УДК 004.514.62 DOI: 10.32362/2500-316X-2019-7-1-5-37

КВАНТОВАЯ ИНФОРМАТИКА: ОБЗОР ОСНОВНЫХ ДОСТИЖЕНИЙ

А.С. Сигов[1],
Е.Г. Андрианова[1],
Д.О. Жуков[1],
С.В. Зыков[2],
И.Е. Тарасов[1]

[1]МИРЭА – Российский технологический университет, Москва 119454, Россия
[2]НИУ «Высшая школа экономики», Москва 101000, Россия
[@]Автор для переписки, e-mail: andrianova@mirea.ru

Обоснована актуальность проведения и выделены перспективные направления научных исследований в области квантовой информатики. По иностранным и российским публикациям и материалам сделан обзор основных научных результатов, характеризующих современное состояние исследований в квантовой информатике. Отмечено, что наиболее интенсивно знания и средства инвестируются в разработку архитектуры квантового компьютера и его элементов. Несмотря на то, что сегодня нет информации о создании физической реализации квантового компьютера, сравнимого по функциональным возможностям с классическим цифровым вычислителем, разработка квантовых алгоритмов является одним из актуальных направлений исследований. Преимущество квантовых алгоритмов заключается в снижении времени решения задачи за счет распараллеливания операций путем генерирования запутанных квантовых состояний и их последующего использования. Указанное преимущество (квантовое ускорение) является наиболее выигрышным при решении задачи моделирования динамики сложных систем и переборных математических задач (общий случай перебора – схема Гровера и ее варианты; задачи поиска скрытых периодов – схема Шора использования быстрого квантового преобразования Фурье и ее аналоги). Отмечена востребованность разработок в области кибербезопасности (поиск уязвимостей в умных пространствах, безопасное хранение и использование больших данных, квантовая криптография). Представлено более десятка статей, посвященных квантовым алгоритмам поиска ключей, распределению ключей на оптическом волокне различной длины, анализу квантовых ресурсов, необходимых для проведения кибератаки. В области искусственного квантового интеллекта внимание уделяется, в первую очередь, «поискам» модели квантовой нейронной сети, оптимальной с точки зрения использования всех преимуществ, представляемых квантовыми вычислениями и нейронными сетями, а также алгоритмам машинного обучения. Приведены примеры использования квантовых вычислений в когнитивных и социальных науках для исследования механизма принятия решений при неполных данных. Сделан вывод о перспективности применения квантовой информатики при моделировании сложных естественных и искусственных явлений и процессов.

Ключевые слова: квантовая информатика, квантовый компьютер, квантовые алгоритмы, моделирование сложных явлений и процессов, нейронные сети, машинное обучение, криптография, когнитивные технологии.

QUANTUM INFORMATICS: OVERVIEW OF THE MAIN ACHIEVEMENTS

A.S. Sigov[1],
E.G. Andrianova[1],
D.O. Zhukov[1],
S.V. Zykov[2],
I.E. Tarasov[1]

[1]MIREA – Russian University of Technology, Moscow 119454, Russia
[2]National Research Univeresity "Higher School of Economics", Moscow 101000, Russia
[@]Corresponding author e-mail: andrianova@mirea.ru

The urgency of conducting research in the field of quantum informatics is grounded. Promising areas of research are highlighted. For foreign and Russian publications and materials, a review of the main scientific results that characterize the current state of research in quantum computer science is made. It is noted that knowledge and funds are invested most intensively in the development of the architecture of a quantum computer and its elements. Despite the fact that today there is no information on the creation of a physical implementation of a quantum computer comparable in functionality to a classical digital computer, the development of quantum algorithms is one of the popular areas of research. An advantage of quantum algorithms is the fact that they reduce the time required to solve the problem due to the parallelization of operations by generating entangled quantum states and their subsequent use. This advantage (quantum acceleration) is most important when solving the problem of modeling the dynamics of complex systems and enumerated mathematical problems. (The general case of enumeration is the Grover scheme and its variants; the tasks of searching for hidden periods: Shor's scheme of using the fast quantum Fourier transform and its analogues.) The demand for cybersecurity developments (search for vulnerabilities in smart spaces, secure storage and use of big data, quantum cryptography) is noted. More than a dozen articles are devoted to quantum algorithms of key search, key distribution on optical fibers of various lengths, and the analysis of quantum resources necessary for conducting a cyber attack. In the field of artificial quantum intelligence, attention is paid, first of all, to the “search” for a model of a quantum neural network that is optimal from the point of view of using all the advantages presented by quantum computing and neural networks, as well as machine learning algorithms. Examples of the use of quantum computing in cognitive and social sciences for studying the decision-making mechanism with incomplete data are given. It is concluded that quantum informatics is promising for the simulation of complex natural and artificial phenomena and processes.

Keywords: quantum computer science, quantum computer, quantum algorithms, modeling of complex phenomena and processes, neural networks, machine learning, cryptography, cognitive technologies.

Введение

В докладе «Цифровая Россия: новая реальность», подготовленным экспертной группой Digital McKinsey, названы наиболее востребованные бизнес-сообществом направления деятельности в области IT-технологий в 2017–2018 гг.: это – облачные техно-

логии, Интернет вещей, технологии больших данных, кибербезопасность [1]. По мнению экспертов, «в соответствии с теорией циклов Кондратьева современный IT-рынок находится в самом начале очередного технологического цикла, который эксперты называют NBIC-конвергенция (конвергенция нано-, био-, информационных и когнитивных технологий). Она должна стать таким же прорывом, как в свое время прядильные, а потом паровые машины. И основной будущий тренд в сфере услуг, не только в IT, но и в конвергенции самых различных сервисов и услуг» [1].

В Программе «Цифровая экономика Российской Федерации», утвержденной летом 2017 года [2], определены направления государственной политики по созданию необходимых правовых, технических, организационных и финансовых условий для развития цифровой экономики в России, и перспективе ее интеграции в пространство цифровой экономики государств – членов Евразийского экономического союза. Цифровая экономика – хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг [3].

Для формирования исследовательских компетенций и технологических заделов, как одного из базовых направлений развития цифровой экономики в Российской Федерации [2], необходимо создание исследовательской инфраструктуры цифровых платформ. Исследовательские цифровые платформы должны стать инструментальным средством поддержки поисковых прикладных исследований в области цифровой экономики, обеспечивая технологическую независимость страны по таким сквозным цифровым технологиям, как большие данные, Интернет вещей и квантовые вычисления.

Эффективная обработка больших объемов данных требует высокопроизводительных вычислений в области искусственного интеллекта, наукоемких производственных направлений, моделирования химических и физических явлений и процессов, то есть там, где перестает хватать возможностей современных суперкомпьютеров. Существует мнение, что развитие транзисторных вычислителей почти достигло своего предела и что закон Мура, суть которого состоит в удваивании компьютерной мощности каждые полтора-два года, скоро перестанет действовать, так как размер транзисторов перестанет уменьшаться каждые 18 месяцев [4–7].

Квантовая обработка информации имеет существенный потенциал для повышения производительности вычислений. Она основана не на использовании традиционной булевой алгебры, а на логических представлениях квантовой механики, что обещает вычислительную мощность, выходящую за пределы возможностей любого классического компьютера, гарантируя при этом безопасную связь.

В связи с вышеизложенным обзор основных направлений развития и достижений квантовой информатики является актуальной задачей.

Квантовая информатика включает в себя вопросы квантовых вычислений и квантовых алгоритмов, физику квантовых компьютеров, квантовую криптографию и квантовую теорию информации, в частности, касается проблемы измерений и описания декогерентности. Базовое физическое явление, которое изучается в квантовой информатике – это запутанные квантовые состояния и порождаемые ими нелокальные свойства кван-

товой физики многих тел. К такому же мнению пришли и зарубежные исследователи. Например, в работе [8] отмечено, что вызовы со стороны секторов торговли, финансов, безопасности и логистики способствуют постоянному росту вычислительной техники. Квантовые вычисления представляют собой перспективную стратегию, которая предлагает новые возможности в безопасном вычислении, надежном хранении данных и эффективных приложениях. В бизнес-сообществе также растет осознание влияния квантовых вычислений на широкий спектр проблем и приложений потребителей.

Современными сферами приложения квантовой информатики являются квантовые вычисления (алгоритмы), квантовый компьютер, квантовая криптография, компьютерное моделирование систем многих частиц, применение в когнитивных технологиях, системах искусственного интеллекта. Рассмотрим важнейшие направления исследований в указанных областях.

Квантовый компьютер

Квантовый компьютер – средство вычислительной техники, в котором в основу работы центрального процессора заложена логика квантовой механики. Такой компьютер принципиально отличается от традиционного компьютера, имеющего архитектуру фон Неймана. Квантовый компьютер применяет для вычисления не классические алгоритмы, а процессы квантовой природы – квантовые алгоритмы, использующие явления квантовой механики, такие, как квантовый параллелизм и квантовая запутанность [9].

Базой квантовых вычислений является кубит (*Qubit*). Чтобы объяснить понятие «кубит», необходимо воспользоваться представлениями квантовой механики. Квантовые частицы имеют определенные характеристики, с помощью которых можно описывать их поведение и которые можно определять на практике (и, соответственно, реализовывать в квантовых компьютерах). В частности, фотоны обладают поляризацией, которую определяют через поведение вектора их электрического поля; некоторые микрочастицы обладают собственным магнитным моментом (спином), проекции которого на направление внешнего магнитного слоя находят экспериментально. В ходе традиционных вычислений используется понятие бита. Оно основано на том, что технически может быть реализовано только два состояния: 0 и 1 – например, ток протекает или нет проводимости (есть заряд или нет заряда) (рис. 1).

У кубита возможно существование не только двух состояний (например, спин квантовой частицы расположен по направлению внешнего поля – 0 или против – 1), но и их суперпозиции, что обусловлено квантовой природой явлений микромира. Суперпозицию состояний кубита представляют графически в виде координатной сетки на сфере, где каждый узел соответствует некоторому состоянию (центральная часть рис. 1).

Если каждое из состояний кубита обозначить $\alpha|0\rangle$ (функция, описывающая состояние, когда спин квантовой частицы направлен против внешнего поля) и $\beta|1\rangle$ (спин квантовой частицы направлен по направлению внешнего поля), то любое из множества возможных состояний будет определяться соотношением (суперпозицией):

$$\alpha|0\rangle + \beta|1\rangle$$

где α и β – комплексные функции, удовлетворяющие соотношению $|\alpha|^2 + |\beta|^2 = 1$ ($|\alpha|^2$ и $|\beta|^2$ являются амплитудами вероятностей переходов в состояния $\alpha|0\rangle$ и $\beta|1\rangle$). На рис. 1 справа

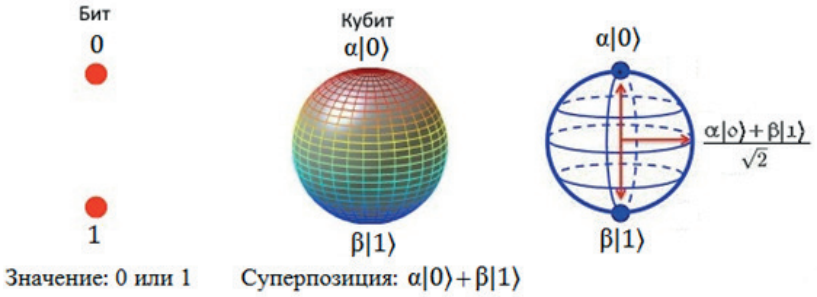

Рис. 1. Представление кубита [10].

показана возможность реализации состояния, когда спин квантовой частицы имеет направление, перпендикулярное внешнему магнитному полю.

Кубиты могут быть связаны (или запутаны) между собой. Это означает, что на них может быть наложена связь, вследствие чего при всяком изменении состояния одного из нескольких кубитов остальные меняются согласованно с ним, а совокупность запутанных между собой кубитов интерпретируется как заполненный квантовый регистр. Подобно отдельному кубиту, квантовый регистр гораздо сложнее классического регистра битов. Он способен не только находиться во всевозможных комбинациях составляющих его битов, но и реализовывать тонкие зависимости между ними, что существенно повышает вычислительные возможности систем, основанных на кубитах.

В состоянии связанности и суперпозиции кубиты представляют собой квантовый регистр. В ходе вычислений в квантовом регистре происходит выстраивание амплитуд кубитов ($|\alpha|^2$ и $|\beta|^2$) таким образом, что положительные значения амплитуды одних кубитов нейтрализуют отрицательные амплитуды других кубитов, и происходит отмена неверных вычислений (положительные амплитуды кубитов, напротив, усиливают друг друга). Так формируются сценарии получения верного ответа.

В [10] работа обычного и квантового компьютеров иллюстрируется поиском выхода из лабиринта: обычный компьютер последовательно перебирает все возможные варианты, упираясь в тупики и возвращаясь, а квантовый компьютер может проверить все возможные ходы за один раз.

Основная инженерная сложность состоит в поддержке состояния суперпозиции и спутанности кубитов в течение времени вычисления – времени когерентности.

Работы по созданию квантового компьютера активно ведутся Microsoft, IBM и Google. В марте 2018 г. из голландского центра Microsoft, расположенного в Техническом университете в Делфте (Delft University of Technology), сообщили об исследованиях по созданию квантового компьютера на базе майорановских фермионов, физические свойства которых позволят создать вычислитель с гораздо более низкой частотой ошибок, чем в проектах IBM и Google [11]. В России также ведутся подобные разработки: 15 февраля 2018 г. Внешэкономбанк, Фонд перспективных исследований, МГУ имени М.В. Ломоносова, «ВЭБ-Инновации» и АНО «Цифровая экономика» подписали соглашение о реализации комплексного научно-технического проекта по созданию в России многокубитного (не менее пятидесяти кубитов) оптического квантового симулятора на основе фотонных чипов и нейтральных атомов [12].

Между тем в статье [13], написанной два года назад, представлен квантовый компьютер на пяти кубитах, который был запрограммирован для реализации произвольных

квантовых алгоритмов на основе последовательности универсальных квантовых логических вентилей и обеспечил среднюю точность вычислений 98%. Переконфигурирование последовательности вентилей дает возможность гибкой реализации алгоритмов без изменения аппаратного обеспечения. В качестве примеров были реализованы алгоритмы Deutsch-Jozsa и Bernstein-Vazirani со средними коэффициентами успеха, соответственно, 95 и 90%. Реализовано также когерентное квантовое преобразование Фурье на пяти кубитах для оценки фазы и нахождения периода преобразования со средней точностью, соответственно, 62 и 84%. Представленный квантовый компьютер можно масштабировать до большего числа кубитов в одном регистре и дополнительно расширить посредством соединения нескольких модулей через челночный или квантовый канал.

Методика и результаты экспериментального сравнения двух архитектур пятикубитовых квантовых компьютеров (рис. 2), основанных на разных технологических платформах, даны в [14]. Здесь использован публичный доступ, предоставленный IBM, через облачную службу IBM «Quantum Experience» (www.research.ibm.com/ibm-q). Это дало возможность авторам работы реализовать в своем эксперименте 5-ти-кубитный квантовый компьютер на основе сверхпроводящих кубитов, связанных микроволновыми резонаторами (рис. 2A). Авторы статьи [14] запустили два одинаковых набора алгоритмов на компьютере IBM и на собственном квантовом компьютере идентичного размера и сопоставимых возможностей, но с физической реализацией на базе массива ионных ловушек, т.е. линейной цепи захваченных ионов, связанных лазерно-опосредованными взаимодействиями (рис. 2B).

Искусственные сверхпроводящие схемы в квантовом компьютере IBM можно рассматривать как «искусственные атомы». Это трансмонитные кубиты или сверхпроводящие островки, соединенные джозефсоновскими контактами и шунтирующими конденсаторами, которые обеспечивают суперпозиции зарядовых состояний, не чувствительных к флуктуациям заряда. Используемое здесь устройство имеет диапазон частот кубита от 5

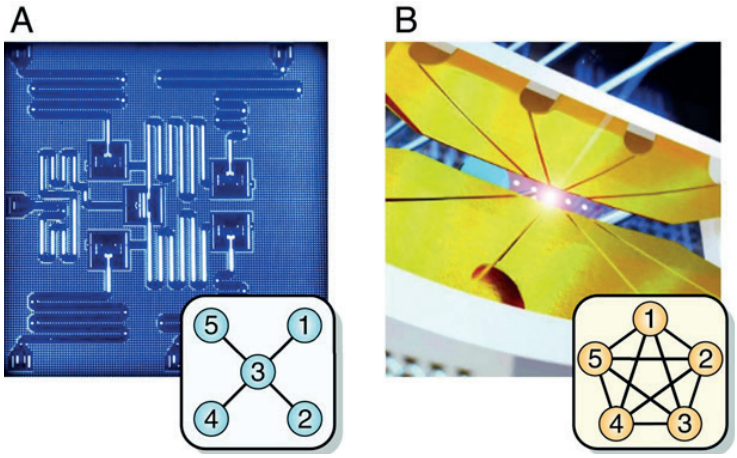

Рис. 2. Графическое представление архитектуры квантовых компьютеров, задействованных в эксперименте [14]: A – архитектура компьютера IBM на основе сверхпроводящих кубитов, связанных микроволновыми резонаторами (на вставке под изображением – график связности Qubit в форме звезды); B – архитектура компьютера авторов статьи, основанная на линейной цепи захваченных ионов, связанных лазерно-опосредованными взаимодействиями (на вставке под изображением – полносвязанный график связности Qubit).

до 5.4 ГГц (www.research.ibm.com/ibm-q). Кубиты связаны между собой и классической системой управления микроволновыми резонаторами. Состояния подготовки и считывания, а также одно- и двухкубитных ворот достигаются путем применения адаптированных микроволновых сигналов к этой сети и измерения отклика. Кубиты разрешаются в частотной области во время адресации и считывания. В аппаратуре Quantum Experience кубиты соединены в форме звезды, обеспечивающей четыре взаимодействия по второму кубиту (см. рис. 2A), которые представляют собой управляемые вентили NOT (CNOT), нацеленные на центральный кубит. Точность считывания с одного кубита обычно составляет 96%, а средняя точность считывания для произвольного состояния с 5 кубитами – 80%. Общедоступная система работает автономно, не требуя вмешательства человека, в течение многих недель (www.research.ibm.com/ibm-q).

Принцип работы второго компьютера (рис. 2B) является одним из подходов к построению крупномасштабного квантового компьютера. Ионы или заряженные атомные частицы могут быть ограничены и приостановлены в свободном пространстве с использованием электромагнитных полей. Кубиты хранятся в стабильных электронных состояниях каждого иона, а квантовая информация может передаваться через коллективное квантованное движение ионов в общей ловушке (взаимодействующей через кулоновскую силу). Лазеры применяются для индуцирования связи между кубитными состояниями (для операций с одним кубитом) или связью между внутренними состояниями кубитов и состояниями внешнего движения (для перепутывания между кубитами). Оба компьютера были запрограммированы независимо от базового оборудования, что позволило сравнить характеристики выполнения идентичных квантовых алгоритмов, работавших на различных физических основах (системах). Исследование показало, что квантовые алгоритмы, использующие больше возможностей подключения, выигрывают за счет более качественной связи системы кубитов. Хотя данное исследование проводилось на маленьких (по сравнению с классическими компьютерами) квантовых компьютерах, представлялось возможным оценить такие критические факторы масштабирования квантовых компьютеров, как связность кубитов и изменчивость сценария выполнения алгоритма. Кроме того, результаты показывают, что координирование конкретных квантовых приложений с самим компьютером будет иметь в дальнейшем решающее значение для успешного использования квантовых компьютеров.

К такому же выводу пришли в исследовании [15], где оценивались перспективы интеграции новых функциональных компонентов (блоков) квантовой обработки (QPU) квантовых процессоров в современные высокопроизводительные вычислительные системы (HPC – *high performance computing*) с учетом требований к функциональности и физическому дизайну. Намечены два подхода к интеграции, дифференцированные по инфраструктурным ограничениям в QPU и вариантам использования, традиционным для современных высокопроизводительных вычислительных систем. То есть возможен подход, когда QPU встраивается полностью, как один из компонентов системы, и параллельная работа, когда инфраструктурные ограничения трудно преодолимы. Получено, что производительность обоих подходов с большой вероятностью будет зависеть от квантового межсоединения, которое служит для запутывания множества кубитов QPU. Выявлены также несколько проблем в оценке производительности QPU для HPC и введены новые

показатели, фиксирующие взаимодействие между системной архитектурой и квантовым параллелизмом, лежащим в основе вычислительной производительности.

Квантовые алгоритмы

Несмотря на отсутствие физической реализации квантового компьютера, сравнимого по функциональным возможностям с классическим цифровым вычислителем, разработка квантовых алгоритмов является одним из востребованных направлений исследований.

Квантовый алгоритм является классическим алгоритмом, задающим последовательность унитарных операций (гейтов или вентилей) с указанием кубитов, над которыми их надо совершить. Квантовый алгоритм задается либо в виде словесного описания таких команд, либо с помощью их графической записи в виде системы вентилей (*quantum gate array*). Наиболее близким классическим аналогом квантового вычисления является вероятностное вычисление, т. е. правильность результата работы квантового алгоритма определена с некоторой вероятностью. Для повышения вероятности правильного результата в квантовых алгоритмах специально увеличивается кратность операций, которые подбираются таким образом, чтобы неправильные результаты с большой вероятностью взаимно уничтожались, и вероятность правильного результата увеличивалась. Множества задач, допускающих решение на квантовом компьютере и на классическом, совпадают.

Преимущество квантовых алгоритмов заключается в снижении времени решения задачи за счет распараллеливания операций путем генерирования запутанных квантовых состояний и их последующего использования. Такие случаи называются квантовым ускорением. Применение квантового ускорения является наиболее выигрышным при решении задачи моделирования динамики сложных систем и переборных математических задач (общий случай перебора – схема Гровера и ее варианты; задачи поиска скрытых периодов – схема Шора использования быстрого квантового преобразования Фурье и ее аналоги). Более подробно с различиями квантовых и классических алгоритмов можно ознакомиться в статьях [16, 17]. Существует и полный список разработанных на настоящий момент квантовых алгоритмов [18].

Одним из самых востребованных для множества задач является алгоритм поиска. Отмечается [19], что переборные задачи, в том числе алгоритм поиска Гровера (Grover), используемый для поиска определенного элемента в неструктурированной базе данных, квантовый компьютер решает быстрее, чем классический. Здесь же [19] приводится пример квантового варианта алгоритма поиска Гровера, исследуется функциональность квантового варианта алгоритма, обсуждаются преимущества квантовой реализации.

Рассмотрен в литературе и улучшенный квантовый алгоритм для подгонки модели линейной регрессии к заданному набору данных с использованием метода наименьших квадратов [20]. В отличие от предыдущих алгоритмов, которые дают квантовое состояние, кодирующее оптимальные параметры, улучшенный алгоритм выводит эти числа в классической форме. Таким образом, запустив его один раз, удастся полностью определить установленную модель, а затем использовать ее для прогнозирования новых данных. Улучшенный алгоритм работает в стандартной модели «Оракула» и может обрабатывать наборы данных с несравненными матрицами проектирования. Временная характеристика алгоритма:

$$\text{poly}\,(\log 2\,(N), d, \kappa, 1/\varepsilon),$$

где N – размер набора данных;

d – количество регулируемых параметров;

κ – номер условия проектной матрицы;

ε – заданная точность результата.

Авторы доказали, что полиномиальная зависимость от d и κ является объективной и, следовательно, данный алгоритм не может быть значительно улучшен. Кроме того, они показали, что разработанный квантовый алгоритм оценивает качество соответствия наименьших квадратов без явного вычисления его параметров, работая быстрее, чем алгоритмы, находящие это соответствие, и, следовательно, его целесообразно рекомендовать для проверки соответствия входного набора данных для линейной регрессии.

Со временем квантовые вычисления могут стать аппаратной платформой, способной существенно ускорить выполнение отдельных семейств классических алгоритмов. Уже сейчас экспериментально получены хорошие результаты в области масштабирования и отказоустойчивости для небольших квантовых вычислений, подтверждающие возможность полномасштабного квантового вычисления. Как и любой классический алгоритм, квантовый алгоритм должен быть эффективно реализован для получения максимально возможного преимущества от его выполнения. Как правило, квантовый алгоритм описывается в терминах процедур высокого уровня, таких, как арифметические операции (сложение, умножение, возведение в степень), или специальные преобразования, такие, как квантовое преобразование Фурье (QFT). Эти преобразования затем комбинируют в логические операции более высокого уровня, например, используя логические вентили Тоффоли, Фредкина. В публикации [21] описан созданный и реализованный авторами квантовый алгоритм аппроксимации одноцикловых вращений Rz (φ) с использованием схемы Clifford+T. Алгоритм способен обрабатывать ошибки в приближении вплоть до размера10^{-15}, что позволяет применять оптимальные схемы с одним кубитом, удобным для реализации масштабируемых квантовых алгоритмов.

Эффективный рандомизированный алгоритм аппроксимации произвольного элемента системы S произведением операторов Clifford+T с точностью до любого заданного порога ошибки ε>0 представлен в [22]. При слабой гипотезе о распределении простых чисел ожидаемое время выполнения алгоритма является полиномиальным 1/ε. Если оператор, который должен быть аппроксимирован, является z-вращением, то результирующая последовательность ворот равна T-count(K)+4log2(1/ε), где K приблизительно равно 10. Наихудшая нижняя граница равна K+4log2(1/ε) и достигается при K=-9. Следовательно, алгоритм находится в аддитивной постоянной оптимального для некоторых z-поворотов. Для произвольного члена S мы достигаем приближений с T-счетом K+12log2(1/ε). Напротив, алгоритм Соловея–Китаева достигает T-count(K)+12logc2(1/ε)), что составляет приблизительно 3.97. Приведенные показатели разработанного авторами алгоритма существенно лучше, чем показатели алгоритма Соловея–Китаева (Solovay–Kitaev).

В [23] описан эффективный синтез вероятностных квантовых цепей с запаздыванием. Цепи с повторением-до-успеха (RUS) могут аппроксимировать заданный единичный кубит с ожидаемым числом T-ворот около 1/3 от того, что требуется оптимальными, детерминированными, безразмерными разложениями по набору ворот Clifford+T. Пред-

лагается более общий и концептуально более простой метод декомпозиции схем [23], позволяющий синтезировать протоколы, которые вероятностно реализуют квантовые схемы над несколькими универсальными наборами ворот, включая, но не ограничиваясь, набором ворот Clifford+T. Протокол, названный авторами вероятностными квантовыми цепями с запаздыванием (PQF), реализует проход по дискретной цепи Маркова. В ней целевое унитарное состояние является поглощающим состоянием, и переходы индуцируются многократными унитарными единицами, за которыми следуют измерения. В отличие от протоколов RUS, представленные протоколы PQF гарантированно завершаются после конечного числа шагов [23]. Здесь же описано применение разработанного метода к наборам Clifford+T, Clifford+V и Clifford+π/12 для достижения разложений с ожидаемыми подсчетами ворот $\log b(1/\varepsilon)+O\{\ln[\ln(1/\varepsilon)]\}$, где b – величина, связанная со свойством расширения базового набора универсальных ворот.

Основные применения квантовых вычислений

Существует два типа задач, которые квантовые компьютеры способны решать намного эффективнее классических компьютеров. Первый тип – это задачи криптографии. На сегодняшний день многие системы шифрования основываются на перемножении больших чисел и их поиске с целью получения взломостойкого шифра. Самый большой интерес состоит в возможности дешифрования данных. В настоящий время безопасность шифрования заключается в том, что на расшифровку данных требуются несоизмеримо большие вычислительные мощности и огромное время, измеряемое в тысячелетиях. Квантовые компьютеры способны раскрыть такой шифр намного быстрее, примерно за то же время, что затрачено на само шифрование. Именно поэтому банковские и технологические компании заинтересованы в развитии квантовых вычислений.

Второй тип задач заключается в способности квантовых компьютеров эмулировать различные квантовые системы. И именно эта возможность, вероятно, перевернет человеческие представления о биологических системах, сверхпроводимых материалах или выведет на новый уровень понимания квантовой химии, не говоря уже о квантовой физике. Моделирование наблюдаемых явлений является незаменимым инструментом для разработки новых технологий, понимания естественного мира и изучения человеческого общества, однако наиболее интересные системы зачастую настолько сложны, что имитация их будущего поведения требует хранения огромных объемов информации о том, как они себя вели в прошлом. В случае более сложных систем симуляция становится все сложнее и, в конечном итоге, ограничивается такими ресурсами, как компьютерная память. Показано [24], что применение квантовых алгоритмов позволит уменьшить указанную потребность в памяти, измеряемую статистической сложностью процесса. Описано экспериментальное исследование приведенного квантового преимущества для моделирования стохастических процессов. Авторская квантовая реализация учитывает потребность в памяти $C_q=0.05\pm0.01$, что намного ниже предельного классического предела $C=1$. Масштабирование этого метода существенно уменьшит объем памяти, необходимый для моделирования более сложных систем.

Рассмотрим направления исследований в различных сферах.

Кибербезопасность. Умные пространства и безопасное хранение и использование больших данных. Рассмотрена возможность применения квантовых вычислений для поиска уязвимостей в умных пространствах [25]. Отмечено, что оба направления сегодня развиваются достаточно бурно и обе технологии вошли в десятку самых значительных трендов 2019 г. по версии исследовательского агентства Gartner, одного из лидеров в области систем хранения данных. Умное пространство должно объединить людей, процессы, сервисы и вещи, что позволит перевести на новый уровень выполнение многих привычных функций, позволит создать «умный дом», «цифровые места» и даже «умные города», подключив всю инфраструктуру к одной сети. Широкое распространение умных пространств потребует изменения подхода к системам хранения данных. В умной среде устройства периодически обмениваются данными по сети – либо напрямую от устройства к устройству, либо через облачные серверы. Появятся новые возможности для кибератак. Эксперты Gartner прогнозируют, что к 2023–2025 гг. бизнес-структуры начнут активно внедрять квантовые технологии, что заставит ввести новые стандарты кибербезопасности для систем хранения данных. Выход видится в разработке новых квантовых алгоритмов поиска уязвимостей и киберзащиты.

В развитие вышеуказанной темы в работе [26] обсуждаются «слепые» квантовые вычисления (*blind quantum computing,* BQC). Понятие «слепое» означает, что квантовый компьютер не имеет полной информации о задачах, которые он решает. Это гарантирует безопасность клиентских вычислительных задач. «Слепые» квантовые вычисления пока не получили распространения, поскольку требуют наличия у клиентов квантовых устройств, с которых задачи передаются на квантовые серверы. Конфиденциальность выполнения квантовых вычислений особенно важна, поскольку многие потенциальные задачи (как, например, умные пространства) требуют высокой степени безопасности. Желательным свойством для любого протокола BQC является проверка, в соответствии с которой клиент может с большой вероятностью проверить, выполнял ли сервер инструкции или произошло некоторое отклонение, приводящее к поврежденному состоянию вывода. Протокол BQC можно рассматривать как интерактивную систему доказательств. Авторами [26] предложена универсальная безопасная схема BQC, в которой клиенту нужно только подготовить отдельные кубиты в разделяемых состояниях, случайным образом выбранных из конечного набора, и отправить их на сервер, имеющий все необходимые квантовые вычислительные ресурсы. Добавив в описанный протокол дополнительные функции, авторы приводят строгое доказательство, что вероятность невозможности обнаружения неправильного вывода экспоненциально мала по параметру безопасности, тогда как затраты ресурсов остаются полиномиальными по этому параметру. Введенные дополнительные функции дают состояние ресурса, позволяющее выполнять запутывание шлюзов между произвольными парами логических кубитов только с постоянными служебными данными. Предложенное улучшение имеет важные последствия для порогов эффективности и отказоустойчивости.

В [27] рассмотрены последние разработки в квантовых алгоритмах, с акцентом на оценках ресурсов для взлома криптографических протоколов на квантовом компьютере. Полученные оценки, в свою очередь, могут быть использованы для получения квантовых параметров безопасности для различных схем. Авторы сравнивают эти криптографические приложения с приложениями, основанными на способности квантового компьютера эффективно имитировать другие системы квантовой механики.

Квантовая криптография. Квантовая криптография направлена на решение практической проблемы построения масштабируемых и защищенных квантовых сетей.

Одной из задач квантовой криптографии является удаленное распространение секретных ключей. Значительным шагом в этом направлении стало введение независимости измерительного устройства, когда секретный ключ между двумя сторонами устанавливается путем измерения ненадежного реле [28]. Ключевые показатели протоколов, реализованных в кубите, как правило, очень низкие, непригодные для требований городской сети. Показано [28], что решением может стать использование квантовых систем связи за счет сетевого протокола с когерентным состоянием. Разработанный протокол по своим количественным показателям превышает существующие на три порядка, и его можно использовать для создания высокоскоростных квантовых сетей, где устройства надежно подключаются к ближайшим точкам доступа или прокси-серверам.

Ключи. В данном обзоре представлено более десятка статей [29–40], посвященных квантовым алгоритмам поиска ключей, распределению ключей на оптическом волокне различной длины, анализу квантовых ресурсов, необходимых для проведения кибератаки.

В [29] представлен квантовый алгоритм Гровера для реализации исчерпывающего поиска ключа применительно к Advanced Encryption Standard (AES, расширенный стандарт шифрования) и анализу квантовых ресурсов, необходимых для проведения атаки. Авторами [29] рассмотрены количество операций алгоритма, количество кубитов и глубина алгоритма как исходная информация оценки трудоемкости квантового алгоритма Гровера. В качестве базового набора выбран Clifford+T gates как основной отказоустойчивый логический набор квантовых вентилей (ворот). Для всех трех вариантов AES (размеры ключа 128, 192 и 256 бит), которые стандартизованы в FIPS-PUB 197, установлены точные оценки числа кубитов и числа элементарных логических квантовых ворот, которые необходимы, чтобы реализовать представленный квантовый алгоритм Гровера для извлечения ключа из небольшого числа пар AES plain text–cipher text.

При базовой атаке ключа, связанного с блочным шифрованием, противник имеет доступ к шифрам под ключами, которые отличаются от целевого ключа бит-флипсами. Показано [30], что для квантового противника такие атаки достаточно сильны при условии, что: 1) секретный ключ однозначно определяется небольшим числом пар символов открытого текста; 2) блочный шифр может быть эффективно оценен и 3) может быть запрошена суперпозиция связанных ключей. Тогда ключ может быть эффективно извлечен.

Быстрая и универсальная система распределения квантовых ключей (QKD, *quantum key disctribution*) с аппаратным переключением ключей и мультиплексированием по длине волны рассматривается в [31]. Авторы описали компактно интегрированную когерентную одностороннюю систему распределения квантовых ключей с тактовой частотой 625 МГц, которая непрерывно распределяет секретные ключи по волоконно-оптической линии связи. Для поддержки высоких скоростей секретных ключей внедрен быстрый механизм перегонки аппаратного ключа, позволяющий в режиме реального времени увеличить скорость передачи до 4 Мбит/с. Данная система использует мультиплексирование по длине волны, чтобы работать только с одним оптическим волокном. На основе использования быстродействующих одиночных фотонных детекторов InGaAs реализовано надежное распределение секретных ключей со скоростью выше 21 кбит/с на 25 км опти-

ческого волокна. Авторы выполнили оптимизацию системы с учетом результатов анализа безопасности, включающих эффекты конечного размера, затраты на аутентификацию и системные ошибки для параметра безопасности $\varepsilon_{QKD} = 4\times10^{-9}$.

Авторы [32] позиционируют свое исследование как первый эксперимент по распределению квантовых ключей (QKD) с потерей в канале 72 дБ с использованием сверхнизких сверхпроводящих нанопроволочных однофотонных детекторов (SSPD, SNSPD) со скоростью теневого счета (DCR) 0.01 сП. Они используют схему дифференциального фазового сдвига QKD (DPS-QKD) с тактовой частотой 1 ГГц. Достигается значение коэффициента квантовой битовой ошибки (QBER) ниже 3%, когда длина волокна с дисперсией сдвига (DSF) составляет 336 км (потеря 72 дБ), что является достаточно низким для создания защищенных ключей.

Как мера противодействия квантовым кибератакам предложено независимое от измеряющего устройства квантовое распределение ключей (*measurement-device-independent quantum key disctribution*, MDI-QKD).

Выбор протокола и оптимизация параметров в MDI-QKD обсуждается в [33]. MDI-QKD продемонстрировано в лабораторных условиях и в полевых испытаниях с использованием ослабленных лазеров в сочетании с техникой приманки. Отмечено [33], что на сегодняшний день отсутствуют результаты строгого сравнения различных протоколов MDI-QKD на основе приманки с двумя или тремя ее состояниями, следовательно, не определено количество типов состояний приманки, необходимое для реализации MDI-QKD. Системные параметры для реализации MDI-QKD с декомпозицией частично оптимизированы в известных авторам предыдущих работах, что ставит под сомнение фактическую производительность указанных демонстраций. Авторы приводят аналитические и численные методы декомпозиции с одним, двумя и тремя состояниями приманки, дают четкое сравнение этих методов и делают вывод, что два состояния приманки уже позволяют получить почти оптимальную оценку, а большее количество состояний приманки не могут значительно улучшить ключевую скорость в настройках асимптотики или конечных данных. Выполнена полная оптимизация параметров системы и показано, что полная оптимизация может значительно улучшить скорость ключа в настройке конечных данных. При проведении эксперимента установлено, что полная оптимизация может увеличить коэффициент ключа более, чем на один порядок по сравнению с неоптимизацией. Предложен локальный метод поиска для эффективной оптимизации параметров системы. Этот метод на четыре порядка быстрее, чем тривиальный исчерпывающий поиск для достижения аналогичной оптимальной скорости ключа.

Анализу конечных ключей для MDI-QKD посвящена работа [34]. Авторы предполагают, что хотя распределение квантовых ключей обещает безоговорочно безопасную связь, реальные устройства могут отклоняться от своих спецификаций, следовательно, безопасность практических систем не может быть гарантирована. В частности, противник может использовать несовершенные извещатели, чтобы изучить большую часть секретного ключа, даже несмотря на то, что обеспечение безопасности доказано иначе. Для решения этой проблемы и предложен практический подход – независимое от измерительного устройства распределение квантовых ключей. Однако до сих пор его безопасность полностью доказана только в предположении, что легальные пользователи си-

стемы имеют неограниченные ресурсы. Авторы восполнили этот пробел и обеспечили строгую защиту от общих атак в режиме с конечным ключом. Данный результат получен применением теории больших уклонений, в частности границ Чернова, для оценки параметров. Впервые продемонстрирована возможность реализации на дальних дистанциях MDI-QKD в приемлемые сроки передачи сигнала.

Продемонстрирована первая реализация поляризационного кодирования MDI-QKD [35], которое невосприимчиво ко всем атакам с боковым каналом извещателя. Активная фазовая рандомизация каждого индивидуального импульса применяется для защиты от атак на несовершенные источники. Путем оптимизации параметров в протоколе состояния decoy (состояние-ловушка) показано, что возможно реализовать поляризационное кодирование MDI-QKD с коммерческими готовыми устройствами. Для оценки безопасной скорости ключа применялся строгий анализ конечных ключей. Данное исследование открывает возможность для реализации сети MDI-QKD, при которой пользователям нужны только компактные и недорогие устройства для подготовки состояний кубитов.

Традиционно статистические флуктуации, принимаемые из различных источников, обрабатываются отдельно. Так, предложена методика улучшенного статистического флуктуационного анализа для MDI-QKD с использованием метода трехуровневых ложных состояний-ловушек [36]. Рассматривая статистические флуктуации, принимаемые из различных источников, как единый поток, авторы представили формулы для ключевых величин, используемых при вычислении безопасного финального ключа. Численное моделирование показало, что с учетом общего количества импульсов, равного 10^{12}, предложенный метод улучшает ключевую скорость примерно на 97% на расстояние 50 км по сравнению с предыдущими результатами и улучшает коэффициент ключа на 145% на расстояние 100 км по сравнению с результатом полной оптимизации всех параметров.

MDI-QKD является существенным шагом на пути к практической теоретико-информационной безопасности для обмена ключами между удаленными легальными пользователями [37]. Как и в случае с другими стандартными протоколами распределения квантовых ключей, зависящими от устройства, такими, как BB84, MDI-QKD предполагает, что эталонные фреймы были разделены между пользователями. На практике часто необходима нетривиальная процедура выравнивания, которая требует системных ресурсов и может значительно снизить скорость генерации безопасного ключа. Авторы [37] предлагают схему MDI-QKD с фазовым кодированием, не требующую фазового выравнивания между интерферометрами двух отдаленных легальных сторон. В качестве демонстрации представлен эксперимент с доказательством принципа с использованием интерферометров Фарадея–Майкельсона. Экспериментальная система работала на частоте 1 МГц, и средняя скорость ключа 8.309 б.п. была получена при длине волокна 20 км между пользователями. Система может поддерживать положительную скорость генерации ключа без компенсации фазы в нормальных условиях. Результаты показывают возможность данной системы для использования в готовых к практическому использованию устройствах MDI-QKD и ее значение для сетевых сценариев.

Распределение квантовых ключей без детекторных уязвимостей с использованием оптических затравочных лазеров показано в [38]. Из-за высокой чувствительности и сложного дизайна детекторы являются наиболее часто атакованными компонентами. Не-

давно было показано, что для устранения любой уязвимости от детекторов может быть использована двухфотонная интерференция из независимых источников света. Эта новая форма MDI-QKD была экспериментально продемонстрирована, но со скромными ключевыми скоростями и использованием новых импульсных методов для получения высокочувствительных помех от лазеров с коммутацией каналов и, таким образом, выполняет MDI-QKD с беспрецедентными скоростями ключа, превышающими 1 мегабит в секунду в режиме конечного размера. Это представляет собой улучшение на два-шесть порядков над существующими реализациями и поддерживает новую схему в качестве практического ресурса для обеспечения надежной квантовой связи.

MDI-QKD на оптическом волокне длиной 404 км обсуждается в [39]. Рассмотренное квантовое распределение ключей не зависит от измерения методом декомпозиции, отрицает угрозы безопасности от несовершенного однофотонного источника, а также от потерь обнаружения. Удлинение дистанции и улучшение ключевой скорости квантового распределения ключей являются жизненно важными проблемами в практических применениях QKD. Приведены результаты MDI-QKD на более 404 км сверхнизкого оптического волокна и 311 км стандартного оптического волокна при использовании оптимизированного метода четырехуровневых ложных состояний-ловушек [39]. Эта рекордная реализация метода MDI-QKD не только обеспечивает новую дистанционную запись для MDI-QKD и всех типов QKD-систем, но и – что более важно – достигает расстояния, которое традиционный BKK-Bassart 1984 BKD не сможет достичь с помощью тех же устройств обнаружения даже с идеальными однофотонными источниками. Указанная публикация [39] представляет собой значительный шаг к доказательству и разработке возможного дальнего QKD.

Организация независимого квантового распределения ключей (QKD) на гибридной логической основе – множественном кубите, который первоначально введен в контексте отказоустойчивых квантовых вычислений в декогерентности свободного подпространства (DFS), имеет конкретные приложения для решения проблемы несоосности опорного кадра в квантовых информационных протоколах [40]. Предлагается безрисковая схема MDI-QKD [40] с вращательно-инвариантным состоянием, которая невосприимчива к коллективному шуму, вызванному несоосностью между двумя удаленными легитимными сторонами. В предложенном протоколе начальный логический кубит создается в гибридном пространстве с поляризованным орбитальным угловым моментом, в то время как передача полностью выполняется в инвариантной по повороту DFS при наличии коллективного шума, связанного с несоосностью. Частичное измерение состояния Белла выполняется на логических кубитах для его сортировки. По сравнению с оригинальными протоколами MDI-QKD численное моделирование показывает, что модифицированная схема существенно лучше и по расстоянию передачи, и по скорости генерации ключей. Кроме того, в предложенном протоколе требуются только обычные оптические элементы.

Квантовые нейронные сети и системы машинного обучения. Существует мнение [41], что интеллектуальная обработка и анализ больших данных – это работа именно для квантового интеллекта. Слияние квантовых вычислений, нейронных сетей и машинного обучения стало быстро развивающейся областью исследований. Однако «камень преткновения» здесь в том, что квантовый компьютер работает на квантовых состояниях, а не

на человекочитаемых данных, и быстрый интерфейс передачи большого объема данных квантовому компьютеру пока не реализован. В качестве примера приводится мощный сотовый телефон, подключенный к медленно работающей сотовой сети, сводящей «на нет» все его мощные характеристики [41].

«Нейронная сеть представляет собой программную или (опто-)электронную систему, обеспечивающую принятие решений путем эволюции сложной нелинейной системы, на вход которой подается вектор входных данных, а выходной сигнал (в общем случае многомерный) кодирует принимаемое решение. По сути, нейронная сеть представляет собой некий черный ящик, способный (в зависимости от своего внутреннего состояния) отображать N-мерный вектор входных данных в M-мерный вектор выходных данных. При этом внутреннее состояние нейронной сети адаптивно, т. е. изменяется в процессе обучения» [42]. Обучение нейронной сети может проходить двумя способами. Первый способ – это самообучение нейронной сети, при котором достаточно иметь только векторы входных данных; изменение состояния сети происходит за счет самоорганизации, т. е. зависит от корреляций между векторами. Второй способ – это обучение с учителем, когда на вход нейронной сети подаются данные, для которых результат работы нейронной сети является известным, и работа сети, соответственно, может быть оценена и скорректирована.

Нейронная сеть состоит из базовых вычислительных единиц-«нейронов», преобразователей входного сигнала в выходной с использованием нелинейной переходной функции. «Сеть представляет собой нелинейный параллельный процессор, основанный в общем случае на связи всех нейронов со всеми» [42]. В процессе обучения сети изменяются интенсивности связей, соединяющих нейроны, и в результате существенно отличными от нуля остаются лишь те связи, которые ведут к правильному решению.

Нейроны располагаются обычно по слоям, контролируя вывод нескольких других нейронов, и меняют свое состояние при определенных условиях. Например, при распознавании изображения начальный слой нейронов принимает входные данные – пиксели, промежуточные слои создают различные комбинации ввода, отображающие некие геометрические фигуры, а заключительный уровень создает описание изображения.

Известно и другое определение нейронной сети [43]: нейронная сеть представляет собой существенно параллельную распределенную систему обработки информации, состоящую из простых идентичных блоков – нейронов, обладающих способностью хранить информацию и предоставлять ее для использования. Квантовая нейронная сеть заменяет классические сигналы, поступающие на вход нейрона, на квантовые состояния, обладающие амплитудой и фазами. На выходе квантовой нейронной сети должно формироваться квантовое состояние, зависящее от линейной суперпозиции входящих состояний [42], т .е. квантовая нейронная сеть построена из набора модели кубитов нейрона, внутреннее состояние которого является когерентной суперпозицией кубитовых состояний.

В настоящее время происходит «поиск» модели квантовой нейронной сети, оптимальной с точки зрения использования всех преимуществ, которые представляют квантовые вычисления и нейронные сети. Например, в [44] дано систематическое перечисление и описание различных подходов и результатов таких исследований. Сделан акцент на сети типа Хопфилда и задачу ассоциативной памяти, и поставлена задача объединить нелинейную диссипативную динамику нейронных вычислений и линейную унитарную

динамику квантовых вычислений. Выработаны также критерии эффективности архитектуры квантовой нейронной сети. В результате из рассмотренных исследований по потенциальной модели квантовой нейронной сети ни один из вариантов не признан полностью удовлетворительным. В качестве перспективного направления исследований отмечена идея открытых квантовых нейронных сетей на основе диссипативных квантовых вычислений.

Имеется информация о новой квантовой сети нейронных деревьев Qubit с улучшенными нейронами Qubit, устанавливаемыми межслойными связями и различными фазовыми операционными функциями для каждого нейрона [45]. Сеть нейронного дерева Qubit может быть построена и оптимизирована с помощью древовидной кодировки на основе эволюционного алгоритма. В отличие от других подобных сетей Qubit разрешает выбор набора терминалов и установку межслойных соединений. Улучшенный нейрон Qubit применяется вместо сигмовидной функции для решения нелинейных задач моделирования. Для оценки эффективности и производительности предлагаемой сети были выбраны три нелинейные задачи моделирования. Результаты моделирования показали, что сеть нейронных деревьев Qubit имеет хорошие показатели по производительности и эффективности при нелинейном моделировании.

Предлагается [46] квантовая нейронная сеть, называемая квантовым персептроном над полем (QPF), которую невозможно смоделировать на классическом компьютере. QPF является прямым обобщением классического персептрона, избавленного от ряда ограничений. В статье приведен основанный на суперпозиции алгоритм обучения с алгоритмом SAL, который оптимизирует веса и архитектуры нейронной сети. SAL ищет лучшую архитектуру в конечном наборе нейронных сетевых архитектур с линейным временем по количеству шаблонов в обучающем наборе. SAL является первым алгоритмом обучения для определения нейронных сетевых архитектур в полиномиальное время, данный результат получен за счет использования квантового параллелизма и нелинейного квантового оператора.

Описан эффективный метод разработки нейронных сетей с несколькими соединениями и высокой степенью классификации: эволюционный алгоритм (QEA), основанный на принципах квантовых вычислений [47]. Получено, что при схождении квантовой эволюционной нейронной сети (QENN) на этапе обучения, последующее обучение бессмысленно. Поэтому важно контролировать количество поколений QENN. Анализ свойства сходимости квантовой эволюции битов дает возможность сформулировать всегда достижимый безопасный критерий завершения обучения, например, основанный на средней скорости конвергенции (ACR). Метод экспериментально опробован и подтвержден на задачах классификации. Результаты показали, что критерий завершения, основанный на ACR, может должным образом остановить процесс обучения QENN и преодолеть ограничения критерия завершения, основанные на вероятности генерации наилучшего решения (PBS).

С целью повышения аппроксимирующей способности традиционной искусственной нейронной сети (ANN) предложена основанная на квантовых началах нейронная сеть (SIQNN) [48]. В этой модели скрытые узлы состоят из нескольких многобайтовых управляемых-НЕ-логических ворот, входы описываются многомерными дискретными

последовательностями кубитов, выходными узлами являются традиционные нейроны. Параметры модели включают в себя углы квантовых вращений в скрытом слое и веса – в выходном слое. Алгоритмы обучения получены с использованием алгоритма Левенберга–Марквардта. Результаты моделирования прогнозирования стока Хунцзядуйского водохранилища в Китае показывают, что SIQNN, очевидно, превосходит ANN.

Эвристические и детерминированные методы оптимизации широко применяются для обучения искусственных нейронных сетей. Оба эти метода имеют свои преимущества и недостатки. Эвристические методы стохастической оптимизации, такие, как генетический алгоритм, выполняют глобальный поиск, но имеют медленную скорость конвергенции вблизи глобального оптимума. Детерминированные методы (например, градиентный спуск) демонстрируют быструю скорость сходимости вокруг глобального оптимума, но могут отставать в локальном оптимуме. Предложен алгоритм гибридного обучения, сочетающий генетический алгоритм (GA) с градиентным спуском (GD), названный HGAGD [49]. Новый алгоритм сочетает в себе глобальную способность исследования GA с точной локальной эксплуатационной способностью GD для достижения более быстрой конвергенции, а также лучшей точности конечного решения. Описано применение HGAGD в качестве нового метода обучения для оптимизации параметров нейронной сети с квантовым введением (QINN) для двух разных приложений [49]. Во-первых, при решении задач аппроксимации функций выбираются две контрольные функции для демонстрации потенциала предлагаемого QINN с алгоритмом HGAGD; во-вторых, изучается эффективность предлагаемого метода в прогнозировании временных рядов Маккея-Гласса и аттрактора Лоренца. Результаты этих исследований показывают преимущество предлагаемого подхода по сравнению с традиционными подходами. Те же авторы в работе [50] описывают возможность применения аналогичного метода для проектирования непрямого адаптивного контроллера для затухания низкочастотных колебаний в энергетических системах. Результаты этих исследований показывают, что предлагаемый контроллер, обученный HGAGD, способен достичь эффективных характеристик управления.

Оценена эффективность кубитной нейронной сети (QNN) посредством предсказания известного аттрактора Лоренца, который создает хаотичные временные ряды тремя динамическими системами [51]. Экспериментально установлено, что QNN способна более точно прогнозировать временные ряды по сравнению с обычными (реальными) нейронными сетями.

Классические автокодеры – нейронные сети, которые могут изучать эффективные низкоразмерные представления данных в пространстве с более высоким пространством и позволяют применять обучение без учителя при использовании метода обратного распространения ошибки. Задача автокодера – задавать вход X для отображения X в более низкую размерную точку Y, так что X, скорее всего, будет восстановлен из Y. Структуру базовой сети автокодера можно выбирать для представления данных меньшего размера, эффективно сжимающих входные данные. Представлена модель квантового автокодера для выполнения подобных задач по квантовым данным [52]. Квантовый автокодер обучен сжимать определенный набор данных квантовых состояний, где классический алгоритм сжатия не может быть использован. Параметры квантового автокодера обучаются с использованием классических алгоритмов оптимизации. Приведен пример простой про-

граммируемой схемы, которую обучают в контексте квантового моделирования как эффективный автокодер для сжатия основных состояний модели Хаббарда и молекулярных гамильтонианов.

Квантовое машинное обучение отвечает за исследование и разработку методов машинного обучения, способных эффективно задействовать параллелизм квантовых компьютеров. Наиболее важные задачи квантового машинного обучения, такие, как распознавание изображений, распознавание речи, оптимизация стратегий, обсуждаются в [53]. Идеи улучшения классических алгоритмов машинного обучения с учетом возможностей квантовой информатики варьируются от эффективных ресурснообъемных дорогостоящих алгоритмов до перевода стохастических методов на язык квантовой теории. Обсуждаются возможные подходы, технические детали данного процесса, оценивается потенциал будущей теории квантового обучения [53].

Несмотря на прилагаемые усилия, разрыв, существующий между большинством исследовательских предложений по квантовому машинному обучению и практическими потребностями, достаточно велик. Сложные задачи машинного обучения, которые могут быть решены с помощью гибридных квантовых устройств, рассмотрены в [54]. Здесь авторы выделили также классические наборы данных с потенциальными квантовоподобными статистическими корреляциями для проблемно-ориентированных квантовых устройств. Ориентируясь на гибридные квантово-классические подходы, авторы выделяют ключевые проблемы, которые считают подходящими для реализации на гибридных квантовых устройствах. Представлена и квантово-вспомогательная машина Гельмгольца (QAHM) [54], как попытка использования гибридных квантовых устройств при обработке больших данных. QAHM использует глубокое обучение для извлечения низкоразмерного двоичного представления данных, подходящего для относительно небольших квантовых процессоров, которые могут помочь в обучении неконтролируемой генеративной модели. Хотя авторы [54] рассмотрели данный вариант на квантовом отжиге, другие квантовые платформы также могут использовать описанную гибридную квантово-классическую структуру.

Рассмотрен случай реализации контролируемого машинного обучения (классификация новых данных на основе уже классифицированных примеров обучения) на квантовой опорной векторной машине [55]. Показано, что опорная векторная машина, организующая работу оптимизированного бинарного классификатора, реализуется на квантовом компьютере со сложностью логарифмической величины векторов и количеством примеров обучения. В тех случаях, когда классические алгоритмы выборки требуют полиномиального времени, получается экспоненциальное ускорение. В основе этого алгоритма с квантовыми большими данными лежит методика экспоненциального несопоставимого матричного метода для эффективного выполнения матричной инверсии матрицы внутреннего продукта (ядра) обучающих данных. Те же авторы в [56] выполнили анализ квантовых базисных компонент. Обычный способ выявления свойств неизвестного квантового состояния, учитывая множество копий системы в этом состоянии, заключается в выполнении измерений дивергентных наблюдаемых и статистическом анализе результатов. Для нерезонансных, но низкоуровневых квантовых состояний выявление собственных векторов и соответствующих собственных значений в классической форме суперли-

нейно масштабируется с размерностью системы 3-6. Показано [56], что для построения унитарного преобразования $e^{-i\rho t}$ можно использовать несколько копий квантовой системы с матрицей плотности ρ. Это позволяет выполнить квантовый анализ главных компонент неизвестной матрицы плотности низкого ранга, выявляя в квантовой форме собственные векторы, соответствующие большим собственным значениям во времени, экспоненциально быстрее любого существующего алгоритма. Возможное применение: анализ данных, технологическая томография.

Алгоритм квантового машинного обучения для эффективного решения класса задач, закодированных в квантовоконтролируемых унитарных операциях, описан в [57]. Центральным физическим механизмом протокола является итерация квантового уравнения с запаздыванием, которое вводит обратную связь в динамике и исключает необходимость промежуточных измерений. Выполнение квантового алгоритма анализируется путем сравнения результатов, полученных при численном моделировании, с результатами классических методов машинного обучения для одной и той же задачи. Использование уравнений с задержкой по времени улучшает инструментарий поля квантового машинного обучения, что может обеспечить беспрецедентное применение в квантовых технологиях.

Рассмотрен алгоритм предсказания на квантовом компьютере, основанный на линейной регрессионной модели с оптимизацией наименьших квадратов [58]. В отличие от предшествующих решений, связанных с проблемой считывания оптимальных параметров соответствия, данный алгоритм фокусируется на задаче машинного обучения угадывания вывода, соответствующего новому вводу, приведенным примерам точек данных. Кроме того, алгоритм адаптирован для обработки несравнимых матриц данных, которые представлены приближениями низкого ранга, что значительно улучшит зависимость от его номера условия. Результат предсказания можно получить через единичное измерение и затем использовать для дальнейших процедур обработки квантовой информации. При линейном росте входных данных время выполнения алгоритма увеличивается по логарифмической зависимости.

Известна работа, посвященная квантовому обучению аппаратно-встроенным вероятностным графическим моделям [59]. Отмечено, что основные методы машинного обучения, такие, как глубокое обучение и вероятностное программирование, в значительной степени зависят от отбора проб из обычно трудноразрешимых распределений вероятностей. Возрастает интерес к потенциальным преимуществам использования технологий квантовых вычислений в качестве механизмов выборки для ускорения этих задач или повышения их эффективности. Однако на данный момент трудно оценить фактическую производительность данных алгоритмов. Редкая связь, возникающая из-за локального взаимодействия между квантовыми битами в физических аппаратных реализациях, считается самым серьезным ограничением качества построения мощных генеративных моделей без надзора в машинном обучении. Стоит отметить, что в [59] использованы методы внедрения для добавления избыточности к наборам данных, что позволило увеличить способность моделирования квантовых отжигов. Результаты проиллюстрированы графическими моделями, встроенными в аппаратные средства, в бинаризованный набор данных рукописных цифр и два набора синтетических данных в экспериментах до 940 квантовых битов. Такая модель может быть обучена без полного знания эффективных

параметров, определяющих соответствующее квантовое распределение Гиббса. Указанный подход позволяет уйти от необходимости определять эффективную температуру на каждой итерации алгоритма отжига, ускоряя обучение; также смягчается влияние шума в контрольных параметрах, делая его устойчивым к отклонениям от эталонного распределения Гиббса. Он обеспечивает возможность использования квантовых отжигов для реализации генерирующих моделей и создает подходящую основу для сопоставления этих квантовых технологий по задачам, связанным с машинным обучением.

В [60] рассмотрены марковские логические сети (MLNs), объединяющие две противоположные школы в машинном обучении и искусственном интеллекте: причинно-следственные сети, которые очень хорошо учитывают неопределенность, и логику первого порядка, которая допускает формальные выводы. MLN – это, по сути, логический шаблон первого порядка для создания сетей Маркова. Вывод в MLN является вероятностным, и его часто выполняют с помощью приблизительных методов, таких, как выборка Гиббса по методу Маркова в цепи Монте-Карло (MCMC). MLN имеет множество регулярных симметричных структур, которые разумно использовать и на уровне первого порядка, и в генерируемой сети Маркова. Различными способами проанализированы созданные графовые структуры и определено, в какой степени квантовые протоколы могут использоваться для ускорения выборки Гиббса с помощью схем подготовки и измерения состояния [60]. На основе анализа различных подходов, оценки их преимуществ, теоретических ограничений, возможностей реализации сделан также вывод, что прямое применение полученного результата приводит к экспоненциальному ускорению по сравнению с классическими эвристиками, что подтверждает их потенциальную полезность для применения в машинном обучении.

В современных моделях глубокого обучения используются высоко оптимизированные сверточные нейронные сети (CNN), обучающиеся на компьютерах с большим графическим процессором (GPU) и довольно простой многоуровневой топологией сети, то есть с высокосвязанными уровнями без внутрислойных соединений. Построение топологий сети глубокого обучения требует ручной настройки, а внедрение сети в аппаратное обеспечение является дорогостоящим как по стоимости, так и по мощности. Выполнена оценка модели глубокого обучения с использованием трех различных вычислительных архитектур для решения этих проблем [61]: квантовых вычислений для обучения сложных топологий, высокопроизводительных вычислений (HPC) для автоматического определения топологии сети и нейроморфных вычислений для маломощной аппаратной реализации. Из-за ограничений на количество вводимых данных в существующих моделях квантовых компьютеров авторы использовали для оценки набор данных MNIST. Результаты оценки показали возможность использования трех архитектур в тандеме для изучения сложных сетей глубокого обучения, которые не подлежат обработке с использованием архитектуры фон Неймана. Показано, что квантовый компьютер может находить высококачественные значения внутрислойных соединений и весов, получая при этом сдержанный результат времени по мере увеличения сложности сети; высокопроизводительный компьютер может найти оптимальные топологии на основе слоев; и нейроморфный компьютер может представлять сложную топологию и весовые коэффициенты, полученные из других архитектур в маломощном мемарном оборудовании. Полученный результат был невозможен при архитектуре фон Неймана.

Квантовые структуры в когнитивных и социальных науках. Одной из проблем социологии и психологии является определение принципов и условий, определяющих такие человеческие когнитивные акты, как принятие решений, категоризация и поведение в условиях неопределенности. Идентификация этих механизмов интересна для большинства сфер человеческой деятельности от психологии до экономики, финансов, политики, информатики и искусственного интеллекта. Преобладающая на сегодня теоретическая парадигма основывается на классической концепции логики и теории вероятностей. Согласно этой парадигме, люди принимают решения, следуя правилам булевской логики, а вероятностные аспекты принятия решений могут быть формализованы теорией вероятности Колмогорова. Подход Колмогорова обеспечивает достаточно полный и точный учет принятия решений людьми как на нормативном уровне (описывая, что люди должны делать), так и на описательном уровне (описывая, что на самом деле делают люди). Однако экспериментальные исследования концептуальной классификации, человеческого суждения и восприятия и поведенческой экономики показали, что эта классическая концепция принципиально проблематична в том смысле, что когнитивные модели, основанные на этих математических структурах, не способны охватить то, как люди принимают решения в условиях неопределенности. В последнее десятилетие возникла альтернативная научная парадигма, в которой используется более общая схема моделирования на основе математического формализма квантовой теории для моделирования ситуаций и процессов в когнитивной и социальной науке [62]. Конъюнктивные и дизъюнктивные заблуждения, эффекты дизъюнкции, нарушения принципа Sure-Thing, парадоксы Allais, Ellsberg и Machina являются лишь некоторыми из примеров, когда применение квантовомеханического формализма показывает значительно большую эффективность по сравнению с традиционными схемами моделирования классического типа.

Обзор текущих исследований, в которых применяется формализм квантовой теории в когнитивных и социально-экономических областях, выполнен в [62]. Цель данных исследований – не изучить микрофизические процессы, происходящие в человеческом мозге, и затем управлять суждениями человека, а рассмотреть квантовую теорию как общую, когерентную и унитарную парадигму человеческого познания. В этом отношении важен обзор [62] исследований аксиоматических и операционных основ квантовой физики, основанных на теории, а не на экспериментах; хотя иногда допускается использование эмпирических данных. Модели построены по общим эпистемологическим и техническим ограничениям квантовой теории; следовательно, успех этого моделирования на основе квантовой теории предполагает, что он может обеспечить общую теорию человеческого познания. Исследования идут по трем направлениям:

- определение причин, лежащих в основе успеха квантовой парадигмы в когнитивной и социально-экономической областях;
- идентификация эмпирических ситуаций, когда квантовый формализм дает преимущества по сравнению с традиционными схемами моделирования и появляются новые подлинные квантовые структуры;
- распространение квантовой парадигмы на новые сферы человеческой деятельности.

Анализ результатов когнитивного теста на конъюнкции и отрицание естественных

понятий [63] показал, что квантово-теоретическая вероятностная модель в гильбертовом пространстве достоверно представляет собранные данные, противоречащие теоретико-множественной колмогоровской модели. Этот результат объясняется предположением о существовании двух типов рассуждений в человеческом познании: доминирующих возникающих рассуждений и вторичных логических рассуждений. Некоторые математические аспекты этой квантово-теоретической модели концептуальных союзов и отрицаний развиваются в [64] путем введения унитарных операторов в гильбертовом пространстве. Исследования показали [63], что квантово-теоретический подход может служить обобщением теории прототипов E. Rosch, в которой признается зависимость прототипа от контекста.

В работе [63], в которой моделируется принятие решений людьми, исследовано взаимное влияние концептуальной конъюнктуры и отрицания путем измерения весомости членов списка экземпляров в отношении двух понятий. Выявлены систематические отклонения от классической (нечеткой) логики и теории вероятностей. Полученные результаты дают еще более весомое доказательство обоснованности квантово-теоретической основы для сочетания двух понятий. Представление концептуального отрицания, естественно, вытекает из общих предположений нашей двухсекторной пространственной модели Фока, и это представление верно согласуется с экспериментальными данными. Обнаружено новое значительное и априорно неожиданное отклонение от классики, и его можно точно объяснить, полагая, что человеческое мышление является суперпозицией «возникающего рассуждения» и «логического рассуждения» и что эти два процесса представлены в пространственной алгебраической структуре Фока.

Человеческое восприятие является объектом исследования в [65], где развивается квантовая модель динамики восприятия, иллюстрируемая с помощью модели бистабильного восприятия конкретной двусмысленной фигуры, лестницы Шредера.

Выполнена проверка возможности применения статистической модели, полученной из физики конденсированных сред, для восстановления структуры социальной сети [66]. Обратная модель Поттса, традиционно применяемая для рекурсивных наблюдений квантовых состояний в ансамбле частиц, здесь обращена к наблюдениям состояний членов в организации и их (анти)корреляциям, тем самым выводя взаимодействия в качестве связей между членами. Решение обратной задачи на основе LBP применено в первый раз для восстановления общей структуры графа, т. е. впервые в области социальных наук применена модель Q-состояния (вместо модели Изинга) для вывода структуры реальной сети. Рассмотрена роль разнообразных вариантов моделирования и конкретных параметров с целью выяснения вопроса, как максимальное значение Q-разрешения моделью Потса может привести к существенным различиям результатов, наряду с априорными знаниями о структуре сети.

На основе обобщения и анализа литературных данных можно сделать вывод, что квантовые структуры систематически присутствуют в объектах и предметах исследования когнитивной и социальной науки и что квантово-подобные модели более эффективны, чем традиционные теоретико-множественные модели вероятности.

Заключение

Квантовая информатика – новый раздел науки, посвященный использованию квантовых объектов для обработки и передачи информации. Сегодня в разработку квантового компьютера инвестируется много усилий и средств. По всему миру идет работа по созданию квантовых элементов, проектированию квантовых алгоритмов и разработке архитектуры квантового компьютера.

Определены перспективные направления применения квантовой информатики:

- моделирование сложных естественных и искусственных явлений и процессов, одним из которых является сам квантовый компьютер;
- квантовая криптография, методы передачи которой гарантируют невозможность расшифровки сообщения;
- квантовые нейронные сети и машинное обучение позиционируется как путь к созданию квантового интеллекта;
- применение квантовых вычислений в когнитивных и социальных науках дает возможность исследовать механизм принятия решений при неполных данных.

Литература:

1. Доклад экспертной группы Digital McKinsey «Цифровая Россия: новая реальность». 2017. 122 с. URL: http://www.mckinsey.com/global-locations/europe-andmiddleeast/russia/ru/our-work/mckinsey-digital (Дата обращения 15.01.2019).

2. Программа «Цифровая экономика Российской Федерации», утвержденная Распоряжением № 1632-р Правительства Российской Федерации от 28 июля 2017 г.

3. Программа «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», утвержденная Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

4. Mohseni M., Read P., Neven H., Boixo S., Denchev V., Babbush R., Fowler A., Smelyanskiy V., Martinis J. Commercialize quantum technologies in five years // Nature. 2017. V. 543. Iss. 7644. P. 171–174. DOI: 10.1038/543171a

5. Гренштейн С. Новое исследование Ассоциации полупроводниковой промышленности: «Через 5 лет закон Мура перестанет действовать». URL: https://habr.com/post/307158/

6. Levchaev P.A. The digital economy as the future of our lives // Russian Journal of Management. 2017. V. 5. № 4. P. 515–523. URL: https://doi.org/10.29039/article_5a5df35550f2d6.65514969

7. Карасев С. Глава Intel: об отношениях с Apple, законе Мура, новых устройствах и материалах // Электронное СМИ «3ДНьюс». URL: https://3dnews.ru/about (Дата обращения 15.01.2019).

8. Humble T. Consumer applications of quantum computing: A promising approach for secure computation, trusted data storage, and efficient applications // IEEE Consumer Electronics Magazine. 2018. V. 7. Iss. 6. P. 8–14. DOI:10.1109/MCE.2017.2755298

9. Кулик С.Д., Берков А.В., Яковлев В.П. Введение в теорию квантовых вычислений (методы квантовой механики в кибернетике): уч. пособие в 2-х кн. Книга 1. М.: МИФИ, 2008. 212 с.

10. Квантовые вычисления для любопытных. URL: https://cloudcoin.ru/quantum-

computing (Дата обращения 15.01.2019).

11. Квантовый компьютер и квантовая связь. URL: http://www.tadviser.ru/index.php (Дата обращения 15.01.2019).

12. Фонд перспективных исследований. URL: https://fpi.gov.ru/press/media/jekspert_mnogokubitniy_kvantoviy_kompyyuter_mozhno_sozdaty_v_rossii_za_god (Дата обращения 15.01.2019).

13. Debnath S., Linke N.M., Figgatt C., Landsman K.A., Wrigh, K., Monroe C. Demonstration of a small programmable quantum computer with atomic qubits // Nature. 2016. V. 536. Iss. 7614. P. 63–66. DOI: 10.1038/nature18648

14. Linke N.M., Maslov D., Roetteler M., Debnath S., Figgatt C., Landsma, K.A., Wright K., Monroe C. Experimental comparison of two quantum computing architectures // Proc. Natl. Acad. Sci. U.S.A. 2017. V. 114. Iss. 13. P. 3305–3310. DOI: 10.1073/pnas.1618020114

15. Britt K.A., Humble T.S. High-performance computing with quantum processing units // ACM Journal. Emerging Technologies in Computing Systems. 2017. V. 13. Iss. 3. Article No. 39. DOI: 10.1145/3007651

16. Сапаев Д., Булычков Д. Квантовые вычисления против классических: зачем нам столько цифр. URL: https://habr.com/company/sberbank/blog/343308/ (Дата обращения 15.01.2019).

17. Сапаев Д., Булычков Д. Квантовые вычисления: отжиг с выключателями и прочее веселье. URL: https://habr.com/company/sberbank/blog/344830/ (Дата обращения 15.01.2019).

18. Список квантовых алгоритмов. URL: https://math.nist.gov/quantum/zoo/ (Дата обращения 15.01.2019).

19. Dumas J.P., Soni K., Rasool A. An introduction to quantum search algorithm and its implementation // In: Balas V., Sharma N., Chakrabarti A. (eds) Data Management, Analytics and Innovation // Advances in Intelligent Systems and Computing. 2019. V. 808. P. 19–31. Springer, Singapore. DOI: 10.1007/978-981-13-1402-5_2

20. Wang G. Quantum algorithm for linear regression // Phys. Rev. A. 2017. V. 96. Iss. 1. Article No. 012335. DOI: 10.1103/PhysRevA.96.012335

21. Kliuchnikov V., Maslov D., Mosc, M. Practical approximation of single-qubit unitaries by single-qubit quantum Clifford and T circuits // IEEE Trans. Comp. 2016. V. 65. Iss. 1. P. 161–172. Article No. 7056491. DOI: 10.1109/TC.2015.2409842

22. Selinger P. Efficient Clifford+T approximation of single-qubit operators // Quantum Information and Computation. 2014. V. 15. Iss. 1-2. P. 159–180.

23. Bocharov A., Roetteler M., Svore K.M. Efficient synthesis of probabilistic quantum circuits with fallback // Phys. Rev. A. Atomic, Molecular, and Optical Physics. 2015. V. 91. Iss. 5. Article No. 052317. DOI: 10.1103/PhysRevA.91.052317

24. Palsson M.S., Gu M., Ho J., Wiseman H.M., Pryde G.J. Experimentally modeling stochastic processes with less memory by the use of a quantum processor // Science Advances. 2017. V. 3. Iss. 2. Article No. e1601302. DOI: 10.1126/sciadv.1601302

25. Столяров А. Квантовые вычисления и умные пространства могут изменить рынок СХД. URL: http://safe.cnews.ru/news/top/2018-11-14_kvantovye_vychisleniya_i_umnye_prostranstva_mogut (Дата обращения 15.01.2019).

26. Fitzsimons J.F., Kashefi E. Unconditionally verifiable blind quantum computation // Phys. Rev. A. 2017. V. 96. Iss. 1. Article No. 012303. DOI: 10.1103/PhysRevA.96.012303

27. Roetteler M., Svore K.M. Quantum computing: Codebreaking and beyond // IEEE Security and Privacy. 2018. V. 16. Iss. 5. P. 22–36. Article No. 8490171. DOI: 10.1109/MSP.2018.3761710

28. Pirandola S., Ottavian, C., Spedalieri G., Weedbroo C., Braunstein S.L, Lloy S., Gehring T., Jacobsen C.S., Andersen U.L. High-rate measurement-device-independent quantum cryptography // Nature Photonics. 2015. V. 9. Iss. 6. P. 397–402. DOI: 10.1038/nphoton.2015.83

29. Grassl M., Langenberg B., Roetteler M., Steinwandt R. Applying Grover's algorithm to AES: Quantum resource estimates // Lecture Notes in Computer Science. 2016. V. 9606. P. 29–43. 7th Int. Workshop on Post-Quantum Cryptography, PQ Crypto 2016; Fukuoka; Japan; February 24–26, 2016; code 164489. DOI: 10.1007/978-3-319-29360-8_3

30. Roetteler M., Steinwandt R. A note on quantum related-key attacks // Information Processing Lett. 2015. V. 115. Iss. 1. P. 40–44. DOI: 10.1016/j.ipl.2014.08.009

31. Walenta N., Burg A., Caselunghe D., Constantin J., Gisin N., Guinnard O., Houlmann R., Junod P., Korzh B., Kulesza N., Legré M., Lim C.W., Lunghi T., Monat L., Portmann C., Soucarros M., Thew R.T., Trinkler P., Trolliet G., Vannel F., Zbinden H. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing // New Journal of Physics. 2014. V. 16. Article No. 013047. DOI: 10.1088/1367-2630/16/1/013047

32. Shibata H., Honjo T., Shimizu K. Quantum key distribution over a 72 dB channel loss using ultralow dark count superconducting single-photon detectors // Optics Lett. 2014. V. 39. Iss. 17. P. 5078–5081. DOI: 10.1364/OL.39.005078

33. Xu F., Xu H., Lo H.-K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution // Phys. Rev. A. Atomic, Molecular, and Optical Physics. 2014. V. 89. Iss. 5. Article No. 052333. DOI: 10.1103/PhysRevA.89.052333

34. Curty M., Xu F., Cui W., Lim C.C.W., Tamaki K., Lo H.-K. Finite-key analysis for measurement-device-independent quantum key distribution // Nature Commun. 2014. V. 5. Article No. 3732. DOI: 10.1038/ncomms4732

35. Tang Z., Liao Z., Xu F., Qi B., Qian L., Lo H.-K. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution // Phys. Rev. Lett. 2014. V. 112. Iss. 19. Article No. 190503. DOI: 10.1103/PhysRevLett.112.190503

36. Yu Z.-W., Zhou Y.-H., Wang X.-B. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method // Phys. Rev. A. Atomic, Molecular, and Optical Physics. 2015. V. 91. Iss. 3. Article No. 032318. DOI: 10.1103/PhysRevA.91.032318

37. Wang C., Song X.-T., Yin Z.-Q., Wang S., Chen W., Zhang C.-M., Guo G.-C., Han Z.-F. Phase-reference-free experiment of measurement-device-independent quantum key distribution // Phys. Rev. Lett. 2015. V. 115. Iss. 16. Article No. 160502. DOI: 10.1103/PhysRevLett.115.160502

38. Comandar L.C., Lucamarini M., Fröhlich B., Dynes J.F., Sharpe A.W., Tam S.W.-B., Yuan Z.L., Penty R.V., Shields A.J. Quantum key distribution without detector vulnerabilities using optically seeded lasers // Nature Photonics. 2016. V. 10. Iss. 5. P. 312–315. DOI: 10.1038/nphoton.2016.50

39. Yin H.-L., Chen T.-Y., Yu Z.-W., Liu H., You L.-X., Zhou Y.-H., Chen S.-J., Mao Y.,

Huang M.-Q., Zhang W.-J., Chen H., Li M.J., Nolan D., Zhou F., Jiang X., Wang Z., Zhang Q., Wang X.-B., Pan J.-W. Measurement-device-independent quantum key distribution over a 404 km optical fiber // Phys. Rev. Lett. 2016. V. 117. Iss. 19. Article No. 190501. DOI: 10.1103/PhysRevLett.117.190501

40. Chen D., Wei L., YaLiang C., Qing P., Lei S. Reference-frame-independent measurement-device-independent quantum key distribution using hybrid logical basis // Quantum Information Processing. 2018. V. 17. Iss. 10. Article No. 256. DOI: 10.1007/s11128-018-2030-7

41. Musser G. Job one for quantum computers: Boost artificial intelligence. // Quanta Magazine. URL: https://www.quantamagazine.org/job-one-for-quantum-computers-boost-artificial-intelligence-20180129/ (Дата обращения 15.01.2019).

42. Алтайский М.В., Капустина Н.Е., Крылов В.А. Квантовые нейронные сети: современное состояние и перспективы развития // Физика элементарных частиц и атомного ядра. 2014. Т. 45. Вып. 5-6. С. 1825–1856.

43. Haykin S. Neural Networks. Pearson Education. NY: IEEE, 1999. 600 p.

44. Schuld M., Sinayskiy I., Petruccione F. The quest for a quantum neural network // Quantum Information Processing. 2014. V. 13. Iss. 11. P. 2567–2586. DOI: 10.1007/s11128-014-0809-8

45. Qi F., Chen C. Qubit neural tree network with applications in nonlinear system modeling // IEEE Access. 2018. V. 6. P. 51598–51606. Article No. 8463464. DOI: 10.1109/ACCESS.2018.2869894

46. da Silva A.J., Ludermir T.B., de Oliveira W.R. Quantum perceptron over a field and neural network architecture selection in a quantum computer // Neural Networks. 2016. V. 76. P. 55–64. DOI: 10.1016/j.neunet.2016.01.002

47. Lv F., Yang G., Yang W., Zhang X., Li K. The convergence and termination criterion of quantum-inspired evolutionary neural networks // Neurocomputing. 2017. V. 238. P. 157–167. DOI: 10.1016/j.neucom.2017.01.048

48. Panchi L.I., Zhao Y. Model and algorithm of sequence-based quantum-inspired neural networks // Chinese Journal of Electronics. 2018. V. 27. Iss. 1. P. 9–18. DOI: 10.1049/cje.2017.11.007

49. Ganjefar S., Tofighi M. Optimization of quantum-inspired neural network using memetic algorithm for function approximation and chaotic time series prediction // Neurocomputing. 2018. V. 291. P. 175–186. DOI: 10.1016/j.neucom.2018.02.074

50. Ganjefar S., Tofighi M. Training qubit neural network with hybrid genetic algorithm and gradient descent for indirect adaptive controller design // Engineering Applications of Artificial Intelligence. 2017. V. 65. P. 346–360. DOI: 10.1016/j.engappai.2017.08.007

51. Ueguchi T., Matsui N., Isokawa T. Chaotic time series prediction by qubit neural network with complex-valued representation // 2016 55th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE). Tsukuba; Japan; September 20-23, 2016. Article No. 7749232. P. 1353–1358. DOI: 10.1109/SICE.2016.7749232

52. Romero J., Olson, J.P., Aspuru-Guzik A. Quantum autoencoders for efficient compression of quantum data // Quantum Science and Technology. 2017. V. 2. Iss. 4. Article No. 045001. DOI: 10.1088/2058-9565/aa8072

53. Schuld M., Sinayskiy I., Petruccione F. An introduction to quantum machine learning //

Contemporary Physics. 2015. V. 56. Iss. 2. P. 172–185. DOI: 10.1080/00107514.2014.964942

54. Perdomo-Ortiz A., Benedetti M., Realpe-Gómez J., Biswas R. Opportunities and challenges for quantum-assisted machine learning in near-term quantum computers // Quantum Science and Technology. 2018. V. 3. Iss. 3. Article No. 030502. DOI: 10.1088/2058-9565/aab859

55. Rebentrost P., Mohseni M., Lloyd S. Quantum support vector machine for big data classification // Phys. Rev. Lett. 2014. V. 113. Iss. 3. Article No. 130503. DOI: 10.1103/PhysRevLett.113.130503

56. Lloyd S., Mohseni M., Rebentrost P. Quantum principal component analysis // Nature Physics. 2014. V. 10. Iss. 9. P. 631–633. DOI: 10.1038/NPHYS3029

57. Alvarez-Rodriguez U., Lamata L., Escandell-Montero P., Martín-Guerrero J.D., Solano E. Supervised quantum learning without measurements // Scientific Reports. 2017. V. 7. Iss. 1. Article No. 13645. DOI: 10.1038/s41598-017-13378-0

58. Schuld M., Sinayskiy I., Petruccione F. Prediction by linear regression on a quantum computer // Phys. Rev. A. 2016. V. 94. Iss. 2. Article No. 022342. DOI: 10.1103/PhysRevA.94.022342

59. Benedetti M., Realpe-Gómez J., Biswas R., Perdomo-Ortiz A. Quantum-assisted learning of hardware-embedded probabilistic graphical models // Phys. Rev. X. 2017. V. 7. Iss. 4. Article No. 041052. DOI: 10.1103/PhysRevX.7.041052

60. Wittek P., Gogolin C. Quantum enhanced inference in Markov logic networks // Scientific Reports. 2017. V. 7. Article No. 45672. DOI: 10.1038/srep45672

61. Potok T.E., Schuman C.D., Young S.R., Patton R.M., Spedalieri F., Liu J., Yao K.-T., Rose G., Chakma G. A study of complex deep learning networks on high performance, neuromorphic, and quantum computers // 2016 2nd Workshop on Machine Learning in HPC Environments (MLHPC). Salt Lake City, Utah, USA, 2016. P. 47–55. DOI: 10.1109/MLHPC.2016.009

62. Aerts D., Broekaert J., Gabora L., Sozzo S. Quantum structures in cognitive and social science (Editorial) // Front. Psychol. 2016. V. 7. Iss. APR. Article No. 577. DOI: 10.3389/fpsyg.2016.00577

63. Aerts D., Sozzo S., Veloz T. Quantum structure of negation and conjunction in human thought // Front. Psychol. 2015. V. 6. Article No. 1447. DOI: 10.3389/fpsyg.2015.01447

64. Aerts D., Sozzo S. Quantum entanglement in conceptual combinations // Int. J. Theor. Phys. 2014. V. 53. P. 3587–3603. DOI: 10.1007/s10773-013-1946-z

65. Khrennikov A. Quantum-like model of unconscious–conscious dynamics // Front. Psychol. 2015. V. 6. Article No. 997. DOI: 10.3389/fpsyg.2015.00997

66. Bisconti C., Corallo A., Fortunato L., Gentile A.A., Massafra A., Pellè P. Reconstruction of a real world social network using the Potts model and loopy belief propagation // Front. Psychol. 2015. V. 6. Article No. 1698. DOI: 10.3389/fpsyg.2015.01698

References:

1. The report of the Digital McKinsey expert group “Digital Russia: a new reality”. 2017. 122 p. URL: http://www.mckinsey.com/global-locations/europe-andmiddleeast/russia/ru/our-work/mckinsey-digital (Access date 01/15/2019). (in Russ.)

2. The program “Digital economy of the Russian Federation”, approved by Decree No. 1632-p of the Government of the Russian Federation of July 28, 2017. (in Russ.)

3. The program “On the strategy for the information society development in the Russian Federation for 2017-2030”, approved by the Decree of the President of the Russian Federation dated May 9, 2017. No. 203. (in Russ.)

4. Mohseni M., Read P., Neven H., Boixo S., Denchev V., Babbush R., Fowler A., Smelyanskiy V., Martinis J. Commercialize quantum technologies in five years. *Nature.* 2017; 543(7644): 171-174. DOI: 10.1038/543171a

5. Grenshtein S. A new study by the Association of the semiconductor industry: "After 5 years, Moore's law will cease to operate". URL: https://habr.com/post/307158/ (Access date 01/15/2019) (in Russ.)

6. Levchaev P.A. The digital economy as the future of our lives. *Russian Journal of Management.* 2017; 5(4): 515-523. URL: https://doi.org/10.29039/article_5a5df35550f2d6.65514969

7. Karasev S. Head of Intel: On relations with Apple, Moore's law, new devices and materials. *Electronic media "3DNews".* URL: https://3dnews.ru/about (Access date 01/15/2019). (in Russ.)

8. Humble T. Consumer applications of quantum computing: A promising approach for secure computation, trusted data storage, and efficient applications. *IEEE Consumer Electronics Magazine.* 2018; 7(6): 8-14. DOI: 10.1109/MCE.2017.2755298

9. Kulik S.D., Berkov A.V., Yakovlev V.P. Introduction to the theory of quantum computation (methods of quantum mechanics in cybernetics): in 2 books. Book 1. Moscow: MEPhI Publ., 2008. 212 p. (in Russ.)

10. Quantum computing for the curious. URL: https://cloudcoin.ru/quantum-computing (Access date 01/15/2019). (in Russ.)

11. Quantum computer and quantum communication. URL: http://www.tadviser.ru/index.php (Access date 01/15/2019). (in Russ.)

12. Foundation for Advanced Studies. URL: https://fpi.gov.ru/press/media/jekspert_mnogokubitniy_kvantoviy_kompyyuter_mozhno_sozdaty_v_rossii_za_god (Access date 01/15/2019). (in Russ.)

13. Debnath S., Linke N.M., Figgatt C., Landsman K.A., Wright K., Monroe C. Demonstration of a small programmable quantum computer with atomic qubits. *Nature.* 2016; 536(7614): 63-66. DOI: 10.1038/nature18648

14. Linke N.M., Maslov D., Roetteler M., Debnath S., Figgatt C., Landsman K.A., Wright K., Monroe C. Experimental comparison of two quantum computing architectures. *Proc. Natl. Acad. Sci. U.S.A.* 2017; 114(13): 3305-3310. DOI: 10.1073/pnas.1618020114

15. Britt K.A., Humble T.S. High-performance computing with quantum processing units. *ACM Journal on Emerging Technologies in Computing Systems.* 2017; 13(3): Article No. 39. DOI: 10.1145/3007651

16. Sapaev D., Bulychkov D. Quantum computing versus classical: Why do we need so many digits. URL: https://habr.com/company/sberbank/blog/343308/ (Access date 01/15/2019). (in Russ.)

17. Sapaev D., Bulychkov D. Quantum calculations: Annealing with switches and other fun. URL: https://habr.com/company/sberbank/blog/344830/ (Access date 01/15/2019) (in Russ.)

18. List of quantum algorithms. URL: https://math.nist.gov/quantum/zoo/ (Access date 01/15/2019). (in Russ.)

19. Dumas J.P., Soni K., Rasool A. An introduction to quantum search algorithm and its implementation. In: Balas V., Sharma N., Chakrabarti A. (eds) Data Management, Analytics and Innovation. *Advances in Intelligent Systems and Computing.* 2019; 808: 19-31. Springer, Singapore. DOI: 10.1007/978-981-13-1402-5_2

20. Wang G. Quantum algorithm for linear regression. *Phys. Rev. A.* 2017; 96(1): Article No. 012335. DOI: 10.1103/PhysRevA.96.012335

21. Kliuchnikov V., Maslov D., Mosca M. Practical approximation of single-qubit unitaries by single-qubit quantum Clifford and T circuits. *IEEE Trans. Comp.* 2016; 65(1): 161-172. Article No. 7056491. DOI: 10.1109/TC.2015.2409842

22. Selinger P. Efficient Clifford+T approximation of single-qubit operators. *Quantum Information and Computation.* 2014; 15(1-2): 159-180.

23. Bocharov,A., Roetteler M., Svore K.M. Efficient synthesis of probabilistic quantum circuits with fallback. *Phys. Rev. A. Atomic, Molecular, and Optical Physics.* 2015; 91(5): Article No. 052317. DOI: 10.1103/PhysRevA.91.052317

24. Palsson M.S., Gu, M., Ho J., Wiseman H.M., Pryde G.J. Experimentally modeling stochastic processes with less memory by the use of a quantum processor. *Science Advances.* 2017; 3(2): Article No. e1601302. DOI: 10.1126/sciadv.1601302

25. Stolyarov A. Quantum computing and smart spaces can change the storage market. URL: http://safe.cnews.ru/news/top/2018-11-14_kvantovye_vychisleniya_i_umnye_prostranstva_mogut (Access date 01/15/2019). (in Russ.)

26. Fitzsimons J.F., Kashefi E. Unconditionally verifiable blind quantum computation. *Phys. Rev. A.* 2017; 96(1): Article No. 012303. DOI: 10.1103/PhysRevA.96.012303

27. Roetteler M., Svore K.M. Quantum computing: Codebreaking and beyond. *IEEE Security and Privacy.* 2018; 16(5): 22-36. Article No. 8490171. DOI: 10.1109/MSP.2018.3761710

28. Pirandola S., Ottaviani C., Spedalieri G., Weedbrook C., Braunstein S.L, Lloyd S., Gehring T., Jacobsen C.S., Andersen U.L. High-rate measurement-device-independent quantum cryptography. *Nature Photonics.* 2015; 9(6): 397-402. DOI: 10.1038/nphoton.2015.83

29. Grassl M., Langenberg B., Roetteler M., Steinwandt R. Applying Grover's algorithm to AES: Quantum resource estimates. *Lecture Notes in Computer Science.* 2016; 9606: 29-43. 7th Int. Workshop on Post-Quantum Cryptography, PQ Crypto 2016; Fukuoka; Japan; February 24-26, 2016; code 164489. DOI: 10.1007/978-3-319-29360-8_3

30. Roetteler M., Steinwandt R. A note on quantum related-key attacks. *Information Processing Lett.* 2015; 115(1): 40-44. DOI: 10.1016/j.ipl.2014.08.009

31. Walenta N., Burg, A., Caselunghe D., Constantin J., Gisin N., Guinnard O., Houlmann R., Junod, P., Korzh B., Kulesz, N., Legré M., Lim C.W., Lunghi T., Monat L., Portmann C., Soucarros M., Thew R.T., Trinkler P., Trolliet G., Vannel F., Zbinden H. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New Journal of Physics.* 2014; 16: Article No. 013047. DOI: 10.1088/1367-2630/16/1/013047

32. Shibata H., Honjo T., Shimizu K. Quantum key distribution over a 72 dB channel loss using ultralow dark count superconducting single-photon detectors. *Optics Lett.* 2014; 39(17): 5078-5081. DOI: 10.1364/OL.39.005078

33. Xu F., Xu H., Lo H.-K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Phys. Rev. A. Atomic, Molecular,*

and Optical Physics. 2014; 89(5): Article No. 052333. DOI: 10.1103/PhysRevA.89.052333

34. Curty M., Xu F., Cui W., Lim C.C.W., Tamaki K., Lo H.-K. Finite-key analysis for measurement-device-independent quantum key distribution. *Nature Commun.* 2014; 5: Article No. 3732. DOI: 10.1038/ncomms4732

35. Tang Z., Liao Z., Xu F., Qi B., Qian L., Lo H.-K. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* 2014; 112(19): Article No. 190503. DOI: 10.1103/PhysRevLett.112.190503

36. Yu Z.-W., Zhou Y.-H., Wang X.-B. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method. *Phys. Rev. A. Atomic, Molecular, and Optical Physics.* 2015; 91(3): Article No. 032318. DOI: 10.1103/PhysRevA.91.032318

37. Wang C., Song X.-T., Yin Z.-Q., Wang S., Chen W., Zhang C.-M., Guo G.-C., Han Z.-F. Phase-reference-free experiment of measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* 2015; 115(16): Article No. 160502. DOI: 10.1103/PhysRevLett.115.160502

38. Comandar L.C., Lucamarini M., Fröhlich B., Dynes J.F., Sharpe A.W., Tam S.W.-B., Yuan Z.L., Penty R.V., Shields A.J. Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nature Photonics.* 2016; 10(5): 312-315. DOI: 10.1038/nphoton.2016.50

39. Yin H.-L., Chen T.-Y., Yu Z.-W., Liu H., You L.-X., Zhou Y.-H., Chen S.-J., Mao Y., Huang M.-Q., Zhang W.-J., Chen H., Li M.J., Nolan D., Zhou, F., Jiang X., Wang Z., Zhang Q., Wan X.-B., Pan J.-W. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* 2016; 117(19): Article No. 190501. DOI: 10.1103/PhysRevLett.117.190501

40. Chen D., Wei L., YaLiang C., Qing P., Lei S. Reference-frame-independent measurement-device-independent quantum key distribution using hybrid logical basis. *Quantum Information Processing.* 2018; 17(10): Article No. 256. DOI: 10.1007/s11128-018-2030-7

41. Musser G. Job one for quantum computers: Boost artificial intelligence. *Quanta Magazine.* URL: https://www.quantamagazine.org/job-one-for-quantum-computers-boost-artificial-intelligence-20180129/ (Access date 01/15/2019).

42. Altayskiy M.V., Kapustina N.E., Krylov V.A. Quantum neural networks: Current state and development prospects. *Fizika elementarnykh chastits i atomnogo yadra* (Physics of Elementary Particles and Atomic Nucleus). 2014; 45(5-6): 1825-1856. (in Russ.)

43. Haykin S. Neural Networks. Pearson Education. NY: IEEE, 1999. 600 p.

44. Schuld M., Sinayskiy I., Petruccione F. The quest for a quantum neural network. *Quantum Information Processing.* 2014; 13(11): 2567-2586. DOI: 10.1007/s11128-014-0809-8

45. Qi F., Chen C. Qubit neural tree network with applications in nonlinear system modeling. *IEEE Access.* 2018; 6: 51598-51606. Article No. 8463464. DOI: 10.1109/ACCESS.2018.2869894

46. da Silva A.J., Ludermir T.B., de Oliveira W.R. Quantum perceptron over a field and neural network architecture selection in a quantum computer. *Neural Networks*, 2016; 76: 55-64. DOI: 10.1016/j.neunet.2016.01.002

47. Lv F., Yang G., Yang W., Zhang X., Li K. The convergence and termination criterion of quantum-inspired evolutionary neural networks. *Neurocomputing.* 2017; 238: 157-167.

DOI: 10.1016/j.neucom.2017.01.048

48. Panchi L.I., Zhao Y. Model and algorithm of sequence-based quantum-inspired neural networks. *Chinese Journal of Electronics*. 2018; 27(1): 9-18. DOI: 10.1049/cje.2017.11.007

49. Ganjefar S., Tofighi M. Optimization of quantum-inspired neural network using memetic algorithm for function approximation and chaotic time series prediction. *Neurocomputing.* 2018; 291: 175-186. DOI: 10.1016/j.neucom.2018.02.074

50. Ganjefar S., Tofighi M. Training qubit neural network with hybrid genetic algorithm and gradient descent for indirect adaptive controller design. *Engineering Applications of Artificial Intelligence.* 2017; 65(10): 346-360. DOI: 10.1016/j.engappai.2017.08.007

51. Ueguchi T., Matsui N., Isokawa T. Chaotic time series prediction by qubit neural network with complex-valued representation. 2016 *55th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE).* Tsukuba; Japan; September 20-23, 2016. Article No. 7749232. P. 1353–1358. DOI: 10.1109/SICE.2016.7749232

52. Romero J., Olson J.P., Aspuru-Guzik A. Quantum autoencoders for efficient compression of quantum data. *Quantum Science and Technology.* 2017; 2(4): Article No. 045001. DOI: 10.1088/2058-9565/aa8072

53. Schuld M., Sinayskiy I., Petruccione F. An introduction to quantum machine learning. *Contemporary Physics.* 2015; 56(2): 172-185. DOI: 10.1080/00107514.2014.964942

54. Perdomo-Ortiz A., Benedetti M., Realpe-Gómez J., Biswas R. Opportunities and challenges for quantum-assisted machine learning in near-term quantum computers. *Quantum Science and Technology.* 2018; 3(3): Article No. 030502. DOI: 10.1088/2058-9565/aab859

55. Rebentrost P., Mohseni M., Lloyd S. Quantum support vector machine for big data classification. *Phys. Rev. Lett.* 2014; 113(3): Article No. 130503. DOI: 10.1103/PhysRevLett.113.130503/

56. Lloyd S., Mohseni M., Rebentrost P. Quantum principal component analysis. *Nature Physics.* 2014; 10(9): 631-633. DOI: 10.1.038/NPHYS3029

57. Alvarez-Rodriguez U., Lamata L., Escandell-Montero P., Martín-Guerrero J.D., Solano E. Supervised quantum learning without measurements. *Scientific Reports.* 2017; 7(1): Article No. 13645. DOI: 10.1038/s41598-017-13378-0

58. Schuld M., Sinayskiy I., Petruccione F. Prediction by linear regression on a quantum computer. *Phys. Rev. A.* 2016; 94(2): Article No. 022342. DOI: 10.1103/PhysRevA.94.022342

59. Benedetti M., Realpe-Gómez J., Biswas R., Perdomo-Ortiz A. Quantum-assisted learning of hardware-embedded probabilistic graphical models. *Phys. Rev. X.* 2017; 7(4): Article No. 041052. DOI: 10.1103/PhysRevX.7.041052

60. Wittek P., Gogolin C. Quantum enhanced inference in Markov logic networks. *Scientific Reports.* 2017; 7: Article No. 45672. DOI: 10.1038/srep45672

61. Potok T.E., Schuman C.D., Young S.R., Patton R.M., Spedalieri F., Liu J., Yao K.-T., Rose G., Chakma G. A study of complex deep learning networks on high performance, neuromorphic, and quantum computers. *2016 2nd Workshop on Machine Learning in HPC Environments (MLHPC)*, Salt Lake City, Utah, USA, 2016: 47-55. doi:10.1109/MLHPC.2016.009

62. Aerts D., Broekaert J., Gabora L., Sozzo S. Quantum structures in cognitive and social science (Editorial). *Front. Psychol.* 2016; 7(APR): Article No. 577. DOI: 10.3389/fpsyg.2016.00577

63. Aerts D., Sozzo S., Veloz T. Quantum structure of negation and conjunction in human thought. *Front. Psychol.* 2015; 6: Article No. 1447. DOI: 10.3389/fpsyg.2015.01447

64. Aerts D., Sozzo S. Quantum entanglement in conceptual combinations. *Int. J. Theor. Phys.* 2014; 53: 3587-3603. DOI: 10.1007/s10773-013-1946-z

65. Khrennikov A. Quantum-like model of unconscious–conscious dynamics. *Front. Psychol.* 2015; 6: Article No. 997. DOI: 10.3389/fpsyg.2015.00997

66. Bisconti C., Corallo A., Fortunato L., Gentile A.A., Massafra A., Pellè P. Reconstruction of a real world social network using the Potts model and loopy belief propagation. *Front. Psychol.* 2015; 6: Article No. 1698. DOI: 10.3389/fpsyg.2015.01698

Об авторах:

Сигов Александр Сергеевич, доктор физико-математических наук, академик РАН, президент ФГБОУ ВО «МИРЭА – Российский технологический университет», заведующий кафедрой наноэлектроники Физико-технологического института ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Андрианова Елена Гельевна, кандидат технических наук, доцент, доцент кафедры корпоративных информационных систем Института информационных технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Жуков Дмитрий Олегович, доктор технических наук, профессор, профессор кафедры информационного противоборства Института комплексной безопасности и специального приборостроения ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Зыков Сергей Викторович, доктор технических наук, доцент, профессор Департамента программной инженерии факультета компьютерных наук Национального исследовательского университета «Высшая школа экономики» (101000, Россия, г. Москва, ул. Мясницкая, д. 20).

Тарасов Илья Евгеньевич, доктор технических наук, профессор, профессор кафедры корпоративных информационных систем Института информационных технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

About the authors:

Alexander S. Sigov, D.Sc. (Physics and Mathematics), Academician of RAS, President of MIREA – Russian Technological University; Head of the Chair of Nanoelectronics, Physics and Technology Institute, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454, Russia).

Elena G. Andrianova, Ph.D. (Engineering), Docent, Associate Professor of the Chair of Corporate Information Systems, Institute of Information Technology, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454, Russia).

Dmitriy O. Zhukov, D.Sc. (Engineering), Professor, Professor of the Chair of Information Confrontation, Institute of Integrated Security and Special Instrument Engineering, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454, Russia).

Sergey V. Zykov, D.Sc. (Engineering), Associate Professor, Professor of the Department of Software Engineering, Faculty of Computer Science, National Research University “Higher School of Economics” (20, Myasnitskaya st., Moscow, 101000, Russia).

Ilya E. Tarasov, D.Sc. (Engineering), Professor, Professor of the Chair of Corporate Information Systems, Institute of Information Technology, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454, Russia).

Для цитирования: Сигов А.С., Андрианова Е.Г., Жуков Д.О., Зыков С.В., Тарасов И.Е. Квантовая информатика: обзор основных достижений // Российский технологический журнал. 2019. Т. 7. № 1. С. 5–37. DOI: 10.32362/2500-316X-2019-7-1-5-37

For citation: Sigov A.S., Andrianova E.G., Zhukov D.O., Zykov S.V., Tarasov I.E. Quantum informatics: Overview of the main achievements. *Rossiyskiy tekhnologicheskiy zhurnal* (Russian Technological Journal). 2019; 7(1): 5-37. (in Russ.). DOI: 10.32362/2500-316X-2019-7-1-5-37