ЕЛЕНА ЛАРИНА,
ВЛАДИМИР ОВЧИНСКИЙ

КВАНТОВОЕ ПРЕВОСХОДСТВО И КВАНТОВАЯ МОБИЛИЗАЦИЯ

В мире началась гонка за квантовое превосходство. В конце 2020 года руководители отдела квантовых исследований *банка "Голдман Сакс"* заявили, что ***квантовые компьютерные вычисления уже в скором времени могут иметь "революционное" воздействие на банки, а также на финансы, да и на всю нашу жизнь в широком смысле.***

Ориентированные на квантовые компьютеры специалисты по биржевому количественному анализу надеются, что эти машины позволят увеличить прибыль за счёт ускорения оценки активов, поиска более выгодных портфелей, а также сделают более точным алгоритмы обучения самих машин. Проведённое в июле нынешнего года испанским *банком bbva* исследование свидетельствует, что квантовые компьютеры могут ускорить процесс оценки кредитоспособности, определить возможности для скупки акций с целью последующей перепродажи, а также ускорят так называемое имитационное моделирование с помощью метода Монте-Карло, который широко используется в финансовой области для моделирования возможного поведения рынков.

Финансы – не единственная отрасль, рассчитывающая получить выгоду даже от небольших и нестабильных квантовых компьютеров, которые доступны в настоящее время, очень многие сектора промышленности – от аэрокосмической до фармацевтической (не говоря уже о военной области) – также рассчитывают воспользоваться ***"квантовым преимуществом"***. Однако есть все основания полагать, что именно финансы смогут первыми найти такой способ.

Такие банки, *как bbva, "Ситигруп", "Джей-Пи Морган" и "Стандард чартед",* создали исследовательские команды из специалистов по квантовым вычислениям, а также подписали соглашения с компьютерными фирмами. Эксперты консалтинговой фирмы *"Бостон консалтинг груп"* считают, что банки и страховщики в Америке и в Европе, по данным на июнь текущего года, наняли на работу более 115 экспертов – это большое количество, даже в академической сфере, для такой узкой специализации.

В некоторых банках сейчас больше докторов физических и математических наук, чем в университетах.

Когда же может произойти финансовая революция? По мнению одних экспертов, простые алгоритмы могут начать использоваться в течение ***ближайших 18 месяцев***. По мнению большинства специалистов, срок ***в три – пять лет*** является более реалистичным.

На пальцах о квантовых компьютерах

Квантовым компьютерам повезло в Рунете ещё меньше, чем искусственному интеллекту. Усилиями псевдоэкспертов, различного рода неспециалистов, особенно с гуманитарным образованием, подавшихся в блогеры и выдающих себя за гуру информатики, тема квантовых компьютеров оказалась ещё более мистифицированной и запутанной, чем проблема искусственного интеллекта.

Сейчас часто говорят, что мир стоит на пороге ***второй квантовой революции.*** Считается, что первая случилась во второй половине прошлого столетия – это ядерные технологии, лазеры и транзисторы, то есть в итоге компьютеры и сотовая связь. Настало время следующего этапа – ***квантовой коммуникации и квантовых вычислений.***

Поэтому, прежде всего, надо чётко и по возможности коротко разобраться, чем квантовый компьютер отличается от обыкновенного и что такое пресловутое "квантовое превосходство". В конечном счёте, привычный нам компьютер или смартфон – не что иное, как внук арифмометра. В отличие от своего дедушки, где вычисления происходили за счёт механического взаимодействия частей арифмометра, в компьютере оно осуществляется в рамках передачи электросигналов через определённые регистры. Регистр – это элементарная единица чипа процессора. Сегодня в смартфоне предусматривается несколько миллиардов регистров, обеспечивающих процесс вычислений. Регистр – и это ключевое слово для понимания отличия квантового компьютера от обычного – принимает два значения: 0 или 1. Соответственно всё, что делают современные компьютеры, включая искусственный интеллект, – это кодировка поступающей информации, превращаемой в нули и единицы, и их вычисление. Привычные нам вычислительные устройства – это плод достижений физики последней четверти XIX века и начала нынешнего. Они базируются на принципах классической физики.

Квантовый компьютер работает иначе, нежели привычный нам компьютер. В его основе лежат достижения самой быстроразвивающейся отрасли естествознания в XX – начале XXI века, а именно квантовой физики. В последние примерно 30–40 лет удалось не только открыть, но и научиться устойчиво воспроизводить условия совершенно невероятного и до сих пор непонятного процесса, который называется суперпозиция.

В мире привычной нам физики и соответственно в компьютерах и смартфонах процессоры могут работать с двумя альтернативными возможностями, которые соответственно шифруются, как 0 и 1. Минимальная единица информации в обычном компьютере – это бит, то есть способность принимать одно из значений: 0 или 1. Квантовый компьютер, в отличие от традиционного, способен работать в состоянии суперпозиции. Применительно к вычислениям это означает, что его элементарные вычислительные ячейки могут оперировать не только 0 и 1, но и во всех возможных промежуточных состояниях между ними. Казалось бы, какая разница между тем, в одном состоянии или в двух и более пребывает вычислительная система. А разница – огромная. Если квантовый компьютер имеет, например, 10 регистров, то он может пребывать одновременно в тысяче состояний. А в 20 регистрах – более 1 млн состояний и т. д.

Квантовый компьютер, или вычислительная физическая система, использующая законы квантовой механики, имеет примерно то же сходство с традиционными компьютерами, как лошадь с самолётом. И тот, и другой способны доставить путника из пункта А в пункт Б, и в этом они схожи. Однако в темпах и иных возможностях доставки самолёт на порядки превосходит лошадь.

Собственно знаменитый термин "квантовое превосходство" фиксирует достаточно простую и очевидную вещь. Квантовый компьютер на порядки превосходит по вычислительным возможностям обычные двоичные вычислительные системы, включая даже суперкомпьютеры. Причём разница в возможностях исчисляется не разами, а тысячами и миллионами раз.

Поскольку тема квантовых компьютеров достаточно запутана и мистифицирована не только среди населения, но и в так называемых элитах, она порождает различного рода домыслы и целенаправленную дезинформацию. Например, время от времени то или иное государство сообщает, что им удалось создать полноценный вычислительный квантовый компьютер, и он устойчиво работает.

Недавно Китай заявил о том, что в стране создан квантовый компьютер, по производительности превосходящий в миллионы раз американские квантовые компьютеры, не говоря уже об обычных суперкомпьютерах. Однако беда в том, что никто из зарубежных специалистов не видел этого компьютера, и уж тем более не имел возможности работать на нём. Грешат этим не только китайцы, но и целый ряд американских компаний.

Пока в мире имеется единственный полноценный квантовый компьютер 53-кубитный квантовый компьютер *Google Sycamore*, который смог решить задачу, недоступную даже для самых мощных "обычных" суперкомпьютеров. Если быть точным, у современного суперкомпьютера IBM Summit решение этой задачи заняло бы 20 000 лет, тогда как Sycamore выполнил все необходимые вычисления всего за 200 секунд. Принципиальное отличие системы Google от иных заявленных достижений в том, что математики, физики и прочие могут подать заявку, и после рассмотрения они будут допущены к работе на компьютере. Соответственно, на нём уже отработало достаточно большое число людей с высокой репутацией в мире программирования и математики. Тем самым он прошёл общественную верификацию.

Ещё одна принципиальная сложность в использовании квантового компьютера состоит в том, что он в некотором смысле воспроизводит механику расчётов, которая существовала в те уже, казалось бы, далёкие времена, когда вместо чипов использовались лампы, а математика, лежащая в основе вычислений, носила непрерывный. а не дискретный характер. Практически это означает, что ***все программы, написанные для современных компьютеров, включая даже суперкомпьютеры, совершенно не подходят для квантового компьютера.*** В этой области пока только делаются первые шаги программирования. Соответственно, все ныне работающие квантовые компьютеры, а они созданы в США, Китае, Южной Корее, Японии и в ЕС, – это специализированные машины, рассчитанные строго на определённый тип вычислений.

Иными словами, квантовый компьютер сегодня не может, подобно смартфону, сначала показать нам фильм, потом напомнить, что надо сходить в магазин, а в итоге провести расчёты оптимального выбора вложений в акции на рынках капитала. Пока все квантовые компьютеры – это специализированные, а не универсальные машины.

Пока полноценный квантовый компьютер – это дело будущего. Пока, и об этом надо говорить чётко и ясно, существуют лишь экспериментальные действующие макеты полноценных квантовых компьютеров. Макеты в том смысле, что они работать уже могут, но ориентированы на строго определённые операции.

Однако анализ динамики развития квантовых вычислений позволяет с уверенностью утверждать, что мы имеем дело с так называемой экспоненциальной технологией. ***В 2019-2020 годах произошёл перелом. Если ещё пару-тройку лет назад наиболее продвинутые, имеющие за плечами выдающиеся достижения специалисты в области IT полагали, что практическое применение квантовых компьютеров – дело конца двадцатых – начала тридцатых годов, то сегодня с уверенностью они утверждают о приходе эры квантовых компьютеров буквально в течение ближайших четырёх-пяти лет.***

Решающее значение имеет то обстоятельство, что ***никто не хочет опоздать на этот праздник. Всех беспокоит то, что кто-то, оказавшийся первым в этой гонке, сможет выбрать такой вариант: незаметно начать получать всю выгоду и не объявлять об этом всему миру.***

Выгоды и угрозы квантовых компьютеров

Как любая технология новой промышленной революции, квантовый компьютер несёт для общества серьёзные выгоды и катастрофические угрозы. Он может преобразить банковское дело, может создать мощную систему кибербезопасности, может на порядок усовершенствовать систему защиты от любого военного нападения, а может стать страшным оружием в руках террористов или мафиозных структур.

Наиболее серьёзные угрозы глобальной и национальной безопасности, экономике и повседневной жизни несёт в себе использование квантовых компьютеров для взлома кодов. Специалисты по криптографии Агентства

Национальной Безопасности США ещё в 2015 году опубликовали на сайте АНБ отчёт, где выразили серьёзную обеспокоенность перспективой появления работающих квантовых компьютеров, поскольку это может привести к чрезвычайно быстрой расшифровке многих использующихся сегодня криптографических алгоритмов. Представители АНБ отмечали, что вопрос разработки криптостойких алгоритмов, способных эффективно шифровать данные в эру квантовых компьютеров, актуален как никогда. По мнению специалистов агентства, вполне реально появление работающего квантового компьютера, существование которого поставит под угрозу сохранность государственных и коммерческих данных во всех сферах. Хотя время от времени в ведущих мировых медиа появляются статьи об угрозах квантовых компьютеров для международных расчётных систем, процессинговых компаний, типа MasterCard, Visa и т. п., а также криптовалют и, в первую очередь, биткойна, реальная ситуация благоприятнее, чем описываемые сценарии.

Дело в том, что ***к настоящему времени разработаны и через два-три года будут готовы к практическому использованию так называемые постквантовые методы криптографии***. Они базируются на сложнейшей математике, а их применение не позволяет квантовым компьютерам вскрывать корпоративные и федеральные сети, как консервный нож банку. Более того, ***во второй половине 2020 года уже были проведены испытания прототипов квантовоустойчивой системы шифрования***, выстоявшей перед атакой квантового компьютера Goggle.

Главный недостаток систем постквантового шифрования – это чрезвычайно высокая цена не только их разработки, но и огромные издержки, связанные с практической эксплуатацией для защиты данных как хранящихся в базах данных, так и передаваемых от телекоммуникационных систем.

Время от времени появляются публикации, предсказывающие конец биткойна и криптовалют при внедрении квантового компьютера. Такого рода статьи пишут обычно либо экономисты, либо журналисты. Не говоря уже о том, что биткойн является одной из самых неудобных мишеней для квантового компьютера даже в нынешнем виде, важно знать, что к следующему году будет подготовлена специальная система шифрования, обеспечивающая его устойчивость к атакам квантовых компьютеров.

Главная и самая большая угроза квантовых компьютеров мировой экономике и повседневной жизни состоит в следующем. ***Даже на начальной стадии квантовые компьютеры могут практически мгновенно сломать любой антивирусник и получить доступ, согласно мнению АНБ, примерно к 97% индивидуальных компьютеров, смартфонов и ноутбуков и не менее 65% – корпоративных.*** Поскольку постквантовое шифрование не только на стадии разработки, но и на стадии эксплуатации требует больших денег, оно, без сомнения, будет развёрнуто в ближайшие два-четыре года для федеральных органов власти, систем национальной безопасности и правопорядка, в ведущих научных центрах и крупнейших компаниях. Причём далеко не во всех странах. Среди них будут, безусловно, США, Китай, Япония, Южная Корея и Россия.

Что же касается всех персональных устройств, IT-инфраструктур малого и среднего бизнеса, они окажутся беззащитными против квантового компьютера в случае, если он попадёт в руки преступников, а тем более террористов или хакерских сетей, работающих на разведку того или иного государства. Это мало осознаваемая, но абсолютно реальная угроза, грозящая подорвать безопасность, коммерцию, а главное, угрожающая повседневной жизни граждан.

Квантовая мобилизация

Прогнозы The Economist в последние годы, несмотря на порой их причудливость, имеют удивительное свойство сбываться. Отставание в гонке за квантовыми компьютерами и квантовыми вычислениями может стать таким же опасным, как отставание в гонке по разработке новейших видов вооружения или в гонке по созданию “сильного” искусственного интеллекта.

Напомним также, что ***АНБ забило тревогу пять лет назад и прогнозировало появление возможно опасных квантовых компьютеров и квантовых вычислений к 2030 году. Но всё случилось на 10 лет раньше.***

Россия располагает мощнейшим человеческим капиталом в области программирования, искусственного интеллекта и квантового компьютинга.

Ещё в 2019 году в России для развития квантовых технологий утверждена *“дорожная карта”,* которая входит в состав национальной программы “Цифровая экономика”. Карта рассчитана на срок до 2024 года и включает три направления: вычисления, коммуникации и сенсоры.

Квантовыми вычислениями и разработкой отечественного квантового компьютера занялись *в “Росатоме”,* квантовыми коммуникациями – в *РЖД,* сенсорами – в *“Ростехе”.*

Ведущие российские компании сотрудничают с “Росатомом” в разработке квантового компьютера – *Сбербанк и “Сбербанк-Технологии”, Газпромбанк, “Газпромнефть”, СИБУР* и другие.

Разработкой квантового компьютера в “Росатоме” занимаются учёные *ВНИИА имени Н. Л. Духова, МГУ имени М. В. Ломоносова, МФТИ, НИТУ МИСиС, НОЦ ФМН МГТУ имени Н. Э. Баумана, ФИАН, ряда академических институтов, а также РКЦ.*

25 ноября этого года объявлено о создании ***консорциума “Национальная квантовая лаборатория” (НКЛ).*** В него вошли *структура госкорпорации “Росатом” (“СП Квант”), Российский квантовый центр, фонд “Сколково”, НИУ “Высшая школа экономики”, НИТУ “МИСиС”, МФТИ и Физический институт имени П. Н. Лебедева.*

Одновременно с созданием квантового компьютера и развитием квантовых вычислений, не дожидаясь дня “Ч” (так у военных обозначается день наступления войск, или день нападения), **в России в мобилизационном режиме необходимо развернуть работу по минимизации потенциальных рисков и угроз применения квантовых компьютеров, связанную со взломом антивирусных систем.**