Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Брэндмайер, Хайе, Войвод
Connections QJ 20, № 2 (2021): 89-111
https://doi.org/10.11610/Connections.rus.20.2.08

Рецензированная статья

Дальнейшее развитие квантовых вычислений и их важность для НАТО

***Руперт Брэндмайер,*[1] *Йорн-Александер Хайе,*[2] *Клеменс Войвод*[2]**

[1] *Школа менеджмента Кутаисского международного университета, https://www.kiu.edu.ge*

[2] *Аналитический центр JAM Systems Cyber Security Europe, http://jamsys.eu*

Аннотация: Первые квантовые компьютеры становятся реальностью и учёные, работающие в разных областях, мечтают воспользоваться их огромным вычислительным потенциалом. В то же время высокая производительность квантовых компьютеров несёт серьёзные риски для кибербезопасности. Можно ожидать гонки вооружений между сторонами: теми, кто защищается, пытаясь гарантировать сохранность и надёжность хранимой и передаваемой информации, и их противниками. Авторы этой статьи попытались описать ход разработки квантовых компьютеров, спрогнозировать следующие шаги и проанализировать возможное влияние будущих квантовых систем на кибербезопасность и военные операции. Сначала мы рассмотрим принципиальные отличия квантовых вычислений от классических и обнаружим, что аналогий между ними немного. Мир квантовых компьютеров уже чрезвычайно разнообразен, и мы поясняем, что и квантовые симуляторы, и универсальные квантовые компьютеры используют q-биты, но работают они совершенно по-разному. Раз уж эксперты в области безопасности изучают новые тенденции квантовых вычислений, мы рассмотрим новейшие технологии и гонку за «квантовое превосходство». Наконец, мы даём детальный анализ конкретных рисков квантовых компьютеров для традиционных систем шифрования и приходим к выводу, что такие асимметричные алгоритмы, как протокол RSA, весьма уязвимы. Угрозы квантовых вычислений для криптографии очевидны, как и проблемность защиты хранимых и передаваемых

данных в военном секторе. Но мы изучаем спектр возможностей квантовых технологий и видим, что взлом асимметричных алгоритмов шифрования – лишь одна грань; другие функции, например, квантовый алгоритм Гровера, могут революционизировать логистику вооружённых сил. Спутниковое квантовое распределение ключей – еще одна перспективная концепция, способная изменить связь между военными подразделениями. Для НАТО квантовые вычисления имеют две стороны: альянсу нужно использовать достижения и быть готовым противодействовать киберугрозам. Мы подсказываем НАТО, что нужно сделать, чтобы подготовиться к квантовой эре.

Ключевые слова: квантовые вычисления, квантовая кибербезопасность, квантовое превосходство, криптография, теория сложности вычислений, квантовая устойчивость, квантовое распределение ключей, НАТО.

Вступление

В нашу эпоху «классических вычислений» обеспечение кибербезопасности представляет собой огромную проблему. После кибератаки 2007 г. на Эстонию НАТО в 2008 г. впервые утвердила Политику киберзащиты и создала Управление киберзащиты в Брюсселе.[1] Стратегическая концепция НАТО 2010 г. признаёт важность гибридных угроз, включая кибератаки, ибо комплексные риски не ограничиваются географическими рамками.

В частности, тревожные масштабы приобретают киберугрозы в финансовом секторе. Cyber Security Ventures и IBM сообщают, что атаки на новичков в этой отрасли ради выкупа происходят каждые 14 секунд. В 2016 г. кибератак на финансовый сектор было на 64% больше, чем на другие сектора.[2] Взлом, то есть перехват или вмешательство в связь между двумя сторонами, представляет особый риск для финансового и других секторов. Поэтому компаниям и ведомствам рекомендуют защищать все точки доступа, реализуя ряд мер безопасности.[3]

С развитием технологий защиты успешные кибератаки на корпоративные, правительственные, военные сети требуют всё больше ресурсов более крупных правительственных или преступных организаций. Анализ источников кибератак показывает, что в то время, как нападения на финансовые

[1] Häly Laasme, “The Role of Estonia in Developing NATO’s Cyber Strategy,” Cicero Foundation Great Debate Paper No. 12/08 (The Cicero Foundation, December 2012), https://www.cicerofoundation.org/wp-content/uploads/Laasme_-Estonia_NATO_Cyber_-Strategy.pdf.

[2] Emma Olsson, “Report: FIs Warned to Prepare for Quantum Threats,” *bobsguide*, December 6, 2019, https://www.bobsguide.com/guide/news/2019/Dec/6/report-fis-warned-to-prepare-for-quantum-threats.

[3] Olsson, “Report: FIs Warned to Prepare for Quantum Threats.”

учреждения по-прежнему в основном совершает небольшая группа мошенников, пытающихся вымогать деньги, разработка правительственных или военных целей ведётся в основном на государственном уровне.[4]

Даже передовой инфраструктуры цифровой защиты скоро может быть недостаточно, поскольку появление квантовых компьютеров изменит качество кибератак. По мнению ряда экономических «тяжеловесов», включая Microsoft и JPMorgan, коммерческий квантовый компьютер появится на рынке к 2030 г., возможно, уже в 2024 г.[5] Мировой рынок квантовых вычислений к 2024 г. может превысить 10 млрд. долларов.[6]

Впрочем, многие эксперты оспаривают такие прогнозы. Исходя из необходимости множества технических разработок, они считают, что пройдут десятилетия, пока будут созданы квантовые компьютеры, способные «расколоть» нынешние системы шифрования, и не исключают, что такие попытки могут быть безуспешными. Поэтому эти эксперты убеждены, что квантовые компьютеры, представляющие угрозу для существующих методов криптографии, появятся не раньше 2030 г.[7] Тем не менее администраторы баз конфиденциальных данных, требующих длительной защиты, например, секретных правительственных документов или старых корневых сертификатов, должны искать альтернативы асимметричным алгоритмам.[8]

Учитывая переворот в системах шифрования из-за квантовых вычислений и важность криптографии для военных операций, НАТО уже сейчас нужно начинать готовить эти системы к квантовым кибератакам. Но криптография – не единственная область, которую революционизируют квантовые технологии; другие сектора, например, дальняя связь, тоже крайне важны для НАТО. В этой статье мы пристальней рассмотрим возможные сценарии.

Далее статья построена таким образом: в разделе II a мы рассмотрим, что отличает квантовый компьютер от классического. В разделе II b рассматриваются разные типы квантовых компьютеров. В разделе II c рассмотрены аспекты технологии квантовых вычислений, а в разделе II d описан термин

---

4 J.R. Wilson, “Military Cyber Security: Threats and Solutions. U.S. Government and Military Are Taking a Lead Role in Protecting Sensitive Computers from Cyber Attack, and Solutions Finally Are on the Horizon,” *Military & Aerospace Electronics*, December 18, 2019, https://www.militaryaerospace.com/trusted-computing/article/14073852/military-cyber-security-tactical-network.

5 Olsson, “Report: FIs Warned to Prepare for Quantum Threats.”

6 Walid Rjaibi, Sridhar Muppidi, and Mary O’Brien, “Wielding a Double-edged Sword: Preparing Cybersecurity Now for a Quantum World” (IBM Corporation, July 2018), https://www.ibm.com/downloads/cas/5VGKQ63M.

7 Arthur Herman and Idalia Friedson, “Quantum Computing: How to Address the National Security Risk” (Washington, D.C.: Hudson Institute, 2018), https://s3.amazonaws.com/media.hudson.org/files/publications/Quantum18FINAL4.pdf.

8 John Preuβ Mattsson and Erik Thormarker, “What Next in the World of Post-Quantum Cryptography?” *Ericsson Blog*, March 4, 2020, https://www.ericsson.com/en/blog/2020/3/post-quantum-cryptography-symmetric-asymmetric-algorithms.

«квантовое превосходство». В разделе III анализируются сложности прогнозирования будущих квантовых вычислений. Раздел IV содержит обзор возможностей квантовых компьютеров по решению задач. В разделе V рассмотрено влияние квантовых вычислений на кибербезопасность в целом. В разделе VI показано, как квантовые возможности связаны с военной сферой, а результаты наших исследований обобщены в разделе VII.

II. Наука и технология квантовых вычислений

a. Классический и квантовый компьютер

Сначала посмотрим на отличия «классических» и «квантовых» компьютеров. В классических компьютерах «биты», принимающие значения 0 или 1 («бинарная система»), представлены электрическими сигналами, а данные обрабатываются в виде линейного потока битов. В квантовых компьютерах классический бит заменён «квантовым битом», или «q-битом», причём q-бит соответствует частице, например, фотону или электрону, а не электрическому сигналу. Квантовые вычисления интересны тем, что небольшое количество q-битов позволяет хранить и обрабатывать огромный объём данных.

Подобно биту, q-бит при измерении тоже может находиться в одном из двух состояний, например, спин вверх или вниз (в квантовой механике спин частицы – характерная форма момента вращения). Так в чём же главное отличие между классическими и квантовыми вычислениями? В классическом компьютере информация обрабатывается линейно, а в квантовом компьютере – экспоненциально. Физическое объяснение этого отличия заключается в том, что микроскопические объекты могут находиться в состоянии «суперпозиции» (до наблюдения спиновое состояние электрона может быть «вверх», «вниз», или их суперпозиция), а коллективным состоянием комбинированной системы из нескольких микроскопических объектов может быть суперпозиция отдельных состояний этих объектов («запутанность»).

«Запутанность» и «суперпозиция» возможны лишь для квантовых, но не классических состояний. В квантовом компьютере ансамбль запутанных q-битов готовят так, что когерентная система находится в суперпозиции всех комбинаторных конфигураций q-битов до измерения. Запутанность делает возможным программирование многокубитных логических вентилей.[9] Время когерентности определяется как время квантовых состояний, которые могут быть использованы в технологических целях.[10]

---

[9] David Cardinal, “How to Make Sense of Google’s Quantum Supremacy Claim,” *ExtremeTech*, October 29, 2019, https://www.extremetech.com/extreme/300987-googles-quantum-supremacy-paper-tldr-edition.

[10] Stuart A. Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD” (Alexandria, Virginia: Institute for Defense Analyses, June 2019), https://www.jstor.org/stable/resrep22809.

Рассмотрим «знания» наблюдателя о квантовой механической системе. Есть принципиальное отличие между моментами «до измерения» и «после измерения», потому что квантовая механика – статистическая теория. В зависимости от количества запутанных q-битов, число возможных результатов наблюдения, соответствующих возможным результатам расчётов, может быть огромным. Для «расчёта», т.е. измерения, выбирают лишь одну случайную конфигурацию состояний запутанных q-битов из множества возможных результатов измерений.

Случайность результата одного наблюдения поясняется вероятностным характером квантовой механики. Квантовая неопределённость означает, что нераспределённый q-бит может принимать любое значение, позволенное суперпозицией состояний.[11] Без манипуляций результаты измерений спина вверх и вниз одинаково вероятны, но каждый результат связан с индивидуальной амплитудой вероятности. Квантовые вычисления соответствуют такой манипуляции q-битов, что шанс увидеть желаемый результат, скажем, спин вверх, растёт.[12] Задача состоит в том, чтобы организовать q-бит так, чтобы вероятность правильного и неправильного ответа была максимальной и минимальной, соответственно. Эксперимент нужно повторять до достижения выборки достаточного размера, гарантирующей статистическую значимость среднего результата.

Из-за запутанности q-битов процесс измерений при квантовых вычислениях может «создать» информационный контент, растущий экспоненциально с числом q-битов. Этап выбора q-битной конфигурации, при которой используется волновая природа квантовых механических состояний, можно интерпретировать как реализацию процессора, выполняющего столько операций, сколько одновременно может быть q-битных конфигураций. Эта характеристика предполагает высокую эффективность квантовых компьютеров при решении специфичных «квантово-адаптированных» математических задач.

Таким образом, квантовые процессоры в целом не «быстрее» классических процессоров при решении любых вычислительных задач, в частности, потому, что они выполняют больше тактовых циклов в единицу времени – так же определяется скорость классических процессоров. Квантовые процессоры могут превосходить классические процессоры, только если вычислительную задачу можно задать в форме, позволяющей использовать свойства квантовой механической волны q-бита. Представим, что система запутанных q-битов может быть организована так, чтобы выборочно улучшать решение математической задачи и отменять все q-битные конфигурации, соответствующие неправильным ответам, через помехи в деструктивной

---

[11] George Johnson, *A Shortcut Through Time: The Path to the Quantum Computer* (New York: Alfred A. Knopf, 2003).

[12] Eric Jodoin, “Straddling the Next Frontier; Part 1: Quantum Computing Primer,” White Paper (Bethesda, Maryland: SANS Institute, 2014), https://www.sans.org/reading-room/whitepapers/securitytrends/paper/35390.

фазе. В этом случае квантовый процессор может дать результат гораздо быстрее, чем классический, потому что требуемое количество квантовых операций («измерений») намного меньше числа классических операций с плавающей запятой.[13]

b. Два типа квантовых компьютеров

В предыдущем разделе мы в общем говорили о «квантовом компьютере», однако нам следует уточнить используемую здесь терминологию. В этом разделе мы даём определения (насколько возможно) разных видов квантовых вычислений. Говоря о программировании многокубитных логических вентилей в предыдущем разделе, мы по умолчанию описывали характеристику «универсального квантового компьютера». Но для двух главных классов квантовых компьютеров – «квантового симулятора» и «универсального квантового компьютера» – характерны и многие другие свойства.

Первый тип квантового компьютера – это квантовый симулятор, или квантовый эмулятор. Квантовые симуляторы можно в какой-то мере рассматривать как аналоговые системы, предназначенные для исследования специфических квантовых явлений, которые трудно исследовать экспериментально и слишком сложно – путём симуляции на классическом суперкомпьютере. Квантовые симуляторы используют квантово-механические свойства суперпозиции и запутанности. Они выполнены в виде разных физических систем, например, как симуляторы на связанных ионах или ультрахолодных атомах.

Квантовый отжиг можно описать как аналоговую версию квантовых вычислений,[14] хотя квантовые отжигатели можно динамически конфигурировать («программировать»), используя программное обеспечение.[15] Эти квантовые процессоры используют q-биты минимальной запутанности, но обеспечивают достаточное время когерентности для выполнения расчётов.

Квантовые отжигатели можно описать как квантовые симуляторы, использующие сверхпроводящие q-биты для определения основных состояний гамильтонианов спиновых систем адиабатным изменением внешнего магнитного поля с начального до конечного значения. Гамильтониан – это математический оператор, определяющий энергетические уровни квантовой механической системы. Термин «адиабатный» означает, что внешнее поле применяют так, что собственные функции системы (квантованные стационарные состояния системы) медленно меняются, а числа заполнения

---

[13] Herman and Friedson, “Quantum Computing: How to Address the National Security Risk.”

[14] Arnab Das and Bikas K. Chakrabarti, “Quantum Annealing and Analog Quantum Computation,” *Reviews of Modern Physics* 80, no. 3 (2008): 1061-1081, https://doi.org/10.1103/RevModPhys.80.1061.

[15] Jack Krupansky, “What Is a Universal Quantum Computer?” *medium.com*, September 1, 2018, https://jackkrupansky.medium.com/what-is-a-universal-quantum-computer-db183fd1f15a.

состояний остаются неизменными. Могут быть разработаны разные профили адиабатного изменения для адиабатной трансформации начального гамильтониана в конечный. Основное состояние этого конечного гамильтониана соответствует решению задачи.[16] При этом подходе используется квантово-механический туннельный переход через потенциальные барьеры для исследования топологии энергетический поверхности.[17]

Квантовые отжигатели специально созданы для поиска глобального минимума функции при многих локальных минимумах, что соответствует решению задач комбинаторной оптимизации, наподобие задачи о коммивояжёре, т.е. задач с пространством дискретного поиска. Режим подсчёта квантовых отжигателей основан на квантовых флюктуациях, а не на манипуляции (контролируемой, неслучайной запутанности) q-битов.

Первый коммерческий квантовый отжигатель в 2011 г. запустила компания D-Wave Systems. В 2015 г. сообщалось об ускорении в 108 раз на наборе сложных задач оптимизации в системе D-Wave 2X, по сравнению с моделированием отжига и квантовыми методами Монте-Карло.[18] В тысячекубитной системе Advantage Pegasus P16, показанной в 2020 г., использован принцип квантового отжига для расчётов при помощи более 5000 случайно запутанных сверхпроводящих q-битов. Этот тысячекубитный адиабатный квантовый отжигатель можно, например, использовать для поиска наркотиков.[19] Однако вопрос о реальных преимуществах квантовых отжигателей при решении некоторых алгоритмов оптимизации перед классическими компьютерами остаётся открытым.[20]

Второй тип квантового компьютера – универсальный квантовый компьютер. Правда, однозначного определения такого устройства не существует.[21] По Крупанскому,[22] универсальный квантовый компьютер использует достаточно большое число q-битов для решения нетривиальных, общих задач, что отличает его от специальных и узкофункциональных квантовых компьютеров, предназначенных для решения некоторых чётко опреде-

---

[16] P. Richerme et al., “Experimental Performance of a Quantum Simulator: Optimizing Adiabatic Evolution and Identifying Many-body Ground States,” *Physical Review A* 88, no. 1 (July 2013): 12334, https://doi.org/10.1103/PhysRevA.88.012334.

[17] Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

[18] Hartmut Neven, “When Can Quantum Annealing Win?” *Google AI Blog*, December 8, 2015, https://ai.googleblog.com/2015/12/when-can-quantum-annealing-win.html.

[19] Nicole Hemsoth, “Glaxosmithkline Marks Quantum Progress with D-wave,” *TheNext Platform*, February 24, 2021, www.nextplatform.com/2021/02/24/glaxosmithkline-marks-quantum-progress-with-d-wave.

[20] Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

[21] Krupansky, “What Is a Universal Quantum Computer?”

[22] Krupansky, “What Is a Universal Quantum Computer?”

лённых вычислительных задач, т.е. квантовых симуляторов. Иными словами, квантовый компьютер делает универсальным слой цифровой обработки, преобразующий микрокоманды в импульсы для манипуляции q-битами, позволяя им работать как квантовый логический вентиль.[23] Таким образом все операции могут выполняться на одном q-бите или паре q-битов.

Поскольку «цифровой» означает «с дискретным значением», стоит отметить, что также продолжаются попытки квантовых вычислений непрерывных переменных, например, проект оптических вычислений Xanadu.[24]

Согласно Крупанскому,[25] универсальные квантовые компьютеры делят на четыре уровня. Квантовый компьютер 1 уровня – это универсальная квантовая машина Тьюринга, неспособная выполнить сложный набор команд. Возможности универсального квантового компьютера возрастают на каждом уровне, достигая 4 уровня, для которого характерны квантовые компьютеры, намного превосходящие по ёмкости и производительности классический компьютер. Создание универсального квантового компьютера 4 уровня зависит от запутанности большого числа q-битов в течение всего времени вычислений, а это крайне сложная задача.

c. Технология квантовых вычислений

Благодаря возможностям квантовых компьютеров интерес науки и промышленности к их созданию огромен, но то же касается и базовых технических требований. Одной из основных проблем при реализации квантового компьютера является непостоянство запутанности. Чтобы квантовый процессор работал, необходимо поддерживать некоторой количество q-битов в суперпозиции состояний достаточно долгое время – время когерентности. Присущая квантовым состояниям нестабильность ведёт к тенденции быстрого рассеивания тщательно организованной запутанности. Этот процесс называют декогеренцией.

Поскольку декогеренцию q-битов усиливают внешние помехи, квантовый компьютер должен быть изолирован от внешней среды. Лучшие условия для квантовых процессоров – вакуумные контейнеры и сверхнизкие температуры, потому что они повышают стабильность суперпозиции и запутанности q-битов.[26]

Сейчас разрабатывают разные концепции реализации q-битов: сверхпроводимость, ионная ловушка, квантовая точка, топологическая, спиновая, триггер. Разработка одних только началась, других – уже продвинулась. Квантовые симуляторы со сверхпроводящими q-битами готовы к выходу на

---

[23] Richard Versluis, “Here’s a Blueprint for a Practical Quantum Computer,” *IEEE Spectrum*, March 24, 2020, https://spectrum.ieee.org/computing/hardware/heres-a-blueprint-for-a-practical-quantum-computer.

[24] Krupansky, “What Is a Universal Quantum Computer?”

[25] Krupansky, “What Is a Universal Quantum Computer?”

[26] Herman and Friedson, “Quantum Computing: How to Address the National Security Risk.”

рынок. Однако q-битную систему, которая позволит создать универсальный квантовый компьютер, ещё предстоит изобрести.

d. Квантовое превосходство

Важным термином при описании развития квантовых вычислений является «квантовое превосходство». Хотя квантовый компьютер, способный расшифровать асимметричное шифрование («премиальный квантовый компьютер», quantum prime computer), может оставаться фантастикой, некоторые эксперты верят в близость ещё одного важного шага в квантовых вычислениях: квантовое превосходство.[27] Квантовое превосходство будет достигнуто, когда квантовый компьютер сможет решить задачу, пусть искусственную, которую за полиномиальное время не может решить классический компьютер.

В октябре 2019 г. команда в составе группы Google AI Quantum и университетских учёных[28] заявила о достижении квантового превосходства случайным программированием 53 физических q-битов квантового процессора Sycamore с применением однокубитных и двухкубитных логических операций (логические вентили).

Из-за нестабильности физических q-битов требуются определённые комбинации физических q-битов для коррекции ошибок в квантовых вычислениях, чтобы получить абстрактный логический q-бит. Код коррекции ошибок в квантовых вычислениях содержит информацию, соответствующую логическому состоянию одного q-бита при запутанном состоянии ансамбля физических q-битов.[29] После коррекции ошибок в квантовых вычислениях процессора Sycamore запутанные физические q-биты сводятся к фракции одного логического q-бита.[30]

Хотя на этапе программирования теоретического квантового процессора все q-биты могут быть коллективно запутаны, в Sycamore запутываются только соседние q-биты. Это ограничение можно в какой-то степени компенсировать взаимозаменой q-битов, что занимает много времени и поэтому вредит когерентности.[31] Тем не менее, согласно Эруту с коллегами,[32]

---

[27] Herman and Friedson, “Quantum Computing: How to Address the National Security Risk.”

[28] Frank Arute et al., “Quantum Supremacy Using a Programmable Superconducting Processor,” *Nature* 574, no. 7779 (October 2019): 505-510, https://doi.org/10.1038/s41586-019-1666-52019.

[29] Giuliano Gadioli La Guardia, ed., *Quantum Error Correction. Symmetric, Asymmetric, Synchronizable, and Convolutional Codes*, Quantum Science and Technology Series (Springer, 2020).

[30] Preuβ Mattsson and Thormarker, “What Next in the World of Post-Quantum Cryptography?”

[31] Cardinal, “How to Make Sense of Google’s Quantum Supremacy Claim.”

[32] Arute et al., “Quantum Supremacy Using a Programmable Superconducting Processor.”

для решения численных задач, выполняемых процессором Sycamore примерно за 200 секунд, суперкомпьютеру IBM Summit понадобится 10 000 лет. В IBM сразу же опровергли утверждение Эрута и его коллег,[33] заявив, что дооснащение Summit вторичной памятью сократит время моделирования цепей Sycamore до 2,5 дней, что достаточно быстро, чтобы развеять заявление о превосходстве Sycamore.[34]

Спор о взгляде на квантовое превосходство Sycamore предвосхищает проблемы толкования и оценки достоверности результатов квантовых вычислений, которые возникнут при достижении этапа невозможности проверки этих результатов с помощью обычных суперкомпьютеров.[35]

Стоит отметить, что обоснованность термина «квантовое превосходство» в последнее время подвергают сомнению, поскольку он предполагает очень маловероятный сценарий, что квантовые компьютеры в целом смогут превзойти классические компьютеры, в то время как будущие квантовые компьютеры могут быть эффективнее классических компьютеров только при решении специфических задач. Поэтому для описания прогресса в квантовых вычислениях рекомендуются выражения наподобие «квантовое преимущество» и «квантовая практичность».[36]

III. Прогноз развития квантовых вычислений

Скорость прогресса квантовых вычислений предугадать очень сложно. Одна из причин такой неопределённости заключается во множестве рассматриваемых в настоящее время q-битных технологий. Чтобы решить, какие q-битные архитектуры окажутся успешными в будущем, нужно ответить на множество теоретических и практических вопросов. Ещё одним фактором является вопрос о том, какое влияние окажет наличие квантовых компьютеров раннего поколения на конструкцию последующих поколений. Наконец, непросто понять, в каком масштабе другие грядущие инновации, такие как искусственный интеллект, могут повлиять на эволюцию квантовых компьютеров.[37]

---

[33] Arute et al., “Quantum Supremacy Using a Programmable Superconducting Processor.”

[34] Edwin Pednault et al., “Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore Circuits,” *arXiv*, 2019, https://arxiv.org/abs/1910.09534.

[35] “Google’s Search for Quantum Supremacy,” *ID Quantique*, March 20, 2018, https://www.idquantique.com/googles-search-for-quantum-supremacy.

[36] Scott Fulton III, “What Happened to Quantum Supremacy? Quantum Computing Needs a New Success Metric,” *ZDNet*, November 2, 2020, https://www.zdnet.com/article/what-happened-to-quantum-supremacy-quantum-computing-needs-a-new-success-metric.

[37] Herman and Friedson, “Quantum Computing: How to Address the National Security Risk.”

Собственно, взаимное усиление обеих научных дисциплин не исключено, поскольку квантовые вычисления также окажут влияние на искусственный интеллект, выполняя определенные операции намного быстрее классических компьютеров. Этот прогноз стимулировал появление междисциплинарного направления «Квантовый искусственный интеллект» (Quantum Artificial Intelligence, QAI). Машинное обучение является подотраслью искусственного интеллекта, а одна из дисциплин QAI – последующее квантовое машинное обучение.

В 2019 г. Институт оборонных исследований (Institute for Defense Analyses, IDA) выполнил для Министерства обороны США всесторонний анализ возможного влияния квантовых технологий на военно-политические интересы.[38] Согласно Вулфу с коллегами,[39] в развитии цифровых квантовых вычислений будет три этапа: квантовые вычисления компонентов (component quantum computation, CQC), квантовые вычисления среднего масштаба с шумами (noisy intermediate-scale quantum computing, NISQ), и устойчивые к ошибкам квантовые вычисления (fault-tolerant quantum computing, FTQC). Для сверхпроводящих q-битов и q-битов со связанными ионами достигнут этап NISQ. Альтернативные архитектуры, например, квантовые точки, всё ещё находятся на этапе CQC. Ни одна q-битная технология пока что не приблизилась к FTQC.

Математик Питер Шор в 1994 г. предложил алгоритм квантового компьютера для факторизации целых чисел в полиномиальный срок.[40] Для реализации алгоритма Шора для факторизации чисел, слишком больших для классических суперкомпьютеров, нужен процессор уровня FTQC с примерно 106 физическими q-битами. По мнению Грумблинг и Горовица,[41] серьёзно ожидать появления такого премиального квантового компьютера в настоящее время не стоит, его реализация может занять не менее 20 лет.

Остаётся увидеть, пройдёт ли проверку реальностью закон Невена, по которому производительность квантовых компьютеров повышается с молниеносной дважды экспоненциальной скоростью по сравнению с классическими компьютерами. Можно сказать, что закон Невена описывает эволюцию числа q-битов в квантовых процессорах, по аналогии с законом Мура, предопределяющим число транзисторов в обычных процессорах.[42]

---

[38] Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

[39] Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

[40] Peter W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Comput. Soc. Press, 1994), 124-134.

[41] Emily Grumbling and Mark Horowitz, eds., *Quantum Computing: Progress and Prospects* (Washington, DC: The National Academies Press, 2019).

[42] Preuβ Mattsson and Thormarker, “What Next in the World of Post-Quantum Cryptography?”

IV. Пригодность квантовых компьютеров для решения конкретных задач

Квантовые компьютеры в целом существенно не превзойдут классические компьютеры при решении задач, но преимущество квантовых компьютеров над классическими будет прямо зависеть от характера решаемых задач. Доказано, что квантовые алгоритмы потенциально могут массово превзойти классические алгоритмы при решении небольшой группы задач. Однако для решения многих других задач квантовые компьютеры, похоже, не дадут особых преимуществ.[43] Квантовые компьютеры смогут дать фору классическим компьютерам при выяснении глобальных свойств математических систем. Также в этом разделе мы покажем, что повышение эффективности вычислений при помощи квантовых алгоритмов зависит от характера конкретной задачи.

Прежде, чем продолжить, нам нужно дифференцировать задачи поиска и проверки решений. Для задач класса сложности *P* решения могут быть найдены и проверены за полиномиальное время. Решение задач класса «недетерминированное полиномиальное время» (*NP*) нельзя найти за полиномиальное время, но можно за полиномиальное время проверить. Задачу называют *NP*-полной, если никакие алгоритмы полиномиального времени, ни классические, ни квантовые, не обеспечивают известного решения.

Одним из примеров «квантовой задачи» является разложение n-значного числа на простые множители. Решение, очевидно, можно проверить за полиномиальное время. Однако при лучшем известном алгоритме для классических компьютеров количество шагов возрастает экспоненциально с *n*. Поэтому считают, что задача факторинга относится к классу *NP* вне *P*. Квантовый алгоритм Шора определяет задачу факторинга как глобальное свойство числа и решает эту задачу за полиномиальное время (алгоритм масштабируется с n^2).[44] Следовательно, задача факторинга не является *NP*-полной.

Но такая производительность алгоритма Шора не означает, что квантовые алгоритмы всегда дадут экспоненциальное ускорение при поиске глобальных свойств математических систем. Хороший пример – задача о коммивояжёре, тоже относящаяся к глобальным свойствам систем. В первом определении задачи о коммивояжёре (travelling salesman problem, TSP), далее – TSP1, цель – найти маршрут, соединяющий все n узлов сети, не превы-

[43] Scott Aaronson, “The Limits of Quantum Computers,” *Scientific American* 298, no. 3 (March 2008): 62-69; Chad Orzel, “What Sorts of Problems Are Quantum Computers Good for?” *Forbes*, April 17, 2017, https://www.forbes.com/sites/chadorzel/2017/04/17/what-sorts-of-problems-are-quantum-computers-good-for.

[44] Shor, “Algorithms for Quantum Computation.”

шающий заданной длины *L*. Если *S* – число маршрутов, то *S* растёт экспоненциально с *n*. При классическом подходе в среднем нужно *S/2* попыток найти маршрут, соответствующий условию.

Для понимания усилий по проверке решения TSP важно обратить внимание на конкретную постановку задачи: если она сформулирована как в TSP1, то проверка решения, очевидно, может быть выполнена за полиномиальное время. Квантовый алгоритм Гровера может выявить связь примерно в $S^{1/2}$ шагов, что значительно лучше, чем при классическом подходе, но не сводит экспоненциальное масштабирование к полиномиальному масштабированию. Этот результат показывает, что TSP1 – задача того же типа, что и поиск в неупорядоченной базе данных. Хотя TSP1 касается глобальных свойств сети, классический или квантовый алгоритм решения TSP1 за полиномиальное время пока что не найден, следовательно, TSP1 считается NP-полной задачей.

Другой вариант TSP – поиск кратчайшего пути между *n* узлами (далее – TSP2). Чтобы ответить на вопрос о кратчайшем пути, недостаточно проверить, соответствует ли длина одного из предлагаемых решений условию снижения определенного предела. Нужно также сравнить длины всех возможных путей. Поэтому даже известный квантовый алгоритм не может проверить решение TSP2 за полиномиальное время. TSP2, вероятно, не *NP*-полная, но принадлежит к более широкому классу PSPACE, что включает задачи, которые может решить классический компьютер с полиномиальной памятью, возможно, требующий экспоненциального масштабирования времени. PSPACE включает классы сложности *P* и *NP*.[45]

Так что же отличает TSP1 от задачи факторинга? Алгоритм Шора использует определённые математические свойства составных чисел и их множителей, которые можно применять для реализации конструктивных и деструктивных моделей вмешательства на квантовом компьютере, что и даёт правильный ответ. Неправильные ответы нейтрализуются деструктивным вмешательством. *NP*-полные задачи типа TSP1, похоже, не позволяют создавать такие механизмы вмешательства.

Обсуждая классы сложности, следует, однако, иметь в виду, что доказательств отсутствия квантовых или даже классических алгоритмов для решения *NP*-полных задач пока предъявлено не было. Тем не менее имеется явная аналогия в дифференциации классов *P* и *NP* с одной стороны и классов *NP* и *NP*-полной с другой. Считают, что $P \neq NP$, потому что не известны никакие классические алгоритмы, способные решать определённые задачи, например, факторинга, за полиномиальное время. Аналогично, выходит, что $NP \neq NP$-полной, потому что ещё не найдены никакие классические или квантовые алгоритмы, позволяющие решать задачи типа TSP1 за полиномиальное время.

[45] Aaronson, “The Limits of Quantum Computers.”

V. Квантовые вычисления и безопасность

В нашу эру классических вычислений в основном применяют два класса алгоритмов шифрования: симметричные и асимметричные. Одним из распространённых симметричных протоколов является Передовой стандарт шифрования (Advanced Encryption Standard, AES), поддерживающий три размера ключей: 128, 192 и 256 битов. Область применения симметричных алгоритмов – защита больших объёмов данных, например, шифрование баз данных.

При асимметричном шифровании применяют так называемые открытые и закрытые ключи для шифрования и дешифрования данных, соответственно. Автоматически связанные ключи генерируют алгоритмы шифрования с так называемой необратимой функцией. Известный асимметричный подход – протокол Rivest, Shamir, Adleman (RSA), использующий тот факт, что факторизация больших простых чисел Био на классических компьютерах занимает слишком много времени.[46] Асимметричные методы медленнее симметричных, но не требуют закрытых каналов для обмена ключами, если зашифрованной информацией обмениваются две или более сторон, как это требуется при симметричных алгоритмах.[47]

Квантовые вычисления представляют угрозу в основном для асимметричных систем шифрования, основанных на простых числах, например, квантовый алгоритм Шора [48] можно использовать для взлома шифрования RSA, в то время как симметричные протоколы не используют факторизацию простых чисел и считаются по-прежнему безопасными. Будущий квантовый компьютер, использующий алгоритм Шора и достаточно мощный, чтобы вскрыть 2048-битную реализацию протокола RSA меньше чем за день, не сможет расшифровать данные, защищённые протоколом AES-128.[49]

В 1996 г. математик Лов Кумар Гровер представил квантовый алгоритм для поиска в неупорядоченных базах данных.[50] Задача поиска в базах данных соответствует ситуации, когда единственный способ решить задачу – угадывать входной аргумент «чёрного ящика» функции и проверять правильность результата. Метод Гровера существенно уменьшает среднее количество попыток для поиска отдельной позиции в базе данных с *S* позиций

---

[46] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, and Audun Jøsang, “The Impact of Quantum Computing on Present Cryptography,” *International Journal of Advanced Computer Science and Applications (IJACSA)* 9, no. 3 (2018), https://arxiv.org/pdf/1804.00200.pdf.

[47] Rjaibi, Muppidi, and O’Brien, “Wielding a Double-edged Sword.”

[48] Shor, “Algorithms for Quantum Computation.”

[49] Preuβ Mattsson and Thormarker, “What Next in the World of Post-Quantum Cryptography?”

[50] Lov Kumar Grover, A Fast Quantum Mechanical Algorithm for Database Search,” in *STOC’96: Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, July 1996, 212-219, https://doi.org/10.1145/237814.237866; Mavroeidis, Vishi, Zych, and Jøsang, “The Impact of Quantum Computing on Present Cryptography.”

(*S* соответствует размеру области функции) до $S^{1/2}$, по сравнению с *S/2* при классических вычислениях.

Но главная сложность расшифровки симметричного стандарта типа AES в том, что размер базы данных *S* растёт экспоненциально с длиной ключа. Подход Гровера не меняет это свойство масштабирования. Алгоритм Гровера можно применять для декодирования данных, зашифрованных по протоколу AES, поиском ключа, соответствующего небольшому числу пар «сообщение-шифртекст». Например, чтобы расшифровать алгоритм AES-128, нужно последовательно выполнить около 265 обратимых оценок блочного шифра, поскольку ни один эффективный метод параллелизации не представляется реальным, и квантовое вычисление функции считается более долгим, чем классическое.[51]

Риск нынешнего широкого применения асимметричного шифрования стимулировал разработку так называемых «квантово-безопасных», или «постквантовых» алгоритмов шифрования. Эти алгоритмы предназначены для защиты данных на классических компьютерах от попыток расшифровки при помощи квантовых компьютеров.[52]

Правительство США недавно объявило, что используемый в настоящее время для шифрования данных Коммерческий набор алгоритмов национальной безопасности (Commercial National Security Algorithm Suite) после 2024 г. будут заменять квантово-безопасные алгоритмы, а это значит, что переход завершится не ранее 2030 г.[53] Поскольку секретность данных должна гарантироваться не менее 50 лет, правительство США, видимо, не ожидает появления квантовых компьютеров, способных расшифровать, например, протокол RSA-3072, в ближайшие десятилетия.[54]

Тем не менее новые квантово-безопасные функции уже активно исследуют. Две системы шифрования с открытым ключом, которые могут заме-

---

[51] Preuβ Mattsson and Thormarker, “What Next in the World of Post-Quantum Cryptography?”

[52] Preuβ Mattsson and Thormarker, “What Next in the World of Post-Quantum Cryptography?”; Thomas Pöppelmann, “Efficient Implementation of Ideal Lattice-Based Cryptography,” Dissertation (Bochum, Germany: Ruhr-University Bochum, Faculty of Electrical Engineering and Information Technology, June 2015), www.seceng.ruhr-uni-bochum.de/media/attachments/files/2019/11/diss_thomas_poeppelmann.pdf; Petros Wallden and Elham Kashefi, “Cyber Security in the Quantum Era,” in *Communications of the ACM* 62, no. 4 (April 2019): 120-128, https://doi.org/10.1145/3241037; Anne Broadbent and Christian Schaffner, (2016): “Quantum Cryptography beyond Quantum Key Distribution,” *Designs, Codes and Cryptography* 78 (2016): 351-382, https://doi.org/10.1007/s10623-015-0157-4.

[53] Jake Tibbetts, “Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers,” Technical Report LLNL-TR-790870 (Lawrence Livermore National Laboratory, September 20, 2019), https://cgsr.llnl.gov/content/assets/docs/QuantumComputingandCryptography-20190920.pdf.

[54] Mattsson and Thormarker, “What Next in the World of Post-Quantum Cryptography?”

нить протокол RSA – криптография на основе стохастической решётки и идеальной кристаллической решётки. Безопасность этих методов основана на неразрешимости задач вычисления на стохастической и идеальной решётке, соответственно. Схемы на основе решётки дали большое разнообразие инструментов шифрования, в том числе совершенно новых. Среди них – алгоритмы шифрования на основе решётки, считающиеся постквантовыми методами.[55]

Другой метод с применением открытых ключей – обмен ключами на основе суперсингулярной изогенности Диффи-Хеллмана (SIDH). SIDH позволяет создать секретный ключ между двумя ранее не связанными сторонами по незащищенному каналу связи. Применяя, при сжатии, 2688-битные открытые ключи на 128-битном квантовом уровне безопасности, SIDH использует один из наименьших размеров ключей для всех постквантовых алгоритмов.[56]

Много исследований также посвящено альтернативам квантово-безопасной криптографии, разработанным для классических компьютеров. Один из вариантов – квантовое распределение ключей (quantum key distribution, QKD), что может дать путь реализации обмена незаверенными ключами в квантовой сети. QKD обеспечивает теоретически безопасное шифрование информации, т.е. система шифрования не может быть взломана, даже если шпион имеет неограниченные возможности для вычислений.[57]

Для пояснения мы кратко вернёмся к понятиям квантовой неопределённости и суперпозиции состояний, касающимся нераспределённого q-бита. Появление квантовой частицы устраняет суперпозицию и означает, что суперпозиция переходит в одно состояние. Этот факт можно использовать для обеспечения секретности связи, поскольку подслушивание или вмешательство человека требуют измерения частицы и последующего прекращения суперпозиции состояний. Поэтому такие попытки шпионажа или манипуляции можно будет сразу же обнаружить.[58]

Поскольку принцип QKD по своей природе физический, а не математический, квантовые компьютеры не угрожают защите квантовых сетей при помощи QKD. Из-за высокой стоимости QKD можно будет использовать

---

[55] Gary Stevens, “Post Quantum Cryptography: Data Security in a Post-Quantum World,” *Security Boulevard*, April 14, 2020, https://securityboulevard. com/2020/04/post-quantum-cryptography-data-security-in-a-post-quantum-world; Pöppelmann, “Efficient Implementation of Ideal Lattice-Based Cryptography.”

[56] Stevens, “Post Quantum Cryptography: Data Security in a Post-Quantum World.”

[57] Andrew Lance, John Leiseboer, and Thomas Symul, “What Is Quantum Key Distribution (QKD)?” White Paper (Quintessence Labs, 2020), www.quintessencelabs.com/wp-content/uploads/2020/12/What-is-Quantum-Key-Distribution-QKD-whitepaper.pdf.

[58] Jodoin, “Straddling the Next Frontier.”

только для краткосрочной защиты самых важных линий. Будущая спутниковая сеть QKD сможет обеспечить безопасный обмен и передачу ключей в мировом масштабе.[59]

Однако применение QKD в других областях криптографии, кроме квантовой сети, маловероятно, потому что понадобится новое оборудование, а затраты будут высокими. Белая книга британского правительства от марта 2020 г.[60] не рекомендует крупных инвестиций в исследования QKD из-за довольно узкого диапазона применения.[61]

В этой статье мы говорили о функциях, разработке и производительности оборудования для квантовых вычислений, но нужно рассмотреть и программное обеспечение, особенно программы, предназначенные для использования на квантовых процессорах. Уже упоминались алгоритмы Шора и Гровера и ясно, что понадобится много лет для применения обеих процедур на универсальных квантовых компьютерах. Однако применение будущих квантовых процессоров на классических компьютерах можно имитировать уже сейчас, имеются и прототипы квантовых устройств для тестового кода. Активно разрабатываются языки квантового программирования. Для ознакомления с прогрессом в этой области мы отсылаем читателя к работе Гархвал с коллегами.[62]

VI. Военное применение квантовых компьютеров

В статье для «больших дебатов» Фонда Cicero в 2012 г. эстонский эксперт по безопасности Хяли Лаасме рассмотрел возможности и проблемы квантовых вычислений для НАТО.[63] Он рекомендовал «НАТО быть готовым к квантовой эре, обсуждение возможных технологических сдвигов и их последствий должно начаться как можно скорее, особенно учитывая медленный прогресс НАТО в кибернетике».

Математические открытия типа алгоритма Шора оказались очень важны для криптографии. Закрытие связи между воинскими частями, а также секретных данных, например, информации о местонахождении ракет, на центральных серверах – очень высокий приоритет для военных операций. Поэтому обеспечение квантовой устойчивости является приоритетом кибернетиков любого национального оборонного ведомства.

---

[59] Lance, Leiseboer, and Symul, “What Is Quantum Key Distribution (QKD)?”

[60] National Cyber Security Center, UK Government, “Quantum Security Technologies,” March 24, 2020, www.ncsc.gov.uk/whitepaper/quantum-security-technologies.

[61] Mattsson and Thormarker, “What Next in the World of Post-Quantum Cryptography?”

[62] Sunita Garhwal, Maryam Ghorani, and Amir Ahmad, “Quantum Programming Language: A Systematic Review of Research Topic and Top Cited Languages,” *Archives of Computational Methods in Engineering* 28 (2021): 289-310, https://link.springer.com/article/10.1007/s11831-019-09372-6.

[63] Laasme, “The Role of Estonia in Developing NATO’s Cyber Strategy.”

Технология, которая способна защитить военную связь и уже была опробована в 2018 г., основана на квантовой механике: спутниковое QKD.[64] Хотя британское правительство видит потенциал QKD для защиты важных линий связи,[65] эта технология весьма интересна для разведслужб. Идут исследования данного вопроса, в частности, в Китае, с обеих сторон: применение QKD для шифрования собственных данных и поиск путей получения информации при использовании шифрования QKD противником.[66] Тем не менее исследование IDA показало, что проблемы аутентификации и наличие безопасных неквантовых альтернатив помешают прорыву в военном применении QKD в ближайшее время.[67]

Кроме изучения возможностей QKD для закрытой связи и его угроз для разведки, развитие постквантовых методов шифрования касается и вооружённых сил, обеспечивая достаточно безопасные каналы связи и базы данных для ведения военных операций в квантовую эру.

Хотя квантовые алгоритмы вряд ли когда-либо смогут решать *NP*-полные задачи за полиномиальное время, ускорение решения TSP1 с $S/2$ шагов вычисления, нужных классическим компьютерам, до $S^{1/2}$ шагов при помощи квантового алгоритма Гровера, существенно. Как мог бы повлиять на военные операции будущий универсальный квантовый компьютер, способный решать высокоразмерные *NP*-полные задачи с масштабированием $S^{1/2}$? Характер TSP1 уже показывает, что метод Гровера может повлиять на военную логистику. Квантовый компьютер может быть способен управлять танками и машинами обеспечения, военными кораблями и самолётами намного эффективней, оптимизируя маршруты между военными базами.

Однако, согласно исследованию IDA, схемы квантовой оптимизации, например, алгоритм Гровера, вряд ли дадут достаточно большое преимущество над классическими эвристическими подходами, чтобы играть важную роль, кроме очень больших проблем оптимизации.[68] Кроме того, квантовая оптимизация по методу Гровера требует FTQC и большой квантовой памяти, что может появиться ещё не скоро.

Квантовые отжигатели при решении задач комбинаторной оптимизации используют принцип, отличный от алгоритма Гровера, а некоторые системы

---

64 Wallden and Kashefi, “Cyber Security in the Quantum Era;” Sheng-Kai Liao et al., “Satellite-Relayed Intercontinental Quantum Network,” *Physical Review Letters* 120, 30501 (January 2018), https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.120.030501.

65 National Cyber Security Center, UK Government, “Quantum Security Technologies.”

66 Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan, “Practical Challenges in Quantum Key Distribution,” *npj Quantum Information* 2, Article number 16025 (2016), https://doi.org/10.1038/npjqi.2016.25.

67 Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

68 Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

уже есть на рынке. Тем не менее квантовое преимущество этих устройств всё ещё сомнительно.[69]

Шахматы по сути имитируют индийское поле боя VI века, и умение играть в стратегические игры типа шахмат остаётся весьма важным для понимания военной тактики. Шахматы или го как игры подобны TSP2; они ставят задачи PSPACE, выходящие за рамки NP. Вопрос производительности квантовых алгоритмов в стратегических играх прямо ведёт к QAI. Собственно, шахматы были главным объектом моделирования искусственного интеллекта с появления этой отрасли. Традиционные шахматные программы используют для поиска и оценки экспертные знания. Шахматная программа AlphaGo Zero реализует идею обучения с обратной связью – подотрасли машинного обучения, которое само является подотраслью искусственного интеллекта.[70] Не полагаясь на опыт шахматистов, путём обучения с обратной связью в ходе игры, AlphaGo Zero в 2018 г. совершила революцию, превзойдя обычные шахматные программы.

Прогресс исследований «классического» искусственного интеллекта позволяет спросить, может ли QAI, в частности, квантовое машинное обучение, придать новый импульс расчёту стратегических игр. Последние исследования показывают, что реализация решений за полиномиальное время для стратегических игр через квантовые алгоритмы невозможна, но существенное ускорение по сравнению с классическими алгоритмами всё ещё представляется достижимым, аналогично сценарию TSP1.[71]

Исследования IDA также показывают, что одна из главных сложностей квантового машинного обучения – необходимость работы с большими массивами учебной информации.[72] Поэтому необходим существенный прогресс в разработке QRAM (квантовый эквивалент динамической оперативной памяти, DRAM) для реализации алгоритмов QAI, например, для игры в шахматы – способность соперничать с реализациями классического машинного обучения, наподобие AlphaGo Zero.

На схеме ниже в виде иерархической структуры показано, как квантовые вычисления могут влиять на военную сферу. Если выделить четыре слоя, дифференцируемые по росту сложности, три направления (кибербезопасность, логистика цепей поставки, анализ данных) особо интересны для военных. На схеме показано, как разные сектора зависят от таких применений, как машинное обучение с учителем, и как сами применения связаны с глав-

---

[69] Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

[70] David Silver et al., “A General Reinforcement Learning Algorithm That Masters Chess, Shogi, and Go through Self-play,” *Science* 362, no. 6419 (December 2018): 1140-1144, https://doi.org/10.1126/science.aar6404.

[71] Aaronson, “The Limits of Quantum Computers.”

[72] Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

ными дисциплинами квантовых вычислений. Разработка лекарств и финансовые оценки – лишь два примера гражданских отраслей, которые изменят квантовые вычисления.

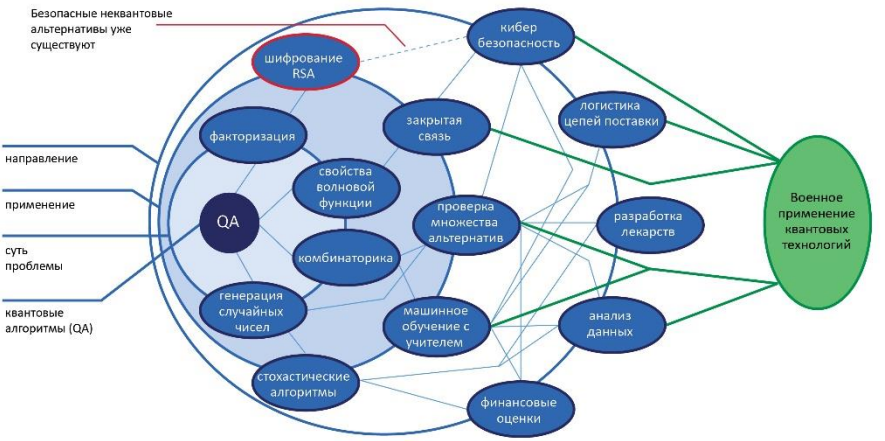

Рис. 1: Потенциальное влияние квантовых вычислений на военную сферу.

Рис. 1 даёт графическое представление о возможном влиянии квантовых вычислений на избранные области военной сферы. Как показано в этом разделе, кибербезопасность и логистика цепей поставки – направления, важные для вооружённых сил, и они же, вероятно, существенно изменятся благодаря развитию квантовых вычислений. Анализ данных – третье направление, интересное для оборонных ведомств, например, в контексте получения информации о военной деятельности противника, что тоже существенно зависит от развития квантовых алгоритмов. Разведывательные спутники собирают огромный объём данных, и квантовые компьютеры, например, в контексте применения QAI, могут помочь с извлечением ценной информации.

VII. Выводы

Во II разделе мы дали общий обзор научно-технической базы разработки квантовых компьютеров в качестве фундамента для обсуждения в последующих разделах. В III разделе коротко описаны будущие варианты квантовых вычислений, в частности, показаны трудности, усложняющие любые прогнозы. Прежде чем обсудить конкретные результаты квантовой эры для военных в VI разделе, мы сделали небольшой экскурс в теорию сложности вычислений (раздел IV), чтобы в целом рассмотреть свойства квантовых алгоритмов. IV раздел касается исключительно будущих универсальных квантовых компьютеров, поскольку они предполагают реализацию кодов, подоб-

ных сформулированным Шором и Гровером. Это логически ведёт к рассмотрению влияния будущих квантовых устройств на кибербезопасность в V разделе.

Эксперты не едины в оценке сроков, когда универсальный квантовый компьютер сможет, например, взломать шифрование RSA-2048 при помощи алгоритма Шора. Эта задача требует поддержания запутанности большего числа q-битов, что представляет огромную техническую проблему. Для создания такого устройства нужен существенный прогресс фундаментальной и прикладной науки, что влечёт значительную неопределённость реальной оценки развития квантовых вычислений. Правительство США не ожидает появления премиального квантового компьютера в ближайшие десятилетия.

Тем не менее ожидаемая способность такого компьютера взламывать ключи шифрования уже сейчас представляет огромный интерес для правительственных ведомств (см. раздел V). Так, квантовые симуляторы производства D-Wave Systems могут решать некоторые задачи оптимизации быстрее классических компьютеров и уже есть на рынке. О важности таких квантовых устройств для НАТО свидетельствует тот факт, что покупателями D-Wave Systems являются Lockheed Martin и Лос-Аламосская национальная лаборатория.

Потенциальная высокая эффективность квантовых симуляторов при решении задач комбинаторной оптимизации делает их привлекательными для применения не только в военной промышленности, но и в тыловом обеспечении войск. Однако пока ещё не ясно, дают ли эти системы реальное квантовое преимущество.[73] Поэтому НАТО следует приступить к изучению рисков и возможностей, связанных с квантовыми симуляторами, для своих операций.

Потенциальное влияние квантовых симуляторов на два других направления, показанные на Рис. 1, как важные для военных – кибербезопасность и анализ данных – менее очевидно. Однако эти два направления существенно изменятся, когда универсальные квантовые компьютеры появятся на рынке.

Квантовые компьютеры, способные взламывать традиционные системы шифрования, могут появиться лишь через десятилетия, но НАТО уже сейчас рекомендуется инвестировать в квантовую устойчивость своих компьютеров и сетевой инфраструктуры. Это может включать применение случайных чисел с полной энтропией, генерируемых квантовыми устройствами, для шифрования и применение более длинных ключей для симметричных алгоритмов, наподобие AES. Длинные и полностью рандомизированные симметричные ключи помогают защитить хранимые или восстановленные

[73] Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

ключи, делая их квантово-безопасными. Криптографическая гибкость администраторов ключей предусматривает совместимость с более длинными ключами и квантово-стойкими алгоритмами. Приоритетом должна быть замена протокола RSA, например, квантово-безопасными альтернативами, такими, как криптография на основе кристаллической решётки или SIDH. Также рекомендуется применять защищённые линии связи между узлами управления при помощи QKD и (или) квантово-безопасные алгоритмы. Решения с обменом ключами, например, QKD, тоже нужно исследовать на предмет пригодности для защиты дальней связи.[74]

Применение квантовых компьютеров для обеспечения тактических операций в ближайшее время не выглядит реальным, поскольку стратегические игры наподобие шахмат соответствуют задачам PSPACE, выходящим за рамки NP. Однако впечатляющий результат применения машинного обучения AlphaGo Zero для шахмат показывает, что QAI, как подотрасль квантового машинного обучения, может применяться для моделирования сценариев боя раньше, чем ожидали многие эксперты, хотя необходимость прорывов, в частности, в разработке QRAM по-прежнему является серьезным препятствием для использования QAI.

Примечание

Представленные здесь взгляды принадлежат исключительно авторам и не выражают официальную позицию Консорциума военных академий и институтов изучения проблем безопасности программы «Партнерство ради мира», организаций-участниц или издателей Консорциума.

Благодарность

Connections: The Quarterly Journal, Vol. 20, 2021, вышел при поддержке правительства США.

[74] "Quantum-Safe Security," *Quintessence Labs* (Canberra), 2021, https://www.quintessencelabs.com/quantum-safe-cyber-security.

Об авторах

Руперт Андреас Брэндмайер изучал экономику (специалист) и археологию (бакалавр) в Университете Людвига-Максимилиана, Мюнхен. Получил степень доктора за анализ результатов аутсорсинга в информационных технологиях. Профессор Школы менеджмента Кутаисского международного университета.
Электронная почта: rupert.andreas.brandmeier@gmail.com

Йорн-Александер Хайе – партнёр JAM Systems Cyber Security Europe OÜ (Таллинн, Эстония), более 28 лет проработавший директором и генеральным директором международных компаний. Офицер связи Бундесвера (в запасе), служил в стране и за рубежом.
Электронная почта: jheye@jamsys.eu

Клеменс Войвод – научный сотрудник JAM Systems Cyber Security Europe OÜ (Мюнхен). Также сотрудничает с кафедрой химии Мюнхенского Технического университета. Доктор наук в области теоретической химии Мюнхенского Технического университета.
Электронная почта: clemens.woywod@ch.tum.de