**Путеводитель по понятиям квантовой тематики**

1. Что такое квантовые технологии

Квантовые технологии — сравнительно молодое наукоемкое направление, основанное на явлениях квантовой физики, которое включено странами–технологическими лидерами в перечень технологий для обеспечения стратегической конкурентоспособности и безопасности.

1. Какие бывают квантовые технологии?

Традиционно выделяют три квантовые технологии: квантовые вычисления, квантовые коммуникации и квантовую сенсорику (квантовые сенсоры).

1. Что такое квантовые вычисления?

Квантовые вычисления — решение задач при помощи манипуляции квантовыми объектами: атомами, молекулами, фотонами, электронами и специально созданными макроструктурами. Их использование позволяет ученым достичь двух квантовых явлений — суперпозиции и запутанности. Благодаря этому, исследователи могут синтезировать новые материалы, лекарства, а также моделировать сложные молекулы и решать оптимизационные задачи, недоступные сейчас для самых мощных компьютеров.

1. Что такое квантовый компьютер?

Квантовые компьютеры — это новое поколение вычислительных устройств, в основе которых лежат эффекты квантовой физики. Такие устройства, использующие специализированные квантовые алгоритмы, способны на некоторых классах задач показать производительность значительно превосходящую классические компьютеры, основанные на полупроводниковых технологиях.

1. За счет чего мощность квантового компьютера превосходит классические ПК и суперкомпьютеры?

В классических вычислительных устройствах вся информация раскладывается на биты — 0 или 1, тогда как в квантовых наименьшей единицей информации является квантовый бит (кубит), способный одновременно находиться в обоих состояниях сразу — и 0, и 1. Количество состояний, в которых находится квантовый процессор, быстро растет с увеличением числа кубит за счет возможности связывать их между собой. Эта особенность позволяет квантовым устройствам решать различные вычислительные задачи на порядки быстрее классических компьютеров и суперкомпьютеров.

1. В России разрабатывают квантовые компьютеры?

Россия позже других стран приступила к разработке квантовых технологий: по-настоящему активная работа с государственной поддержкой ведется лишь последние несколько лет. В 2019 году Правительство РФ разработало дорожную карту по развитию квантовых технологий, а позже приняло решение разбить ее на 3 отдельные дорожные карты: по развитию квантовых вычислений, квантовых коммуникаций и квантовых сенсоров.

В 2022 году проявил себя накопленный эффект совместных усилий государства, высокотехнологичных компаний, университетов и академических институтов в квантовой сфере. Еще несколько лет назад технологический разрыв с ведущими странами составлял 7-10 лет, а в настоящее время по ряду направлений Россия оказалась в числе лидеров и вошла в десятку государств с наиболее развитыми квантовыми технологиями. По некоторым направлениям, таким как технология квантовых процессоров на кудитах, Россия присутствует уже в ТОП-3, а ряд квантовых алгоритмов был разработан у в нашей стране впервые в мире.

1. Кто возглавляет работу по строительству отечественных квантовых компьютеров?

В России работа по созданию квантового компьютера ведется в рамках реализации правительственной дорожной карты высокотехнологичной области «Квантовые вычисления», координатором которой является Госкорпорация «Росатом». Основная цель дорожной карты заключается в построении отечественных квантовых компьютеров на четырех различных платформах, а также создании специализированного облачного софта. Для реализации данной задачи в 2021 году создана Национальная квантовая лаборатория, объединяющая высокотехнологичные компании, академические институты, университеты и стартапы.

1. Какие платформы обсуждаются в связке с квантовыми компьютерами?

Квантовые компьютеры строятся на четырех основных платформах: сверхпроводящих цепочках, ионах, нейтральных атомах и фотонах. На самом деле платформ существует намного больше: еще есть интегральная оптика, квазичастицы (экситоны, поляритоны, магноны и др.), примесные атомы, полупроводниковые квантовые точки и центры окраски. Один компьютер может быть создан на базе нескольких платформ. Все они могут работать отдельно друг от друга.

1. На какие классы делятся квантовые вычислительные системы?

Как классические компьютеры разделяются на процессоры общего назначения и интегральные схемы специального назначения, так и квантовые вычислительные системы разделяются на два основных класса — квантовые компьютеры и квантовые симуляторы.

1. Что надо знать о квантовых симуляторах?

Квантовые симуляторы могут решать достаточно узкий круг задач за счет имитации качеств и функций реальных квантовых систем. Симуляторы можно назвать своеобразными предшественниками полноценных устройств, поскольку они позволяют в более управляемом режиме фиксировать их текущие несовершенства: например, повышать время жизни кубит или работать над эффективностью алгоритмов для компенсации ошибок.

1. Часто можно услышать об универсальных квантовых компьютерах. А бывают какие-то еще?

В работе над квантовым компьютером применяются несколько подходов. В первую очередь, это модель вентилей (цифровая), на основе которой строят так называемые универсальные квантовые компьютеры, способные реализовывать произвольные квантовые алгоритмы. Решение задачи на подобном устройстве выглядит следующим образом: исследователь берет исходное состояние квантовой системы, программирует к ней преобразования и считывает полученное состояние — оно и является ответом на заданный машине вопрос.

Ещё одной популярной парадигмой являются адиабатические вычисления, основанные на одноименной теореме квантовой механики, сформулированной Максом Борном и Владимиром Фоком. Адиабатические компьютеры — вычислительные устройства на основе квантового отжига, способные решать исключительно задачи оптимизации, но в то же время куда более эффективно, чем это делают классические компьютеры или суперкомпьютеры. В 2020 году D-Wave Systems [представила](https://www.dwavesys.com/press-releases/d-wave-announces-general-availability-first-quantum-computer-built-business) подобную машину на 5000 кубитах, но стоит помнить, что такие квантовые вычислители не являются квантовым компьютером в его привычном понимании.

Суть квантового отжига состоит в том, что при необходимой низкой температуре система всегда находится в своем обычном состоянии с минимальной энергией. Такой уровень наименьшей энергии определяется [гамильтонианом](https://ru.wikipedia.org/wiki/%D0%93%D0%B0%D0%BC%D0%B8%D0%BB%D1%8C%D1%82%D0%BE%D0%BD%D0%B8%D0%B0%D0%BD_%28%D0%BA%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BC%D0%B5%D1%85%D0%B0%D0%BD%D0%B8%D0%BA%D0%B0%29), который задается видом исследуемой функции — ее минимум достигается с помощью перераспределения энергии между ближайшими кубитами, в процессе чего регистр релаксирует к состоянию термодинамического равновесия.  Изменившееся (эволюционировавшее) состояние системы считывается в качестве ответа.

1. Как измеряется качество квантового компьютера?

Вычислительные возможности квантового компьютера определяются двумя основными характеристиками: количеством кубит и их качеством (уровнем ошибок при совершении операций).

1. В чем заключаются основные сложности при создании квантовых компьютеров?

Первая сложность — заставить кубиты стабильно сохранять когерентное состояние, то есть существовать и хранить информацию.

Вторая состоит в том, чтобы обеспечить слаженное функционирование как можно большего количества кубит одновременно. Самые совершенные квантовые компьютеры сегодня содержат десятки и сотни кубит, тогда как для революционного прорыва в производительности их потребуется на порядки больше — от тысяч до миллионов.

1. Что такое квантовые коммуникации?

Коммуникация — набор технологий для передачи информации. В современном мире мы передаем информацию, кодируя ее в какие-либо физические сигналы: например, передавая данные в виде световых импульсов по оптоволоконному кабелю. В квантовых коммуникациях, в отличие от традиционных, в качестве носителя выступают не обычные световые импульсы достаточно большой мощности, а квантовые сигналы, то есть те, которые обладают существенной квантовой природой. Оказывается, что в ряде случаев они дают возможность решать совершенно недоступные ранее задачи.

Наиболее развитое направление в рамках технологии квантовых коммуникаций — квантовая криптография, или, более точно, квантовое распределение ключей. Это совокупность методов, направленных на выработку между удаленными пользователями общего секретного ключа, который в дальнейшем используется для шифрования.

Наряду с задачами квантовой криптографии (квантового распределения ключей) квантовые коммуникации включают в себя передачу квантовой информации между квантовыми компьютерами. Технологии плавно идут к развитию распределенных квантовых вычислений, то есть к созданию, например, центрального квантового компьютера и множества периферийных машин, которые решают часть подзадач и передают данные друг другу. Альтернативой этому может быть набор связанных между собой удаленных квантовых процессоров. В феврале 2021 года группа исследователей из Германии продемонстрировала возможность передачи квантовой информации между двумя модульными квантовыми процессорами. Результаты эксперимента [опубликовал](https://science.sciencemag.org/content/371/6529/614) журнал Science. Это важный шаг в развитии технологий, который показал, что увеличивать мощность квантовых вычислительных технологий возможно за счет объединения нескольких устройств в сеть.

1. Что такое квантовая криптография?

Наиболее развитое направление в рамках технологии квантовых коммуникаций — квантовая криптография, или, более точно, квантовое распределение ключей. Это совокупность методов, направленных на выработку между удаленными пользователями общего секретного ключа, который в дальнейшем используется для шифрования.

1. Зачем нужна квантовая криптография?

Квантовые технологии открывают доступ к сверхбыстрым вычислениям — и они манят не только ученых, но и злоумышленников. И хотя пока что не существует квантовых компьютеров, достаточно мощных для массового взлома криптографических систем, все указывает на то, что они появятся в ближайшем будущем. Квантовая криптография обеспечивает защиту от атак с применением квантовых компьютеров.

1. Как работает квантовая криптография?

До того, как обмениваться зашифрованной информацией, отправитель сообщения передает получателю ключ — набор случайных чисел, необходимых для дальнейшей расшифровки сообщения. Этот ключ распределяется по оптоволоконному кабелю частицами света — фотонами. Если злоумышленник каким-либо образом перехватит ключ, получатель сообщения об этом узнает — на это укажет уровень ошибок в системе. Создать точную копию фотона для замены перехваченного тоже не получится — это гарантируют фундаментальные законы физики (в том числе теорема о запрете клонирования). Таким образом, можно гарантировать, что ключ, а значит и доступ к секретной информации, имеется лишь у легитимных — законных — пользователей.

1. Как передается квантовая информация?

Интересная технологическая особенность состоит в том, что если в квантовых компьютерах мы выбираем платформу, которая наиболее эффективно подойдет для решения тех или иных задач, то с обменом квантовой информацией все очевидно: лучше всего справляются фотоны, то есть частицы света. Поэтому исследователи уже осознают, какой будет элементная база.

1. Что такое квантовые сенсоры?

Квантовые сенсоры — высокоточные измерительные приборы, работа которых построена на эффектах квантовой механики. Они отличаются крайне высокой чувствительностью, благодаря чему способны делать измерения, недоступные классическим датчикам.

1. Где применяются квантовые сенсоры?

Такие устройства используются в автомобилестроении, здравоохранении, промышленности, геологии, транспортной отрасли, компьютерной разработке и многих других сферах. Но по-настоящему бесценный вклад квантовая сенсорика может привнести в медицину. Благодаря своей чувствительности датчики способны зафиксировать первые сигналы заболевания еще до того, как их можно будет «поймать» другими методами диагностики. А выявление болезни на ранней стадии — один из главных факторов успешного лечения.

1. Как квантовые сенсоры применяются в медицине?

Одно из основных направлений применения квантовых сенсоров в медицине — магнитоэнцефалография. Эта процедура позволяет изучать состояние мозга через измерение магнитных полей, которые возникают в ходе его электрической активности.

Большинство современных методов диагностики заболеваний мозга фиксируют не магнитные, а электрические компоненты — например, по этому принципу работает электроэнцефалография. Но эта процедура не дает полной информации: датчикам приходится ловить сигнал сквозь череп и ткани, а тело человека — плохой проводник электрических полей.

С магнитными полями все по-другому: магнитный сигнал из участка мозга проходит сквозь ткани в неизменном состоянии, так что мы можем получить от него больший объем данных. Сложность в том, что магнитные поля нашего мозга сложно уловить, поскольку их мощность крайне мала: в 10 млрд раз меньше, чем у Земли. Для этого нужны очень чувствительные приборы — такие, как квантовые сенсоры. Фиксируя эти маленькие магнитные поля, сенсоры дают возможность диагностировать различные мозговые опухоли, синдром Альцгеймера или эпилепсию.

1. В России тоже имеются подобные разработки?

Квантовые сенсоры для сверхчувствительного магнитоэнцефалографа уже существуют,  а в 2021 году команда QLU с учеными из Сколтеха и НИУ ВШЭ разработала их новый тип — первый в мире твердотельный сверхчувствительный магнитометр, который может работать при комнатной температуре. Сейчас в России создается первый прототип сверхчувствительного магнитоэнцефалографа.