрочем, эта классификация не является ни исчерпывающей, ни полной, так что для разных задач представленный классификатор квантовых технологий можно как дополнять, так и дробить на более мелкие направления.

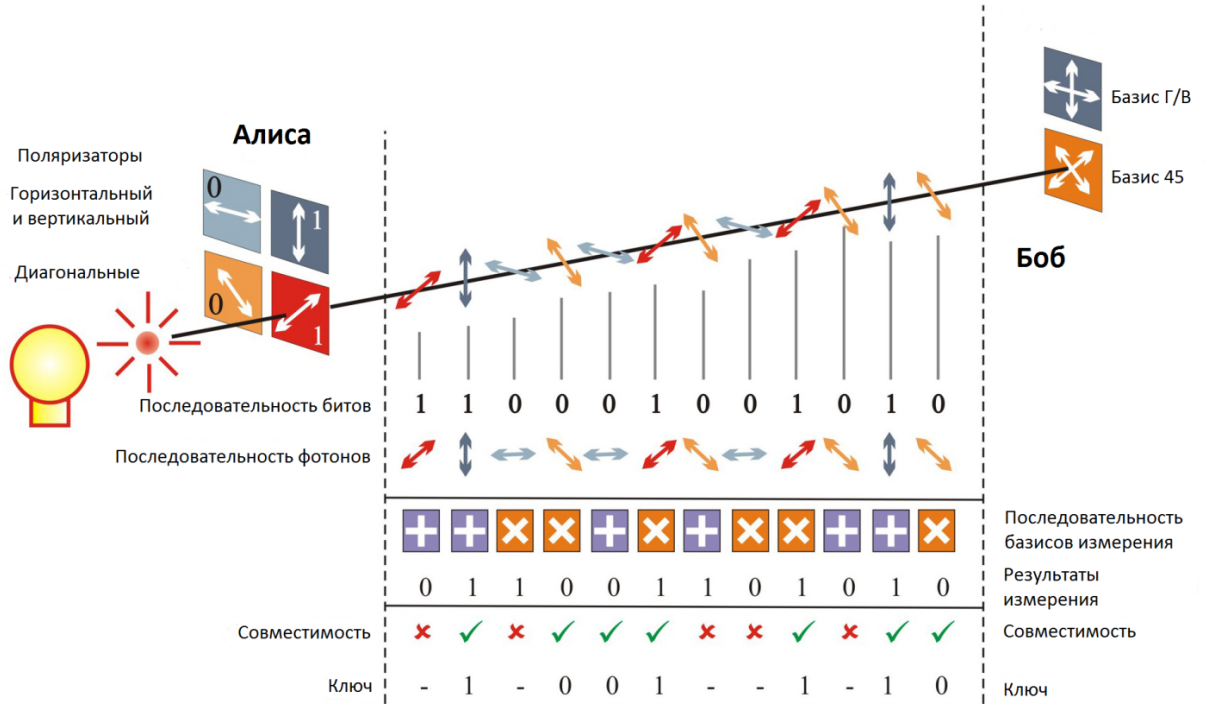

Рис. 2. Схема квантового протокола передачи информации BB84
Алиса и Боб взаимодействуют при помощи квантового канала связи. Алиса посылает Бобу случайную последовательность битов, причем бит 0 может быть закодирован фотоном горизонтальной поляризации или диагональной слева-направо. Соответственно, бит 1 может быть закодирован фотоном вертикальной поляризации или диагональной справа-налево. Боб измеряет получаемые фотоны, случайным образом выбирая базис для измерения — горизонтально-вертикальный или диагональный. В результате измерения Боб получает последовательность битов. После этого они с Алисой взаимодействуют по открытому каналу, и Алиса передает Бобу информацию о том, в каких измерениях Боб выбрал правильную поляризацию. Результаты измерений с неправильной поляризацией отбрасываются. В результате этого процесса у Алисы и Боба появится одинаковая последовательность случайных битов. Внедрение человека посередине нарушит протокол, поскольку измерения фотонов, производимые между Алисой и Бобом, «схлопывают» их волновые функции и нарушают совместимость базисов измерений, в результате чего Боб и Алиса могут понять, что канал скомпрометирован, сравнив некоторое количество оставшихся битов, и если хотя бы один из них не совпадет, то канал скомпрометирован.

Несмотря на это, к настоящему времени созданы практические реализации квантовых систем распределения ключей и систем криптографической защиты информации на их основе. Существуют многочисленные коммерческие решения (например, такие компании, как MagiQ Technologies, США; ID Quantique, Швейцария; Quintessense Labs, Австралия). В Китае запущена сеть для высших государственных деятелей, информация в которой шифруется при помощи квантовых методов [Грищенко, 2017]. При этом повсеместное внедрение таких сетей пока натыкается на ограничение, накладываемое теоремой о запрете клонирования [Wootters, 1982]: ретранслировать квантовое состояние на большие расстояния пока очень сложно. Но работы в этом направлении ведутся [Ulanov, 2015]. Реализация квантовых повторителей и маршрутизаторов позволит объединить квантовые измерительные и вычислительные системы в сеть для выполнения единых функций и получения аддитивного эффекта.

Таким образом, на текущий момент существуют следующие квантовые протоколы распределения ключей:

- *Протокол BB84*, разработан в 1984 г., основан на коллапсе волновой функции [Bennet, 1984]. При практической реализации возможны атака на приемник или передатчик, а также атака разделения числа фотонов.

- *Протокол E91*, разработан в 1991 г., основан на использовании ЭПР-пар и модифицированной теореме Белла [Ekert, 1991]. Возможно повышение эффективности использования кубитов вплоть до теоретически достижимых 100 % [Hwang, 2007].
- *Протокол B92*, разработан в 1992 г., основан на принципе неопределенности Гейзенберга [Bennet, 1992]. Имеет те же недостатки, что и протокол BB84, но злоумышленник вносит в передачу в два раза меньше ошибок за счет снижения расстояния передачи.
- *Протокол 4+2*, разработан в 1995 г. как комбинация протоколов BB84 и B92 [Huttner, 1995]. Это была первая попытка противостоять атаке разделения числа фотонов (неудачная), однако появилось важное свойство: возможная максимальная длина оптоволоконного канала связи при использовании этого протокола составляет 150 км.
- *Протокол SARG04*, разработан в 2004 г. как расширение протокола BB84 с успешным противостоянием атаке разделения числа фотонов [Acin, 2004]. Фактически это первый квантовый протокол, который открыл возможности по использованию заявленных методов распределения ключей на практике.
- *Протокол Lo05*, разработан в 2005 г. и использует так называемые состояния-ловушки для мониторинга чистоты канала [Lo, 2005]. При практической реализации протокола всегда учитываются параметры каналообразующего оборудования, что дает максимальный выигрыш по сравнению с другими протоколами. На текущий момент это самый быстрый и самый далеко действующий протокол.

Под квантовой сенсорикой понимается создание сенсоров, датчиков, измерительных приборов, основанных на квантовых эффектах. Дело в том, что квантовые системы очень легко взаимодействуют со средой, и при помощи них можно измерять различные свойства тех объектов, с которыми квантовая система взаимодействует [Фёдоров, 2017]. Квантовые сенсоры, как ожидается, будут иметь высокое пространственное и временное разрешение, что позволит максимально повысить точность и частоту измерений. Это, в свою очередь, приведет к появлению широкого ряда неинвазивных методов измерения произвольных свойств заданных объектов. Поскольку квантовые системы имеют очень маленькие размеры, они могут быть встроены в состав наномашин, выполняющих различные функции внутри объектов исследования и управления. Тем самым может быть построен обычный кибернетический контур управления, при помощи которого управление может быть осуществлено в режиме реального времени.

Сегодня квантовые датчики представлены довольно громоздкими устройствами, самыми известными из которых являются квантовые или атомные часы, квантовые стандарты времени и частоты, квантовые магнитометры и сенсоры других полей, а также любые измерительные приборы, основанные на лазерах. Уже сегодня такие приборы показывают необычайную точность измерений, и при этом ведутся работы по их миниатюризации.

Квантовая сенсорика также развивается семимильными шагами, находясь на стыке таких дисциплин, как квантовая механика, нанотехнологии и материаловедение. Достижения в этой области позволят существенно повысить точность и разрешение измерений, а также сделать многие измерения неинвазивными. В этом направлении уже сегодня есть много практических достижений [Proctor, 2017].

В то же время квантовые вычисления и, как база для них, квантовый компьютер до сих пор находятся в области разработки прототипа [Trabesinger, 2017]. Если квантовые вычисления сами по себе довольно глубоко проработаны теоретически, реализовать эту математическую вычислительную модель на обычной архитектуре современных компьютеров невозможно даже в режиме эмуляции, так как потребности в вычислительных мощностях возрастают экспоненциально с ростом числа кубитов. А вот полноценный, универсальный квантовый компьютер «в железе» до сих пор не разработан, на текущий момент имеется информация только о прототипах с числом кубитов порядка 50 [Dario, 2017]. Этого числа кубитов пока еще слишком мало, чтобы реализовать более или менее серьезный квантовый алгоритм.

Идеи и мысли о квантовом компьютере и модели квантовых вычислений впервые высказал в 1980 году Ю. И. Манин [Манин, 1980], а затем, в 1981 году, Ричард Фейнман предложил

так называемую задачу Фейнмана [Feynman, 1982], которая заключается в моделировании квантовых систем. Он обратил внимание на то, что моделирование простейших квантовых систем на классической архитектуре требует огромных вычислительных ресурсов, что делает задачу практически неразрешимой. С того времени и было запущено это направление исследований, а в 1985 году Дэвид Дойч представил первый в истории квантовый алгоритм (алгоритм Дойча) [Deutsch, 1985], показавший так называемое квантовое превосходство над классической вычислительной моделью. С тех пор появилось порядка 60 различных квантовых алгоритмов, которые показывают превосходство над классическими алгоритмами в разных случаях, от линейного до экспоненциального [Jordan, 2018].

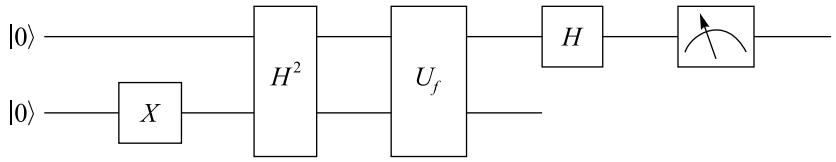

Рис. 3. Схема квантового алгоритма Дойча

Алгоритм Дойча предназначен для решения задачи классификации двоичной функции на константные (всегда возвращающие одинаковое значение независимо от входа) и сбалансированные (возвращающие одинаковое количество 0 и 1 на всем множестве своего определения). На вход алгоритму передается два кубита в базовом состоянии $|0\rangle$, после чего второй кубит обращается в состояние $|1\rangle$ при помощи квантового гейта X (гейт отрицания). Далее оба кубита при помощи гейта Адамара H^2 переводятся в запутанное состояние, после чего к ним применяется квантовый оракул U_f, полученный из исследуемой функции f. После выхода из квантового оракула к первому кубиту вновь применяется гейт Адамара, а затем он измеряется. Значение первого кубита, полученного по результатам измерения, точно отвечает на вопрос о свойстве функции f: если кубит находится в состоянии $|0\rangle$, функция является константной; если кубит находится в состоянии $|1\rangle$, функция является сбалансированной. С тем, как работает этот алгоритм и его расширение на произвольную функцию (алгоритм Дойча–Йожи), можно в деталях ознакомиться в [Душкин, 2015].

Несмотря на то что до сих пор не существует действующей модели универсального квантового компьютера на произвольно большое число кубитов, магистральным является мнение о том, что какие-либо фундаментальные препятствия для его создания отсутствуют. Поэтому в конечном итоге он будет создан, и это вопрос технологий и времени. Противоположная точка зрения заключается в том, что при росте размера квантовой системы с запутанными кубитами время ее декогеренции[2] при любой технологии построения квантового компьютера в какой-то момент будет меньше планковского времени, и это именно тот порог числа кубитов, выше которого невозможно подняться по объективным причинам [Валиев, 1999]. Тем не менее на сегодняшний день нет ни подтверждений, ни опровержений этой гипотезы, а исследования в области создания квантового компьютера ведутся во все ускоряющемся и даже в конкурентном режиме.

В соответствии с [Zurek, 1984; Zurek, 2002] время декогеренции τ_D квантовой системы рассчитывается по следующей формуле:

$$\tau_D \cong \gamma^{-1}\left(\frac{\lambda_{dB}}{\Delta x}\right)^2 = \tau_R\left(\frac{\hbar}{\Delta x\sqrt{2mk_BT}}\right)^2,$$

где

- $\lambda_{dB} = \hbar/\left(2mk_BT\right)^{1/2}$ — термальная длина волны де Бройля [de Broglie, 1924],
- $\tau_R = \gamma^{-1}$ — время релаксации,

[2] *Декогеренция* — процесс нарушения квантовой запутанности квантовой системы, вызываемые ее взаимодействием с окружающей средой посредством необратимого с точки зрения термодинамики процесса.

- Δx — мера размера квантовой системы,
- $\hbar$ — приведенная постоянная Планка,
- m — масса квантовой системы,
- k_B — постоянная Больцмана,
- T — температура квантовой системы.

Из представленной формулы понятно, что время декогеренции тем больше, чем меньше размер квантовой системы (то есть фактически количество запутанных кубитов), меньше ее масса и меньше температура. Именно поэтому современные достижения в ряде технологий построения запутанных квантовых систем, которые могли бы выступить в качестве основы для универсального квантового компьютера, содержат небольшое число кубитов, которые работают при температурах, близких к абсолютному нулю.

Таким образом, сегодня уже можно зафиксировать определенные достижения, которые получены в области квантового компьютера и квантовых вычислений. Можно отметить следующие:

- детально проработана математическая модель квантовых вычислений, доказано квантовое превосходство [Нильсен, 2006];
- полностью проработана методика квантовой коррекции ошибок при передаче информации и осуществлении квантовых вычислений [Gregg, 2006];
- разработано большое количество разнообразных квантовых алгоритмов [Jordan, 2018], создан метод преобразования произвольной вычислимой функции в квантовый оракул [Душкин, 2015];
- разработано несколько языков квантового программирования: Qasm [Glendinning, 2017], QCL [Glendinning, 2017], Q# [Dubois, 2017], Quipper [Selinger, 2016] и некоторые другие;
- существует несколько облачных решений с доступом к универсальным квантовым компьютерам с ограниченным количеством кубитов для всех желающих; сегодня доступно несколько облачных предложений:
  - решение компании Rigetti (19 кубитов): https://goo.gl/7y5g1E,
  - решение компании IBM (20 кубитов): https://goo.gl/p7WK8H,
  - решение компании NTT (20 кубитов): https://goo.gl/Uuvb5T,
  - решение компании Microsoft (40 кубитов): https://goo.gl/o5kqkf;
- создано и успешно работает на коммерческой основе неуниверсальное вычислительное устройство на квантовых принципах (адиабатический квантовый компьютер D-Wave), решающих задачу оптимизации методом квантового отжига[3] [Das, 2008];
- прототип универсального квантового компьютера на текущий момент содержит 50 кубитов [Dario, 2017].

На текущий момент рассматривается несколько возможных технологий построения кубитов и их запутанности для использования в универсальном квантовом компьютере. В таблице 1 даются обзор и сравнение наиболее перспективных технологий [Popkin, 2016].

Ведущие физические лаборатории, государственные квантовые центры и коммерческие компании-гиганты начали новую гонку вооружений в области квантовых технологий. И вполне понятно, почему она началась — ведь тот, кто первым получит квантовое превосходство над вычислительными системами, получит превосходство и в политической сфере. Фактически создание универсального квантового компьютера даст первому создателю неоспоримое преимущество перед остальными игроками.

[3] *Квантовый отжиг* (или квантовая нормализация) — общий метод нахождения глобального минимума заданной функции среди некоторого набора решений-кандидатов. Преимущественно используется для решения задач, где поиск происходит по дискретному множеству с непустым набором локальных минимумов.

Таблица 1. Сравнение технологий построения кубитов

	Вакуумные ловушки	**Квантовые точки**	**Сверхпроводящие элементы**	**Фотоны и топологические кубиты**	**Вакантные места в алмазной решетке**
Время до декогеренции (в секундах)	Более 1000	0.03	0.00005	—	10
Точность работы	99.9 %	~ 99 %	99.4 %	—	99.2 %
Количество запутанных кубитов	14	2	9	—	6
Плюсы	• Очень стабильная работа • Наивысшие достигнутые результаты	• Стабильная работа • Построена на существующей технологии	• Работает быстро • Построена на существующей технологии	• Работает практически без ошибок	• Может работать при комнатной температуре
Минусы	• Работает медленно • Требуется большое количество лазеров	• Очень мало кубитов • Требует сильного охлаждения	• Легко коллапсирует • Требует сильного охлаждения	• Пока существует только в виде теоретической модели	• Сложно образовывать запутанные кубиты
Компании, работающие над образцом	• ION Q	• Intel	• Google • IBM • QCI	• Microsoft • BELL Labs	• Quantum Diamond Technologies

Однако у существующих прототипов универсального квантового компьютера имеется еще одна проблема. Как бы разработчики ни защищали кубиты от воздействий окружающей среды, декогеренция наступает сравнительно быстро при использовании любой технологии. Это значит, что для обеспечения надежности для моделирования одного логического кубита требуется использовать несколько физических кубитов, причем методы обеспечения запутанности логических кубитов становятся еще более сложными с учетом того, что физические кубиты могут быть подвергнуты декогеренции при случайном взаимодействии со средой или в принципе могут декогерировать из-за вероятностной природы квантовых систем. Сегодня квантовая коррекция ошибок на теоретическом уровне проработана довольно подробно, но на практике, как это обычно происходит, имеются определенные технологические проблемы [Нильсен, 2006].

Какая бы технология ни использовалась для получения универсального квантового компьютера, сам по себе компьютер будет представлять собой лишь аппаратное обеспечение, на котором будут исполняться квантовые алгоритмы. И именно квантовые алгоритмы несут то самое квантовое превосходство, ради которого начинается новая гонка вооружений. Поэтому и рассмотрение изменений в постквантовую эру имеет смысл производить с точки зрения программного обеспечения [Душкин, 2015].

Можно сказать, что главной целью квантовых вычислений является решение задачи Фейнмана. Доказано, что любую квантовую систему можно смоделировать с необходимой точностью на универсальном квантовом компьютере. Это позволит не только продвинуться в понимании глубинных основ мироздания, но и решить большое количество прикладных задач в таких областях, как материаловедение и фармакология. Моделирование молекул и их поведения в различных условиях позволит целенаправленно искать вещества с заданными свойствами, строить молекулярные комплексы для выполнения заданных функций и позволит продвинуться в области нанотехнологий.

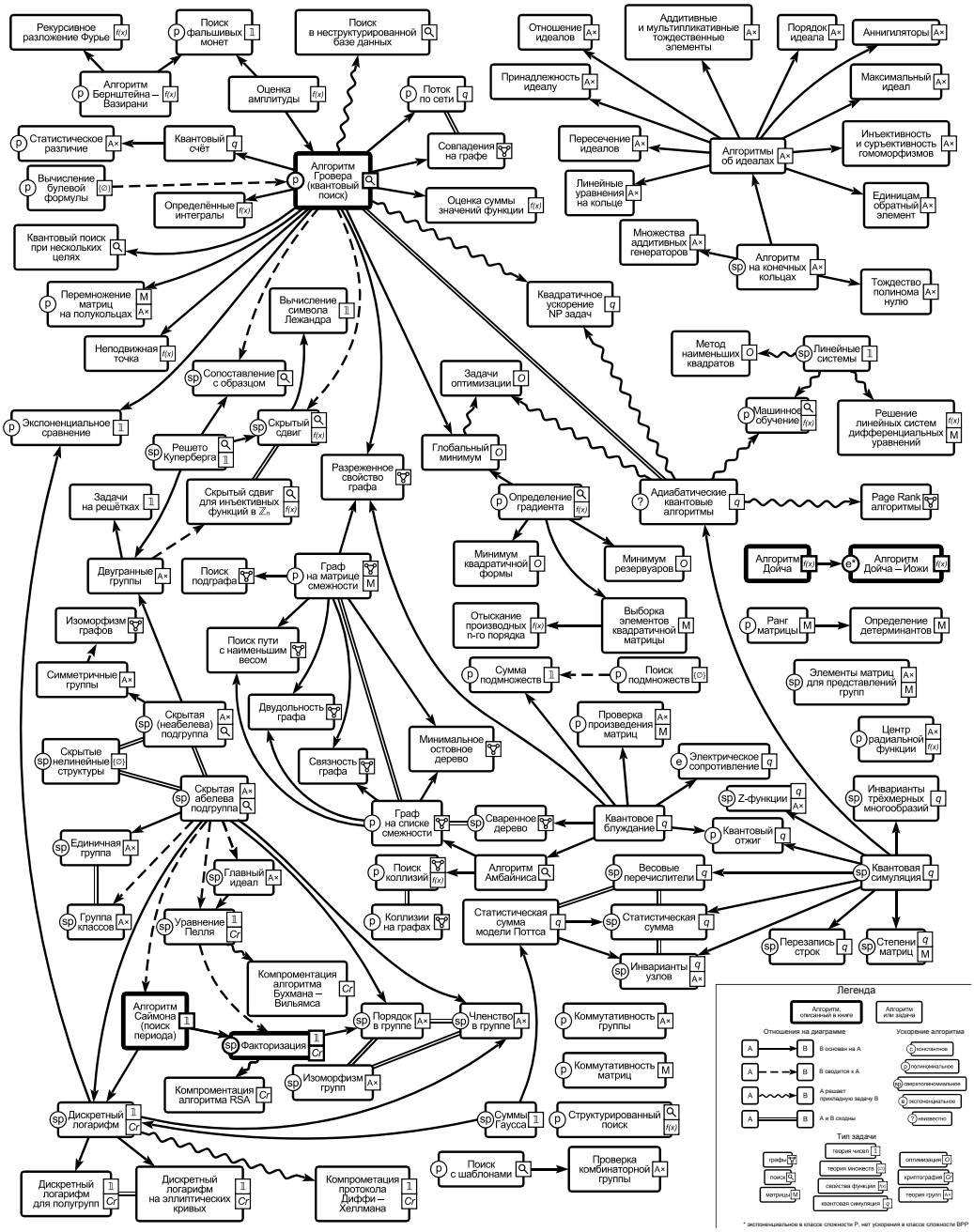

Рис. 4. «Зоопарк» квантовых алгоритмов (по [Душкин, 2015])

Каждый прямоугольник представляет собой один квантовый алгоритм. Слева у каждого алгоритма приведен символ, указывающий на ускорение алгоритма по сравнению с традиционным: C — константное ускорение, P — полиномиальное ускорение, SP — сверхполиномиальное ускорение, E — экспоненциальное ускорение, ? — степень ускорения неизвестна. Справа у каждого алгоритма приведены символы, указывающие на классы задач, которые решаются соответствующим алгоритмом. К таким классам относятся задачи на графах, поисковые задачи, задачи с матрицами, задачи теории чисел, задачи теории множеств, изучение свойств функций, задача квантовой симуляции, задачи оптимизации, криптографические задачи, задачи теории групп. Между квантовыми алгоритмами могут быть отношения, которые на диаграмме отображены стрелками разных видов. Обычная прямая стрелка от алгоритма A к алгоритму B обозначает, что алгоритм B основан на A. Пунктирная стрелка от A к B обозначает, что B сводится к A. Волнистая стрелка от A к B обозначает, что алгоритм A решает прикладную задачу B. Двойная линия между алгоритмами обозначает, что эти алгоритмы сходны друг с другом.

Квантовый алгоритм в общем виде представляет собой последовательное выполнение следующих шагов:

1) подготовка начального состояния кубитов,
2) последовательное применение к кубитам квантовых гейтов (с коррекцией ошибок на аппаратном уровне),
3) измерение выбранных кубитов.

Схема одинакова для любых квантовых алгоритмов, и сами по себе алгоритмы отличаются друг от друга количеством кубитов, их начальным состоянием, набором квантовых гейтов и набором кубитов, которые измеряются в конце алгоритма.

Обычно в качестве начального состояния всех кубитов используется равновероятностная суперпозиция, которая соответствует одновременному отправлению в функцию, которая закодирована при помощи последовательности квантовых гейтов, всех возможных значений входных параметров на выбранном подмножестве области определения. В этом заключается массовый «квантовый параллелизм» вычислений, на котором основано квантовое превосходство. Однако было бы неправильно полагать, что в результате измерения кубитов можно будет получить больше информации, чем это было бы возможно в классической вычислительной парадигме. Несмотря на то что после прохождения квантовых гейтов кубиты находятся в суперпозиции всех значений функции на выбранной области определения, при измерении волновая функция схлопывается, суперпозиция разрушается, а на выходе имеется только одно значение функции, вероятность получения которого равна квадрату модуля волновой функции для полученного значения. Мощь квантовых вычислений в ином: по результатам таких измерений можно сделать выводы о тех или иных свойствах функции, что действительно дает больше информации, но опосредованно. Именно на этом эффекте основано большинство квантовых алгоритмов.

В 1994 году Питер Шор разработал квантовые алгоритмы [Shor, 1997], названные его именем. Эта пара алгоритмов позволяет решить две задачи за логарифмическое время, что дает экспоненциальное преимущество перед традиционной архитектурой. Эти задачи — разложение на простые множители и дискретное логарифмирование — лежат в основе всех современных методов асимметричной криптографии с открытым ключом, поскольку считается, что они неразрешимы с практической точки зрения. Создание универсального квантового компьютера

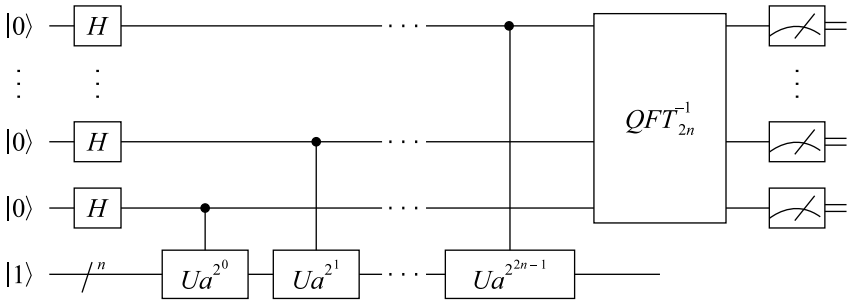

Рис. 5. Схема квантового алгоритма Шора

Квантовый алгоритм Шора является вспомогательным для решения задач факторизации чисел и дискретного логарифмирования. На вход подается некоторое количество кубитов в базовом состоянии $|0\rangle$, число которых рассчитывается по специальной формуле. Все эти кубиты вводятся в состояние связанности при помощи гейта Адамара. Дополнительно подается один кубит в состоянии $|1\rangle$. К последнему кубиту последовательно применяются контролируемые гейты для конструктивной интерференции так, чтобы получить квантовый оракул специального вида. Наконец, ко всем входным кубитам применяется квантовое преобразование Фурье *QFT*, после чего эти кубиты измеряются. Результат измерения с большой вероятностью дает период функции, оракул которой строится перед применением квантового преобразования Фурье. О том, как работает этот алгоритм, можно в деталях прочитать в [Душкин, 2015].

с произвольным числом кубитов скомпрометирует всю современную криптографическую защиту. Любая информация, зашифрованная такими асимметричными системами шифрования, как RSA, может быть раскрыта. Любое распределение ключей по открытым каналам при помощи таких протоколов, как протокол Диффи–Хеллмана, может быть перехвачено. В этом случае квантовое превосходство ломает всю устоявшуюся мировую систему криптографии. Впрочем, сегодня уже ведутся работы по так называемой постквантовой криптографии, в рамках которой разрабатываются многочисленные методы, защищенные от атак при помощи квантовых алгоритмов [PCQ, 2008].

Принимая во внимания данное ранее описание методов квантового распределения ключей, можно сказать, что сегодня сами квантовые технологии уже дали ответ на вопрос о том, как в условиях существования универсального квантового компьютера осуществлять криптографическую защиту информации. Поскольку уже на практике реализованы квантовые протоколы передачи информации, которые позволяют осуществить секретный обмен ключами по открытому каналу с достоверной возможностью определить, был ли канал скомпрометирован в процессе, сама квантовая природа реальности не позволяет прослушать такой канал без того, чтобы факт такого вмешательства был распознан. В итоге при массовом внедрении таких каналов возможно использование теоретически невзламываемых схем криптографической защиты, в том числе и схемы одноразового блокнота.

Сегодня еще не до конца осознаны те достижения, которые будут доступны человечеству после появления универсального квантового компьютера, поскольку имеющиеся несколько десятков квантовых алгоритмов являются довольно фундаментальными с точки зрения математики, и еще много работы предстоит для того, чтобы найти им применение в прикладном аспекте. Тем не менее уже ясно, что простое преобразование функций в квантовые оракулы в общем случае не даст ожидаемого увеличения производительности [Валиев 2004], так как разработка квантового алгоритма — вопрос скорее интуитивного озарения, нежели механического преобразования функций из одной вычислительной модели в другую.

Квантовое превосходство хорошо видно на примере алгоритма Гровера. Этот алгоритм осуществляет поиск в неструктурированной базе данных, которая должна быть специальным образом преобразована в квантовый оракул. Ускорение по сравнению с обычным перебором менее выражено, чем в других алгоритмах, но все равно существенное: в базе данных с N записями алгоритм находит требуемую запись за $O(\sqrt{N})$ итераций, в то время как перебор вариантов требует $N/2$ итераций. Это позволяет эффективно решать, к примеру, задачу определения значений обратной функции для произвольной функции на определенной ограниченной области определения. Если в базу данных внесены все значения функции для заданных значений аргументов, то алгоритм Гровера эффективно находит значения аргумента для заданного значения функции, причем если функция принимает одинаковое значение на нескольких значениях аргумента, то полный список аргументов будет найден еще быстрее [Душкин, 2015b]. Эта методика позволяет, к примеру, ускорять подбор вариантов решений там, где нет эффективного способа решения задачи, а используется либо прямой перебор, либо специфические эвристические методы.

Универсальный квантовый компьютер позволяет осуществлять симуляцию квантовых систем произвольной сложности, причем для такой симуляции требуется линейное число кубитов и времени [Прескилл, 2008]. Именно это открывает самые широкие возможности по решению задачи Фейнмана. Исследование свойств молекул на квантовом уровне позволит проектировать сложные молекулы и наномашины с заданными свойствами. Это, в свою очередь, позволяет предположить, что в области материаловедения, фармакологии и биохимии вообще будут произведены самые фантастические открытия и изобретения.

Однако не только задача Фейнмана может быть решена при помощи универсального квантового компьютера. Любая задача, которая полностью или частично сводится к задаче перемножения матриц гигантских размеров, может быть эффективно решена при помощи

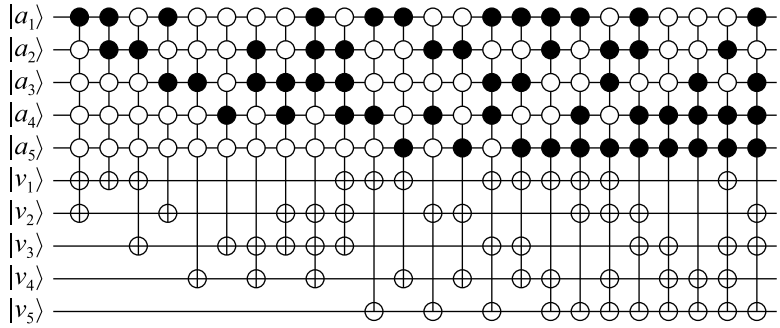

Рис. 6. Пример квантового оракула[4] для поискового запроса в алгоритме Гровера

Алгоритм Гровера предназначен для неструктурированного поиска в списке пар вида $\left[\langle a_i, b_i\rangle\right]_{i=1}^{N}$. Для такого списка создается квантовый оракул, который ставит в соответствие входному вектору $\overline{a_i}$ выходной вектор $\overline{b_i}$, после чего по заданному значению a_i возвращается значение b_i за $\sqrt{N}$ итераций, что дает сверхполиномиальное ускорение по сравнению с обычным перебором. О том, как работает этот алгоритм, можно в деталях прочитать в [Душкин, 2015].

квантовых вычислений, так как сама модель квантовых вычислений в своей основе представляет собой умножение входного вектора на матрицу унитарного преобразования волновой функции. Именно это осуществляют квантовые системы в процессе своей эволюции, и здесь речь идет о массовом параллелизме квантовых вычислений. И таким способом, к примеру, могут быть эффективно решены задачи моделирования сложных систем и хаотических динамических процессов (моделирование погоды, турбулентных потоков, ядерных взрывов и т. п.) и прогнозирования развития состояния сложных систем в фазовых пространствах большой размерности. Впрочем, необходимо помнить, что, несмотря на квантовый параллелизм, извлечь из кубита после измерения можно только один классический бит, так что часто в процессе решения подобных задач требуется выполнение ансамбля вычислений для оценки распределения вероятностей результатов. И в подобных случаях квантовое превосходство может быть сведено на нет, если требуемое для оценки количество запусков квантового алгоритма поглощает выигрыш от его исполнения.

В конечном итоге повсеместное использование квантовых технологий и модели квантовых вычислений может привести к появлению того, что называется сильным искусственным интеллектом, то есть искусственной интеллектуальной системы с самоосознанием. Другими словами, такой сильный искусственный интеллект будет осознавать себя разумным живым существом. Несмотря на то что гипотеза о квантовой природе сознания является довольно маргинальным направлением в науке [Пенроуз, 2011], ничто не запрещает искусственному сознанию проявиться именно в универсальном квантовом компьютере.

Квантовая механика, а за ней и модель квантовых вычислений — совершенно контринтуитивные вещи, о чем говорили даже отцы-основатели этой науки. Для того чтобы разобраться в ней, необходимо поистине совершить тектонический сдвиг парадигмы, осознать и принять многие явления, которые невозможны в воспринимаемой реальности. В качестве «мягкого введения» в квантовую механику можно использовать книгу [Иванов, 2015].

Cerne futurum[5].

[4] *Квантовый оракул* — квантовый аналог устройства типа «черного ящика». Фактически это «традиционная» функция, преобразованная специальным образом так, чтобы представлять собой квантовый гейт для использования в рамках квантовых вычислений.

[5] Предвосхищай будущее (лат.).

Список литературы (References)

Валиев К. А. Квантовые компьютеры: можно ли их сделать «большими»? — УФН. — 1999. — Т. 169. — С. 691—694.
Valiev K. A. Kvantovye kompyutery: mozhno li ikh sdelat' «bol'shimi»? [Quantum computers: could they be «big»?] // UFN. — 1999. — Vol. 169. — P. 691–694 (in Russian).

Валиев К. А., Кокин А. А. Квантовые компьютеры: надежды и реальность. — Ижевск: РХД, 2004. — 320 с.
Valiev K. A., Kokin A. A. Kvantovye kompyutery: nadezhdy i real'nost' [Quantum computers: hopes and reality]. — Izhevsk: RHD, 2004. — 320 p. (in Russian).

Грищенко Н. Китай ввел в эксплуатацию первый в мире спутник квантовой связи // Российская Газета, 18.01.2017. URL: https://rg.ru/2017/01/18/kitaj-vvel-v-ekspluataciiu-pervyj-v-mire-sputnik-kvantovoj-sviazi.html (дата обращения: 01.04.2018).
Grischenko N. Kitay vvyol v ekspluatatsiyu pervy v mire sputnik kvantovoy svyazi [China put into operation the world's first quantum communication satellite] // Rossiyskaya Gazeta, 18.01.2017 (in Russian). — URL: https://rg.ru/2017/01/18/kitaj-vvel-v-ekspluataciiu-pervyj-v-mire-sputnik-kvantovoj-sviazi.html (accessed: 01.04.2018).

Душкин Р. В. Квантовые вычисления и функциональное программирование. — М.: ДМК Пресс, 2015. — 232 с.
Dushkin R. V. Kvantovye vychislenia i funkcional'noye programmirovaniye [Quantum computing and functional programming]. — Moscow: DMK Press, 2015. — 232 p. (in Russian).

Душкин Р. В. (2015b) Факторизация числа при помощи квантового алгоритма Гровера. URL: https://eax.me/grovers-algorithm/ (дата обращения: 02.04.2018).
Dushkin R. V. Faktorizatsiya chisla pri pomoschi kvantovogo algoritma Grovera [Numbers Factorization by using of Quantum Grover's Algorithm] (in Russian). — URL: https://eax.me/grovers-algorithm/ (accessed: 02.04.2018).

Иванов М. Г. Как понимать квантовую механику. — Изд. 2, испр. и доп. — М.: УРСС, 2015. — 532 с.
Ivanov M. G. Kak ponimat' kvantovuyu mechaniku [How to understand quantum mechanics]. — 2nd ed. — Moscow: URSS, 2015. — 532 p. (in Russian).

Манин Ю. И. Вычислимое и невычислимое. — М.: Советское радио, 1980. — 128 с.
Manin Yu. I. Vychislimoye i nevychislimoye [Computable and non-computable]. — Moscow: Soviet radio, 1980. — 128 p. (in Russian).

Нильсен М., Чанг И. Квантовые вычисления и квантовая информация / пер. с англ. — М.: Мир, 2006 г. — 824 с.
Nielsen M. A., Chuang I. L. Quantum Computation and Quantum Information. — Cambridge: Cambridge University Press. (Russ. ed.: Nielsen M., Chuang I. Kvantivye vychisleniya i kvantovaya informaciya. — Moscow: Mir, 2006. — 824 p.)

Пенроуз Р. Тени разума. В поисках науки о сознании / пер. с англ. А. Р. Логунова, Н. А. Зубченко. — М.–Ижевск: ИКИ, 2011. — 688 с.
Penrose R. Shadows of the Mind. A Search for the Missing Science of Consciousness. — Vintage Books, 3. Oktober 1995. (Russ. ed.: Penrose R. Teni razuma. V poiskakh nauki o soznanii. — Moscow–Izhevsk: ICS, 2011. — 688 p.)

Прескилл Дж. Квантовая информация и квантовые вычисления. — М.–Ижевск: РХД, 2008–2011. — 464 + 312 с.
Preskill J. Lecture notes for physics 229: Quantum information and computation. — California Institute of Technology 16. (Russ. ed.: Preskill J. Kvantovaya informaciya i kvantovye vychisleniya. — Moscow–Izhevsk: RHD, 2008–2011. — 464 + 312 p.)

Фёдоров А. Квантовый компьютер: большая игра на повышение. Лекция в Яндексе. — URL: https://habrahabr.ru/company/yandex/blog/332106/ (дата обращения: 25.02.2018).
Fyodorov A. Kvantovy kompyuter: bol'shaya igra na povysheniye. Lekciya v Yandexe [Quantum computer: Big Game on Boosting] (in Russian). — URL: https://habrahabr.ru/company/yandex/blog/332106/ (accessed: 25.02.2018).

Янковская Ю. Ю., Марина А. А. Стойкость квантовых протоколов распределения ключей. — 2013. — С. 1–5.
Yankovskaya Yu. Yu., Marina A. A. Stoykost' kvantovykh protokolov raspredeleniya klyuchey [Persistence of quantum key distribution protocols]. — 2013. — P. 1–5.

Acin A., Gisin N., Scarani V. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks // Physical Review Letters. — 2004. — P. 69, 012309.

Bennett C. H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing // Proceedings of International Conference on Computers, Systems & Signal Processing, Dec. 9–12, 1984, Bangalore, India. — IEEE, 1984. — P. 175.

Bennett C. H. Quantum Cryptography: Uncertainty in the Service of Privacy // Science / M. McNutt. — American Association for the Advancement of Science, 1992. — Vol. 257, is. 5071. — P. 752-3. — DOI:10.1126/SCIENCE.257.5071.752

de Broglie L. Recherches sur la théorie des quanta [Researches on the quantum theory] // Thesis (Paris), 1924; L. de Broglie, Ann. Phys. (Paris). — 3, 22 (1925).

Dario G. The Future of Computing: AI and Quantum // IEEE Industry Summit on the Future of Computing, 10 November 2017.

Das A., Chakrabarti B. K. Colloquium: Quantum annealing and analog quantum computation // Rev. Mod. Phys. — 2008. — Vol. 80. — P. 1061–1081. — DOI:10.1103/revmodphys.80.1061

Deutsch D. The Church-Turing principle and the universal quantum computer // Proceedings of the Royal Society of London A. 400. — 1985. — P. 97. — DOI:10.1098/rspa.1985.0070

Dubois C. Q# Is for Quantum Computing: A New Programming Language from Microsoft. — December 2017. — URL: https://www.allaboutcircuits.com/news/q-is-for-quantum-computing-programming-language-Microsoft/ (accessed: 28.02.2018).

Ekert A. K. Quantum Cryptography Based on Bell's Theorem // Physical Review Letters. — 1991. — Vol. 67. — P. 661–663.

Feynman R. Simulating Physics with Computers // Int. J. Theor. Phys. — 1982. — Vol. 21. — P. 467–488.

Glendinning I. Quantum Programming Languages and Tools. — March 2017. — URL: http://www.vcpc.univie.ac.at/~ian/hotlist/qc/programming.shtml (accessed: 28.02.2018).

Gonçalves C. P. Quantum Cybernetics and Complex Quantum Systems Science — A Quantum Connectionist Exploration // NeuroQuantology. — February 2014. — Vol. 13 (1). — DOI:10.14704/nq.2015.13.1.804

Gregg J. Quantum Information: An Overview. — Berlin: Springer, 2006.

Huttner B., Imoto N., Gisin N., Mor T. Quantum Cryptography: Public Key Distribution and Coin Tossing // Physical Review A. — 1995. — P. 11–15.

Hwang T., Lee K.-C. EPR quantum key distribution protocols with potential 100 % qubit efficiency // Information Security, IET. — 2007. — Vol. 1, No. 1. — DOI:10.1049/iet-ifs:20060124

Jordan S. Quantum Algorithm Zoo. — Comprehensive catalog of quantum algorithms. — NIST, 2013. — URL: https://math.nist.gov/quantum/zoo/ (accessed: 25.02.2018).

Lo H., Ma X., Chen K. Decoy state quantum key distribution // Phys. Rev. Lett. — 2005. — Vol. 94. — P. 230504.

Popkin G. Scientists are close to building a quantum computer that can beat a conventional one. — December 2016. — URL: http://www.sciencemag.org/news/2016/12/scientists-are-close-building-quantum-computer-can-beat-conventional-one (accessed: 28.02.2018).

(PQC, 2008) Post-Quantum Cryptography. — Springer, 2008. — P. 245.

Proctor T. J., Knott P., Dunningham J. Multi-parameter estimation in networked quantum sensors. — 2017.

Selinger P. The Quipper Language. — July 2016. — URL: https://www.mathstat.dal.ca/~selinger/quipper/ (accessed: 28.02.2018).

Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Foundations of Computer Science: Conference Publications. — 1997. — P. 1484–1509.

Trabesinger A. Quantum computing: towards reality // Nature. — March 2017. — 543 (7646): S1–S1. — DOI:10.1038/543S1a

Ulanov A. E., Fedorov I. A., Pushkina A. A., Kurochkin Y., Ralph T. C., Lvovsky A. I. Undoing the effect of loss on quantum entanglement. — arXiv.org:1504.00886

Wootters W. K., Zurek W. H. A Single Quantum Cannot be Cloned // Nature. — 1982. — Vol. 299. — P. 802–803.

Zurek W. H. Reduction of the Wave Packet: How Long Does It Take? In Frontiers of Nonequilibrium Statistical Physics. Edited by P. Meystre and M. O. Scully. — New York: Plenum, 1984.

Zurek W. H. Decoherence and the Transition from Quantum to Classical — Revisited // Los Alamos Science. — 2002. — Number 27.