

ФОРУМ
БУДУЩИХ
ТЕХНОЛОГИЙ

РОСКОНГРЕСС
Опережая время

Соорганизаторы



КВАНТОВЫЕ
ТЕХНОЛОГИИ
РОСАТОМ



ГАЗПРОМБАНК



ПРАВИТЕЛЬСТВО
МОСКВЫ

Квантовые технологии для медицины

Новые подходы в вычислениях,
защите данных и сенсорике

При поддержке



Отчет подготовлен коллективом авторов



В аналитическом отчете представлены направления применения квантовых технологий для биомедицины по направлению облачных квантовых вычислений, программно-аппаратным решениям для квантово-устойчивой защиты информации и квантовым сенсорам. Данная информация будет полезна представителям государственных и частных медицинских организаций, профильных институтов развития и научно-технологическому сообществу. Отчет сформирован на основе открытых российских и зарубежных источников

Аналитический отчет носит информационный характер. Отчет подготовлен коллективом авторов Российского квантового центра (ООО «МЦКТ») в партнерстве с компаниями Куборд (ООО «ОКТ»), QApp (ООО «КуАпп»), QRate (ООО «КуРЭйт»), QLU (ООО «М-Гранат») и ООО «СП «Квант».

Основные авторы отчета:

А.К. Федоров,
А.П. Гугля,
А.А. Божедаров,
М.И. Острась,
П.Е. Воробьев,
М.А. Кольченко.

**Замечания, предложения
и идеи просьба присылать
по адресу: apq@rqc.ru**

Содержание

Квантовые технологии	3
<hr/>	
Квантовые вычисления	5
<hr/>	
<i>Технология</i>	5
<i>Применение в медицине</i>	8
Квантово-устойчивая защита данных	11
<hr/>	
Квантовая угроза	11
Квантовые коммуникации	12
<i>Технология</i>	12
<i>Применение в медицине</i>	13
Постквантовые алгоритмы	14
<i>Технология</i>	14
<i>Применение в медицине</i>	15
Квантовые сенсоры	19
<hr/>	
<i>Технология</i>	19
<i>Применение в медицине</i>	19

« На стыке биомедицины и других передовых направлений, таких как квантовые технологии и искусственный интеллект сегодня создаются как новые исследовательские направления, так и прикладные разработки.

Сегодня многие квантовые разработки для медицинской сферы не только существуют в лабораториях, но и начинают выходить на рынок. Речь идет как о пилотных проектах в области квантовых вычислений в интересах крупных фармакологических компаний, так и, например, промышленных прототипах квантовых сенсоров для медицинской диагностики. Газпромбанк традиционно поддерживает научные исследования, технологические проекты и наукоемкие направления производства.

В 2023 году при поддержке Банка был создан «ЛИФТ Центр» (LIFT, Life Improvement by Future Technologies Center) — биомедицинский центр, в котором ведущие нейрофизиологи, медики, материаловеды, химики и физики России объединили свои усилия для реализации междисциплинарных исследований в области биомедицины, разработки лекарственных средств и медицинских изделий. Мы убеждены, что поддержка подобных инициатив значительно ускорит внедрение передовых решений в биомедицинскую сферу».



Дмитрий Владимирович Зауэрс
Заместитель Председателя Правления
Газпромбанка

« Потенциал квантовых технологий в целом и квантовых компьютеров в частности пока до конца не раскрыт, но однозначно они найдут свое применение в медицине.

Например, с помощью некоторых квантовых алгоритмов можно будет осуществлять моделирование динамики химических реакций, что, в свою очередь, даст возможность разрабатывать новые, более эффективные лекарственные средства. Хотя квантовые компьютеры с необходимой для таких задач производительностью еще не созданы, практически все крупнейшие фармкомпании уже экспериментируют в этом направлении. Проводятся интереснейшие исследования по моделированию динамики сворачивания белков — сложнейшей задачи биохимии, которая классическими вычислительными методами не решается. Среди других областей — новые методы диагностики и анализа медицинских изображений, моделирование распространения вируса, оптимизация логистики в больницах и многое другое. Если говорить про чувствительный мониторинг течения заболеваний мозга, то особо интересным направлением является магнитоэнцефалография, в которой главную роль играют высокочувствительные квантовые датчики магнитного поля. С помощью квантовых сенсоров можно измерять и визуализировать биомагнитные поля, что в перспективе позволит диагностировать опухоли головного мозга, эпилепсию и синдром Альцгеймера неинвазивно и с большей точностью, чем существующие методы, такие как ЭЭГ и МРТ. Пока отдельных национальных инициатив по применению квантовых технологий в сфере здравоохранения в России нет, но я надеюсь, что в ближайшее время с развитием этих технологий и повышением соответствующего интереса они появятся».



Руслан Рауфович Юнусов
Советник генерального директора
госкорпорации «Росатом»

«Применение квантовых технологий в медицине открывает уникальные возможности для преодоления сложных вызовов как в диагностике, так и в поиске новых методов инновационного лечения.

Здесь можно говорить и об использовании квантовых систем для более точного и раннего обнаружения заболеваний. К примеру, разработка квантовых сенсоров и маркеров для диагностики рака или других тяжелых заболеваний. К методам лечения, базирующимся на квантовых технологиях, можно отнести использование квантовых точек для доставки лекарственных препаратов в организм или разработку квантовых компьютерных моделей для эффективной оптимизации лекарственных препаратов. Применение квантовых вычислений для изучения генома и эпигенетики организма может помочь в понимании процессов развития заболеваний, индивидуализации лечения и создании персонализированной медицины. С точки зрения передовых инженерных разработок, также высокий интерес представляют различные биосистемы, например, такие как интерфейсы для связи нервной системы с искусственными устройствами и программно-аппаратные решения для защиты медицинских данных. Для Сеченовского Университета сотрудничество в этом направлении означает не только возможность применения фронтальных вычислительных технологий в своих исследованиях и разработках в области биомедицины, но и междисциплинарное взаимодействие с ведущими учёными в области квантовых технологий, позволяющее принципиально на ином уровне говорить о развитии отечественной медицины и фармацевтики».

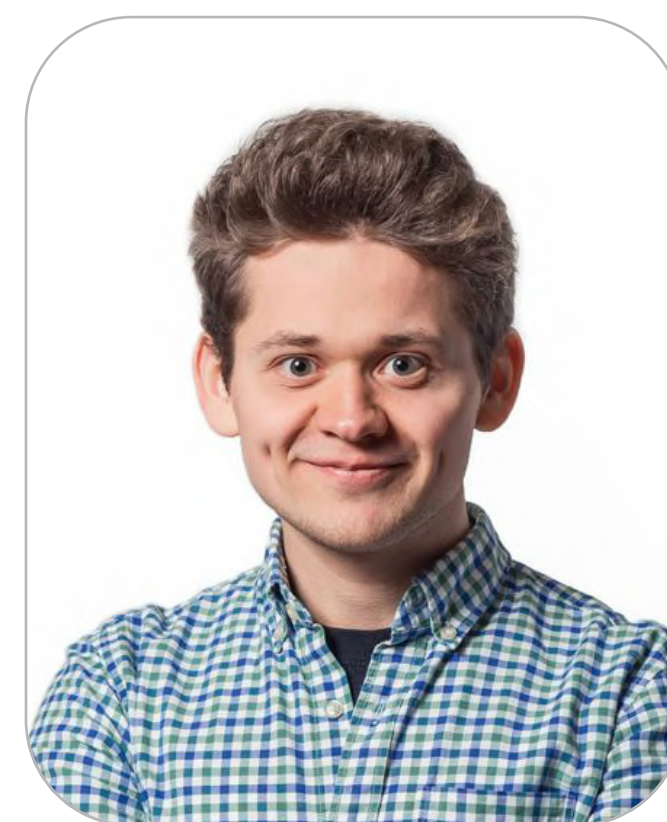


Пётр Витальевич Глыбочко
Ректор Сеченовского Университета
Минздрава РФ, академик РАН

«Квантовые технологии сегодня – одно из наиболее перспективных и бурно развивающихся научно-технологических направлений»

Разработки в области квантовых технологий – это сверхмощные квантовые компьютеры, защищенные коммуникации с использованием квантовой криптографии, а также высокоточные квантовые сенсоры.

Квантовые компьютеры уже сейчас начинают решать задачи, которые непосильны для классических суперкомпьютеров. Следующий шаг – полезное квантовое преимущество, которые в ряде задач могут обеспечить квантовые технологии. Одна из перспективных сфер применения квантовых технологий – биомедицина. Приложения, например, квантовых компьютеров могут быть очень разнообразны: от ускорения анализа медицинских изображений до полноценного моделирования новых лекарств. Квантово-устойчивые технологии защиты информации актуальны в связи с постоянно возрастающим объемом цифровых коммуникаций в медицинской сфере. Наконец, квантовые сенсоры – инструмент для создания как новых технологий диагностики, так и лечения. В этом отчете дан обзор наиболее интересных кейсов применения квантовых технологий в биомедицинской сфере».



Алексей Константинович Федоров
Руководитель научной группы
«Квантовые информационные технологии»
Российского квантового центра, директор
Института физики и квантовой инженерии
Университета «МИСИС»



Квантовые технологии

Квантовые вычисления

Использование свойств индивидуальных квантовых систем для решения сложных вычислительных задач:

- создание новых лекарственных препаратов;
- ускорение сборки и анализа генома (включая задачи нахождения последовательностей кодонов в гене);
- квантовое машинное обучение в медицине (включая задачи открытия новых биомаркеров и задачи классификации, повышение точности диагностики заболеваний и задачи эпидемиологического прогнозирования);
- моделирование биологических систем.

Квантово-устойчивые решения кибербезопасности

Надежная защита медицинских и генетических данных от атак настоящего и будущего. Технологии квантовых коммуникаций и постквантовые алгоритмы можно использовать для комплексной защиты данных на различных уровнях информационных систем:

- телемедицина (протоколы, используемые для защиты трафика видеоконференций);
- инфраструктура интернета вещей (шлюзы интернета вещей, сервисы доступа к клиентским данным и внутренняя инфраструктура, контроль целостности передаваемых обновлений программного обеспечения носимых устройств);
- цифровые сервисы хранения и передачи генетических и других данных (каналы связи, аутентификация и блокчейн-сервисы).



Квантовые сенсоры

Принципиально новые устройства, использующие для измерения физических величин свойства квантовых систем, такие как особенности энергетических уровней в атомах, квантовая когерентность, квантовая запутанность, квантовая интерференция и сжатие квантового состояния. Использование квантовых состояний приводит к гораздо более высокой чувствительности квантовых датчиков относительно классических, вплоть до возможности измерения минимально возможных отклонений измеряемой величины:

- диагностика на клеточном и молекулярном уровнях;
- магнитоэнцефалография и магнитокардиография;
- адресная доставка лекарств.

Квантовые технологии являются одними из ключевых в обеспечении цифрового суверенитета России и уже входят в концепцию нового нацпроекта «Экономика данных». Развитием квантовых технологий активно занимаются ведущие ВУЗы, институты развития, крупнейшие промышленные компании, такие как Банк ГПБ (АО) и ГК «Росатом», а также стартапы Куборд, QApp, QRate и QLU.

Достижения в области квантовых технологий были представлены на Форуме будущих технологий-2023 первым лицам государства.



Квантовые вычисления

Технология

Современная эпоха информационных технологий привела к стремительному развитию компьютерных наук и вычислительной техники. В этом контексте квантовые вычисления представляют собой новаторскую область, которая имеет потенциал изменить общепринятые принципы обработки информации и решения сложнейших вычислительных задач. Квантовые вычислительные устройства основаны на особых принципах квантовой механики, где кубиты (от англ. quantum bit), единицы квантовой информации, могут находиться в суперпозиции основных состояний (нуля и единицы) благодаря явлению квантовой суперпозиции. А явление квантовой запутанности позволяет создавать и обрабатывать сложные состояния из нескольких кубит. **Мощности современных суперкомпьютеров позволяют эмулировать квантовые компьютеры размером до 50-60 кубит, при этом отдельные квантовые компьютеры состоят уже из более чем 1000 кубит.**

Потенциал квантовых вычислений в медицине особенно важен, поскольку этот сектор нуждается в обработке больших объемов данных, анализе сложных систем и моделировании биохимических процессов. В медицинской практике присутствуют множественные задачи, начиная от диагностики и лечения заболеваний до разработки новых лекарств и персонализированной медицины, где квантовые вычисления могут принести значительные выгоды.

Развитие квантовых вычислений ведется одновременно по нескольким основным направлениям:

Разработка квантовых вычислительных устройств и их программных эмуляторов

Создание квантовых алгоритмов

Адаптация существующей ИТ-инфраструктуры для обеспечения доступа к квантовым вычислительным устройствам, включая разработку облачных интерфейсов доступа

Построение квантового компьютера является сложной научной и инженерной задачей. В классических вычислительных устройствах уже несколько десятилетий в качестве основы для компонентной базы используются транзисторы на основе кремния. Для реализации квантовых компьютеров пока не выбраны основные технологии. Однако большой ряд существующих квантовых вычислительных устройств позволяет выделить наиболее перспективные технологии для реализации кубитов. Среди них: сверхпроводниковые цепи, ионы, холодные атомы и кубиты на основе фотонов.

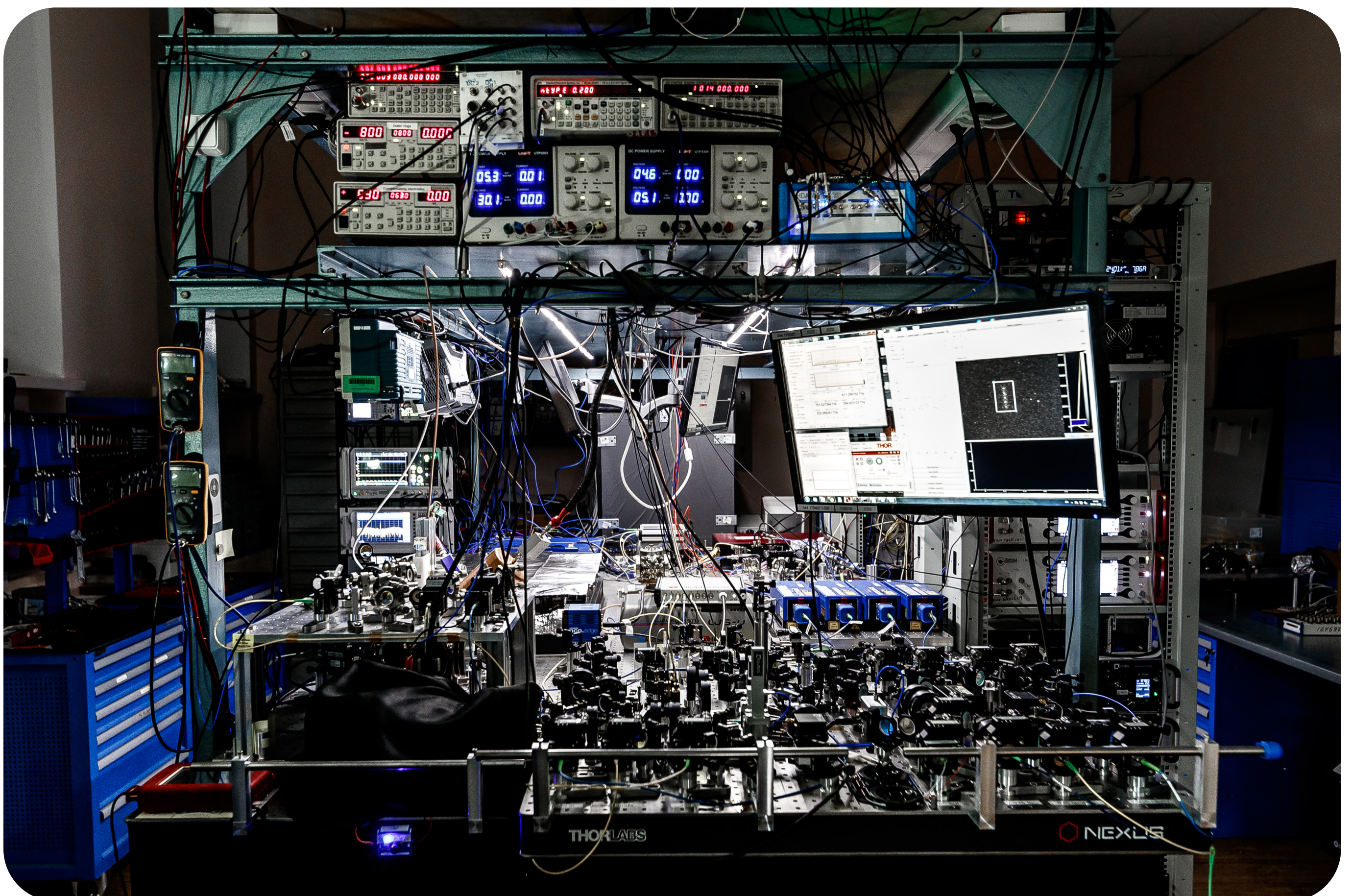
Современные квантовые компьютеры

Универсальные квантовые компьютеры

способны выполнять разнообразные квантовые операции. Они предназначены для решения разнообразных задач, включая квантовые алгоритмы поиска, факторизации, оптимизации и моделирования, а также для обработки обширных объемов данных.

Узкоспециализированные квантовые компьютеры

Например, квантовые симуляторы, устройства квантового отжига. Специализируются на решении конкретных классов задач. Зачастую, такие квантовые системы могут иметь ограниченный набор логических операций. Узкоспециализированные компьютеры могут быть разработаны для конкретных применений, таких как решение задач дискретной оптимизации или моделирование химических структур.



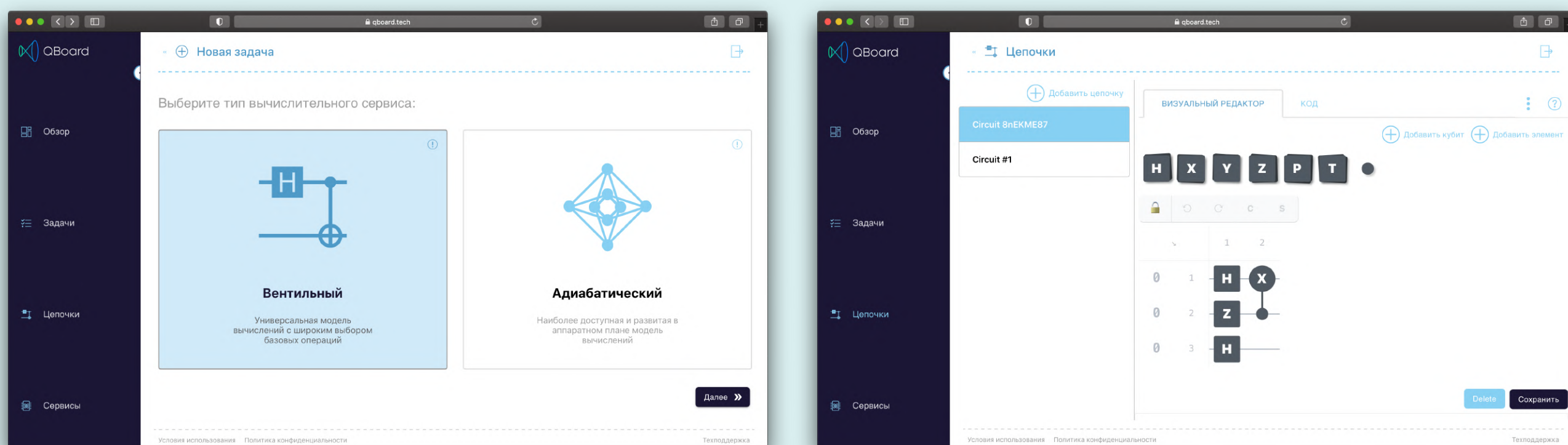
↑ Первые экспериментальные версии отечественных квантовых компьютеров уже функционируют



Эмуляторы квантовых вычислений

Программные эмуляторы квантовых вычислений могут до определенного предела имитировать работу квантовых компьютеров, используя классические вычислительные ресурсы. Эмуляторы обычно предоставляют пользователю интерфейс для создания квантовых алгоритмов, математического моделирования запуска квантового компьютера и анализа результатов.

Программные эмуляторы квантовых компьютеров могут быть полезны при разработке новых алгоритмов, проверки их работоспособности на различных входных данных, а также при обучении специалистов в области квантовых вычислений. А отдельные типы эмуляторов могут быть использованы в качестве метода решения практических задач дискретной оптимизации. В отдельных классах задач программные эмуляторы квантовых компьютеров превосходят по точности и скорости работы классические оптимизационные пакеты при решении практических задач.



Современные отечественные облачные платформы квантовых вычислений уже позволяют специалистам по работе с медицинскими данными выполнять проекты квантовых вычислений, используя low-code подход

Облачные платформы квантовых вычислений представляют собой единый интерфейс удаленного доступа пользователей к квантовым компьютерам и программным эмуляторам, а также средства, упрощающие процесс тестирования квантовых приложений и прогнозирования бизнес-эффектов от их промышленного применения.

Применение в медицине

По мнению ученых, квантовые вычисления сыграют ключевую роль в таких областях, как открытие лекарств, молекулярный анализ и персонализированная медицина

По этой причине в мире начинают уже открываться специализированные медицинские центры, задачей которых является разработка и раннее внедрение квантовых вычислительных методов для здравоохранения.

2021 год

IBM и клиника Кливленда открыли совместный центр Discovery Accelerator для проведения исследований в области биологии и здравоохранении с использованием высокопроизводительных квантовых вычислений и технологий искусственного интеллекта.

2023 год

В Израиле появился квантовый центр для здравоохранения и наук о жизни, сооснователями которого стали компания NVIDIA, израильский стартап Classiq, а также расположенная в Тель-Авиве клиника Ихилон (Сураски) — одна из первых в мире, начавшая внедрение технологий искусственного интеллекта в медицине.



Создание лекарственных препаратов

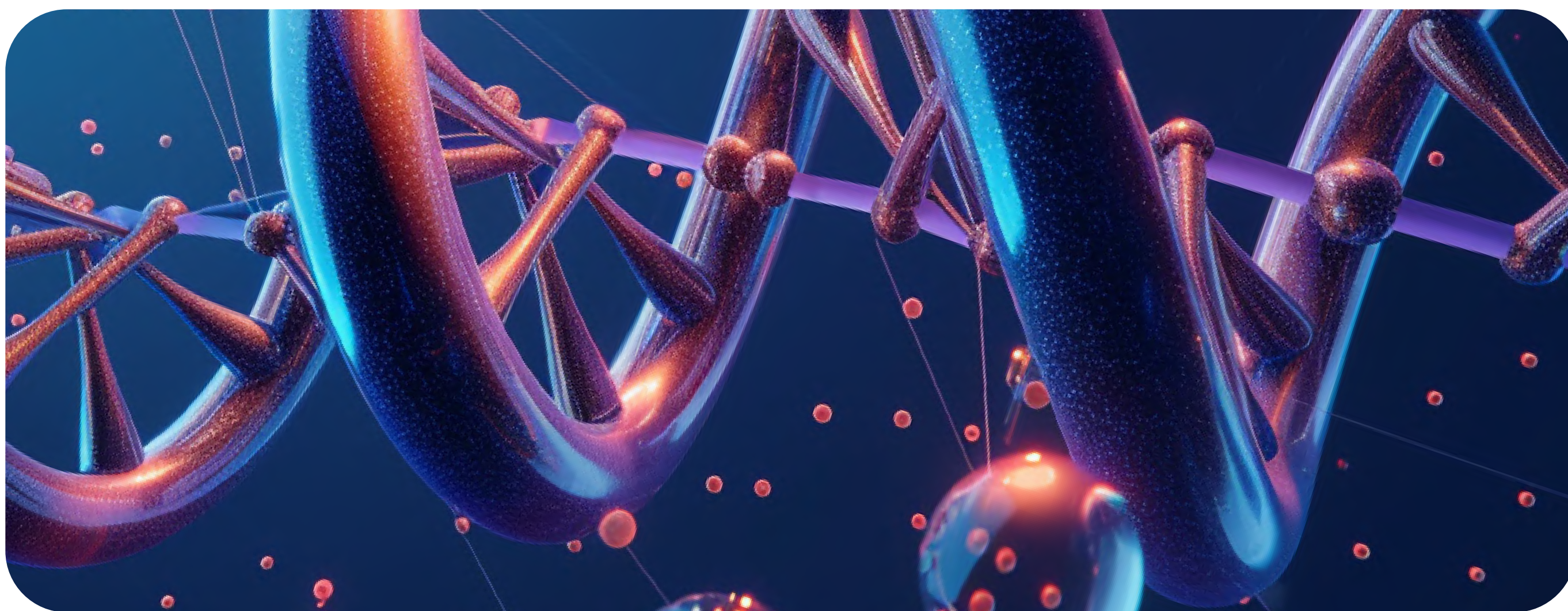
Область создания новых лекарств привлекает наибольшее количество гигантов рынка, в числе которых Moderna, Sanofi, AstraZeneca, JSR Life Sciences, Roche, немецкий фармацевтический гигант Boehringer Ingelheim и другие. Квантовые вычисления позволят более точно моделировать сложные химические структуры. Использование квантовых вычислений поможет ускорить процесс создания новых лекарственных препаратов. Уже сейчас разрабатываются подходы к применению квантовых аннилеров,

а также демонстрируется принципиальная возможность использовать текущее поколение квантовых компьютеров для решения практических задач в области медицины.

2023 год

IBM и Moderna работают над усовершенствованием мРНК-вакцин. Целью проекта является разработка оптимального материала для липидной оболочки, позволяющей доставить мРНК в целевую клетку. Для этого Moderna планирует использовать предобученную квантовую нейронную сеть IBM MoLFormer, которая умеет предсказывать физические свойства различных молекулярных комплексов по данным об их структуре.

Другие направления исследований в области квантовых вычислений направлены на прогнозирование положительных терапевтических эффектов и оценку побочных эффектов на ранних стадиях открытия медикаментов.



Генетика

Квантовые вычисления уже используются для сборки генома — метода восстановления последовательности структуры ДНК на основе коротких фрагментов генетической информации, полученных при секвенировании генома. Квантовые алгоритмы уже апробированы для сборки генома простейших бактериофагов. С ростом вычислительной мощности квантовых компьютеров разработанные алгоритмы будут применимы для анализа генома человека.

Отдельные фармацевтические компании уже начали экспериментировать с квантовыми вычислительными устройствами, решая задачи нахождения последовательностей генетического кода, называемых кодонами. Например, разработанная Российским квантовым центром, компанией Куборд и компанией Genotek методика сборки генома с использованием квантовых алгоритмов значительно облегчила изучение новых видов и структурных изменений ДНК, которые не удастся обнаружить методом классического картирования, и геномных перестроек в раковых клетках.

Опыт российских компаний

Разработана методика сборки генома с использованием квантовых алгоритмов



Квантовое машинное обучение в медицине

Потенциал квантового машинного обучения может быть использован для открытия новых биомаркеров для лечения рака. Ряд исследований в области квантового машинного обучения направлен на изучение генетических заболеваний — разработаны квантовые алгоритмы, которые могут классифицировать геномные данные многократно быстрее, чем обычный компьютер. Квантовые алгоритмы предложено использовать для повышения качества изображений, полученных методами медицинской визуализации, таких как компьютерная, магнитно-резонансная томография и рентгеновское сканирование.

2023 год

Компания QC Ware, специализирующаяся на квантовом программном обеспечении, сообщила о результатах совместного исследовательского проекта с Roche Pharma Research и INRIA CNRS — ведущими биотехнологическими компаниями.

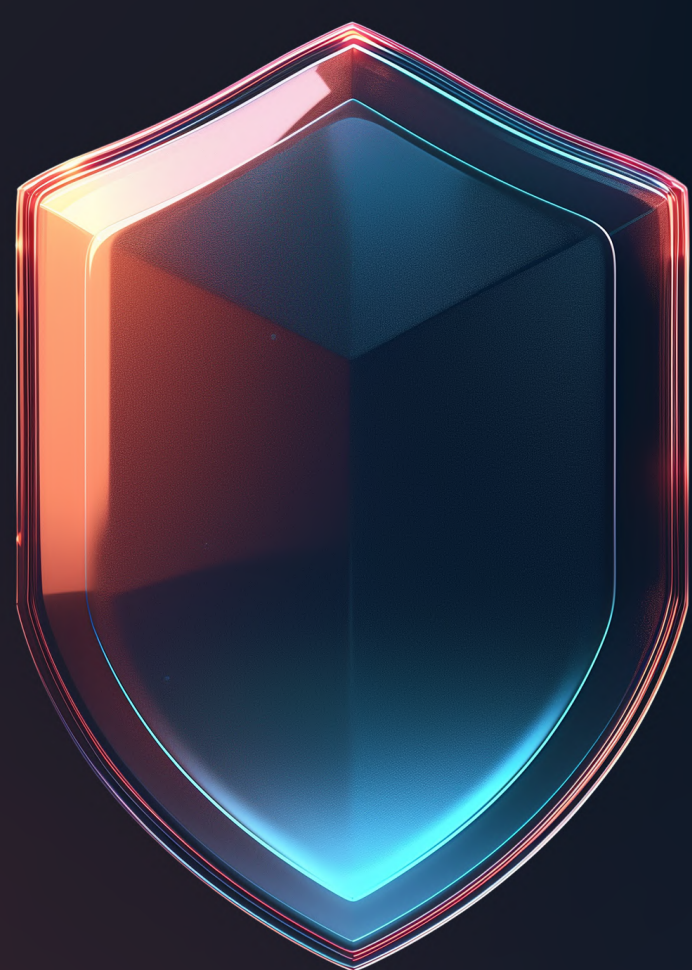
Изучались возможности квантового машинного обучения в задаче анализа медицинских изображений сетчатки глаза для выявления диабетической ретинопатии и определения её типа. Исследование проводилось с помощью программного эмулятора квантового компьютера, а также с использованием до 6 кубитов квантового компьютера IBM. Результаты показали, что квантовые алгоритмы машинного обучения оказались заметно эффективнее классических при анализе изображений с высоким разрешением.



Моделирование биологических систем

Квантовые компьютеры позволят проводить более точное и детальное моделирование биологических систем, включая биохимические процессы и молекулярные взаимодействия. Эти исследования позволят разработать более точные прогнозы эффективности лекарственных препаратов, предсказать развитие заболеваний и определить оптимальные методы лечения для каждого конкретного пациента.

Квантово-устойчивая защита медицинских и генетических данных



Квантовая угроза

Это новый вызов информационной безопасности. Квантовая угроза связана с возможностью получения злоумышленником доступа к зашифрованным традиционными методами данным в результате проведения кибератаки с применением квантового компьютера.

Новые поколения вычислительных устройств – мощные квантовые компьютеры – за счет принципиально новых принципов обработки информации смогут взломать существующие методы защиты информации.

В перспективе нескольких лет полностью небезопасными становятся многие традиционные алгоритмы:

Распределение ключей
(ECDH, DH)

⚠ Небезопасно

Асимметричное
шифрование (RSA)

⚠ Небезопасно

Электронная подпись
(ECDSA, DSA, ГОСТ Р
34.10-2012)

⚠ Небезопасно

Технологии квантовых коммуникаций (квантового распределения ключей) и постквантовые алгоритмы позволяют надежно защитить данные от атак с применением как классических, так и квантовых компьютеров

✔ **Безопасно**

Квантовые коммуникации

Технология

Квантовые коммуникации — это технология кодирования, передачи и приема квантовой информации.

Один из видов квантовых коммуникаций, квантовое распределение ключей, — метод распределения симметричных ключей между узлами сети связи, использующий квантовые явления. Данный метод позволяет гарантировать быструю и безопасную передачу симметричного криптографического ключа между абонентами, что дает возможность решить широко известную проблему распределения симметричного ключа — одну из центральных проблем в криптографии. Использование квантового криптографического ключа, полученного таким образом, повышает криптостойкость классических методов шифрования

и автоматизирует процесс распределения ключей, исключая человеческий фактор. Различные методы распределения квантовых ключей в совокупности с классическими криптографическими алгоритмами часто называют «квантовая криптография».

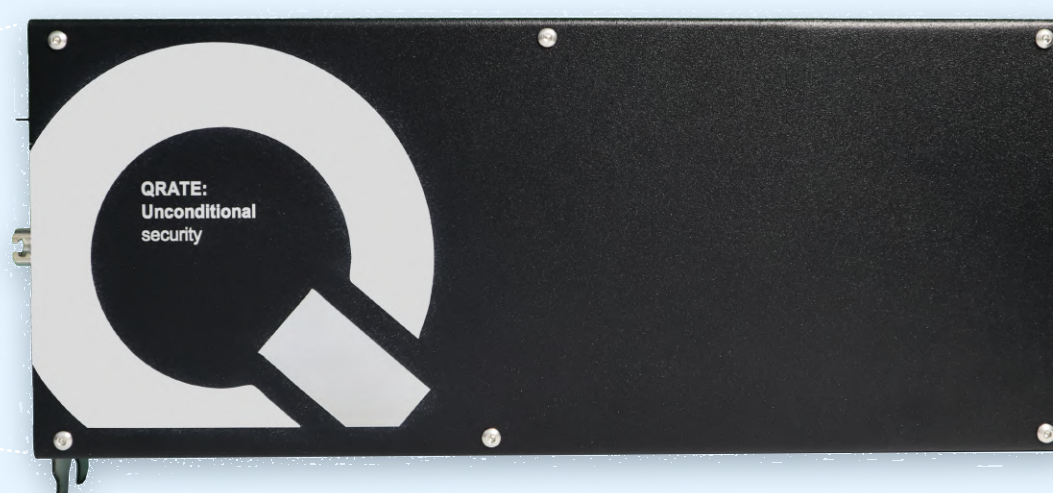
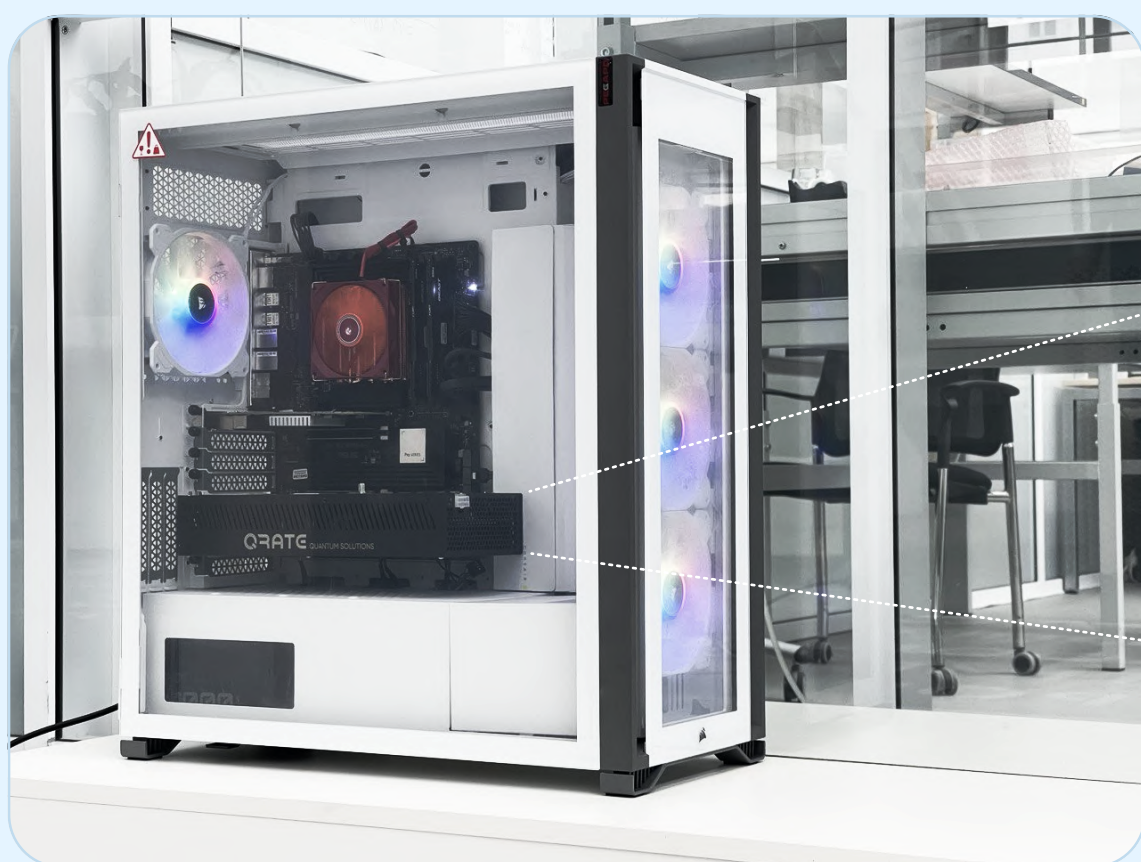
В современных условиях появление мощных персональных вычислителей, методов искусственного интеллекта, передовых математических алгоритмов не только упростило получение доступа к чувствительной информации, как для отдельных людей, так и для больших организаций. Это также создает существенную угрозу растущему интернету вещей, на базе которого функционирует всё больше промышленных, промышленных и государственных предприятий. В свою очередь развитие систем квантовых коммуникаций стало ответом на еще более серьезный вызов: создание квантовых вычислителей, которые способны взламывать многие современные алгоритмы шифрования.

Атака на данные с помощью квантовых компьютеров «Сохранение данных сейчас — взлом потом»



Одной из перспективных мер по надежной защите информации в свете возникающих угроз является использование систем квантового распределения ключей с использованием волоконно-оптических линий связи. Использование выработанного таким образом квантового криптографического ключа в совокупности с шифром «одноразовый блокнот» (шифр Вернама) может обеспечить информационно-теоретическую стойкость.

Системы квантового распределения ключей позволяют полностью исключить возможность перехвата ключа на стадии передачи, а также исключить влияние человеческого фактора из процедуры управления ключами. Ключ создается на основе данных истинно случайного генератора случайных чисел и является неизвестным ни одному из администраторов.



Отечественные миниатюрные решения квантового распределения ключей позволят доставлять ключ до конечных пользователей

Системы квантового распределения ключей могут применяться с традиционными системами криптографической защиты информации, используемых для обеспечения безопасности сетевой инфраструктуры, где позволяет вырабатывать и распределять ключи с помощью принципов квантовой физики, сильно снижая человеческий фактор.

Например, в рамках проекта ЕС OpenQKD, совместными усилиями Медицинского университета Граца (Австрия), компании FragmentiX и ее партнерам удалось успешно реализовать проект по использованию технологий квантовых коммуникаций для защиты цифровых медицинских снимков и генетических данных.

Применение в медицине

Многие технические устройства, используемые в медицине, производящие мониторинг и влияющие на функциональные жизненные показатели, в обозримом будущем будут представлять из себя единое сетевое интерфейсное окружение, определяющее себя как медицинский интернет вещей.

Стоит отметить также, что несмотря на развитую базу в области регулирования средств защиты информации (в том числе криптографических), сохраняется тенденция к наделению особым статусом и выделению в отдельную категорию с присвоением собственной классификации медицинским кибернетическим изделиям, имеющим возможность нанесения потенциального ущерба здоровью и безопасности пользователя.

Обоснование предложения происходит по причине различного жизненного цикла информационных управляющих систем и конечных исполнительных устройств. Данная тенденция четко прослеживается в современном информационно-технологическом кластере и демонстрирует большое количество обновлений программной составляющей аппаратно-программных комплексов за время жизненного цикла аппаратной составляющей изделия.

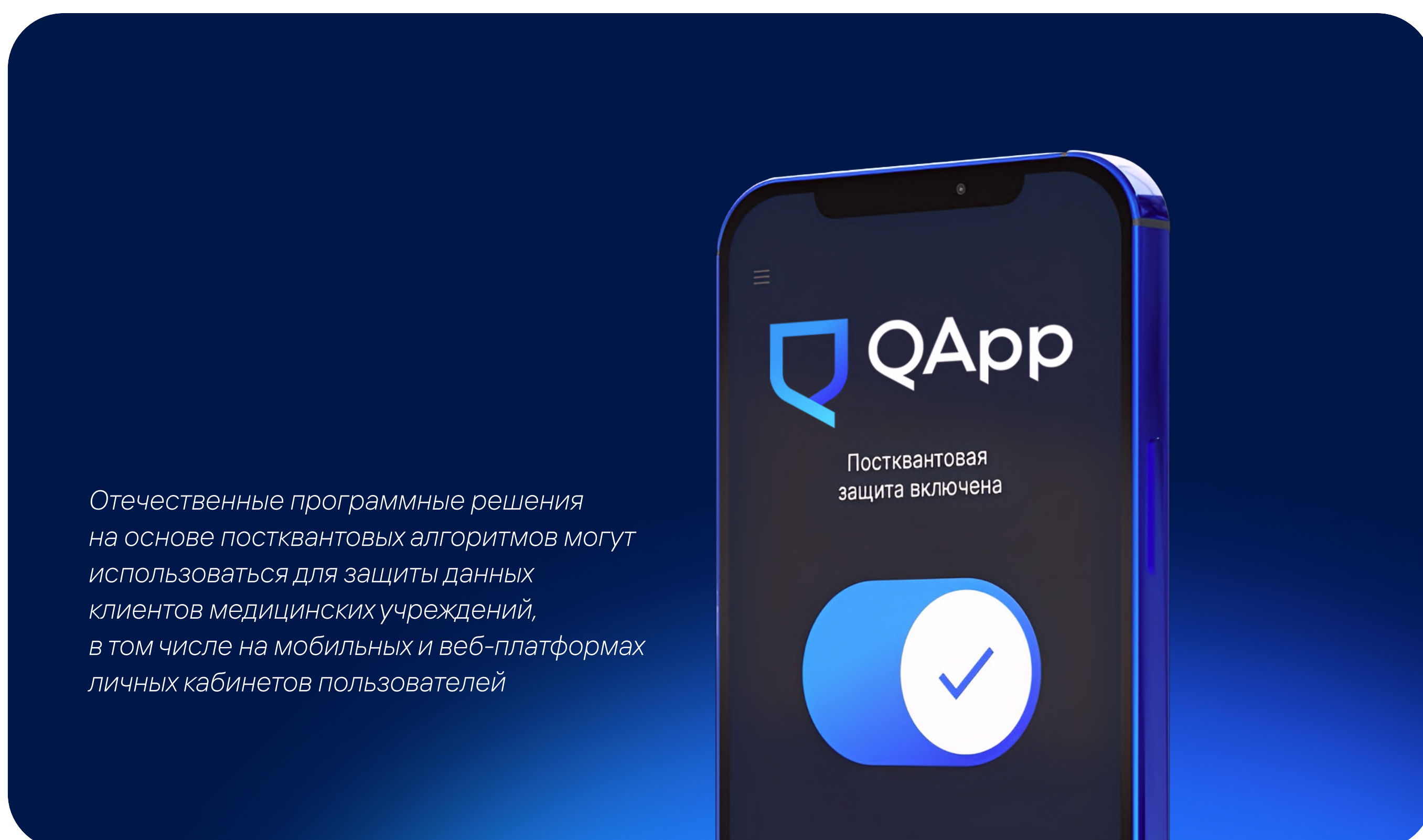
При всем этом, распределенные системы повсеместной цифровизации медицинских карт, содержащих сведения о пациенте, могут быть перехвачены и использованы злоумышленниками в корыстных целях. Совокупность всех факторов и угроз информационной безопасности делает перспективной применение систем квантовых коммуникаций в медицине.

Постквантовые алгоритмы

Технология

Постквантовые алгоритмы — новый класс криптографических алгоритмов, устойчивых к кибератакам с применением как классических, так и квантовых компьютеров. Постквантовые алгоритмы могут быть достаточно легко интегрированы в существующую инфраструктуру, например, мобильные приложения и веб-сервисы, а также инфраструктуру интернета вещей.

Программные решения на основе постквантовых алгоритмов не требуют привнесения новых специализированных аппаратных решений в инфраструктуру конечного бизнес-клиента, при этом некоторые параметры постквантовых алгоритмов могут быть ускорены на аппаратном уровне.



В России идет процесс разработки государственных стандартов для постквантовых алгоритмов, а компании различных индустрий активно тестируют программные решения. Например, Национальная платежная система МИР (НСПК), Газпромбанк, МЦСТ Эльбрус и другие компании уже имеют успешный опыт завершения научно-исследовательских и пилотных интеграционных проектов.

Применение в медицине

Промышленный и потребительский интернет вещей

Медицинские IoT-устройства позволяют врачам получать основные медицинские данные о пациентах, корректировать лечение и устанавливать дозировку удаленно. Наиболее распространенное применение IoT в медицине – удаленный мониторинг состояния здоровья пациента. IoT-устройства могут собирать такие показатели здоровья, как частота сердечных сокращений, артериальное давление, температура и т. д., от пациентов, которые физически не присутствуют в медицинском учреждении, что устраняет необходимость для пациентов ездить к поставщикам медицинских услуг или пациентам собирать их самостоятельно. Отдельное место в этом ряду занимают IoT-устройства, занимающиеся непрерывным измерением уровня глюкозы в крови больного сахарным диабетом. Такие устройства способны предупреждать пациентов/врачей о резком изменении уровня глюкозы.

К другим IoT-устройствам относятся приборы, отслеживающие частоту сердцебиения, «умные ингаляторы», позволяющие собирать данные о возбудителях приступов астмы, устройства, отслеживающие симптомы у больных болезнью Паркинсона, и многие другие. Чтобы максимально эффективно использовать IoT в здравоохранении, необходимо решить критические проблемы безопасности: конфиденциальность собираемых IoT-устройствами данных и обеспечение доступа к управлению этими устройствами только со стороны «доверенных» пользователей. Постквантовая криптография позволяет защитить IoT-устройства от квантовой угрозы.

Телемедицина

Телемедицина является одной из наиболее быстро растущих областей здравоохранения в мире. Одним из основных ее направлений являются телемедицинские консультации. Очевидно, что во время такой консультации существует риск раскрытия медицинских данных пациента, поэтому используемые каналы связи должны быть надежно защищены с помощью криптографических методов, часть из которых уязвимы к атакам с применением квантовых компьютеров. Таким образом, для обеспечения информационной безопасности телемедицины в условиях существования квантового компьютера необходимо внедрение постквантовых криптографических алгоритмов в протоколы, используемые для защиты трафика видеоконференций.

Защита генетических данных

Генетические данные должны подлежать особой защите, поэтому к вопросам безопасности используемых для этого криптографических алгоритмов необходимо подходить с особой тщательностью. Квантовая угроза не несет опасности в случае локального хранения генетических данных, однако ее нельзя вычеркивать из рассмотрения при рассмотрении случая защищенной передачи этих данных. В таком случае необходимо использование постквантовых алгоритмов для выработки общего криптографического ключа, который будет использоваться для шифрования генетических данных. Помимо этого постквантовая криптография дает новые возможности для исследований ДНК. Речь идет об использовании конфиденциальных вычислений, позволяющих сохранять в секрете данные, над которыми производятся вычисления.

Изучение последовательностей ДНК и РНК человека является важным для биологии и медицины. Некоторые исследования сложных заболеваний или вирусов требуют тысячи образцов ДНК для выявления закономерностей и получения достоверных результатов. Однако последовательности ДНК и РНК являются биометрическими идентификаторами человека, что делает их передачу в руки исследователей затруднительной. Таким образом, использование конфиденциальных вычислений позволят производить обработку/анализ генетических данных без их раскрытия. Конфиденциальные вычисления могут быть произведены с использованием постквантового гомоморфного шифрования.

Интеллектуальная собственность

Фармацевтические компании и компании, производящие медицинское оборудование, вкладывают значительные средства в исследования и разработки. Защита интеллектуальной собственности, связанной с разработкой лекарств и новых медицинских устройств, имеет ключевое значение в конкурентной борьбе.

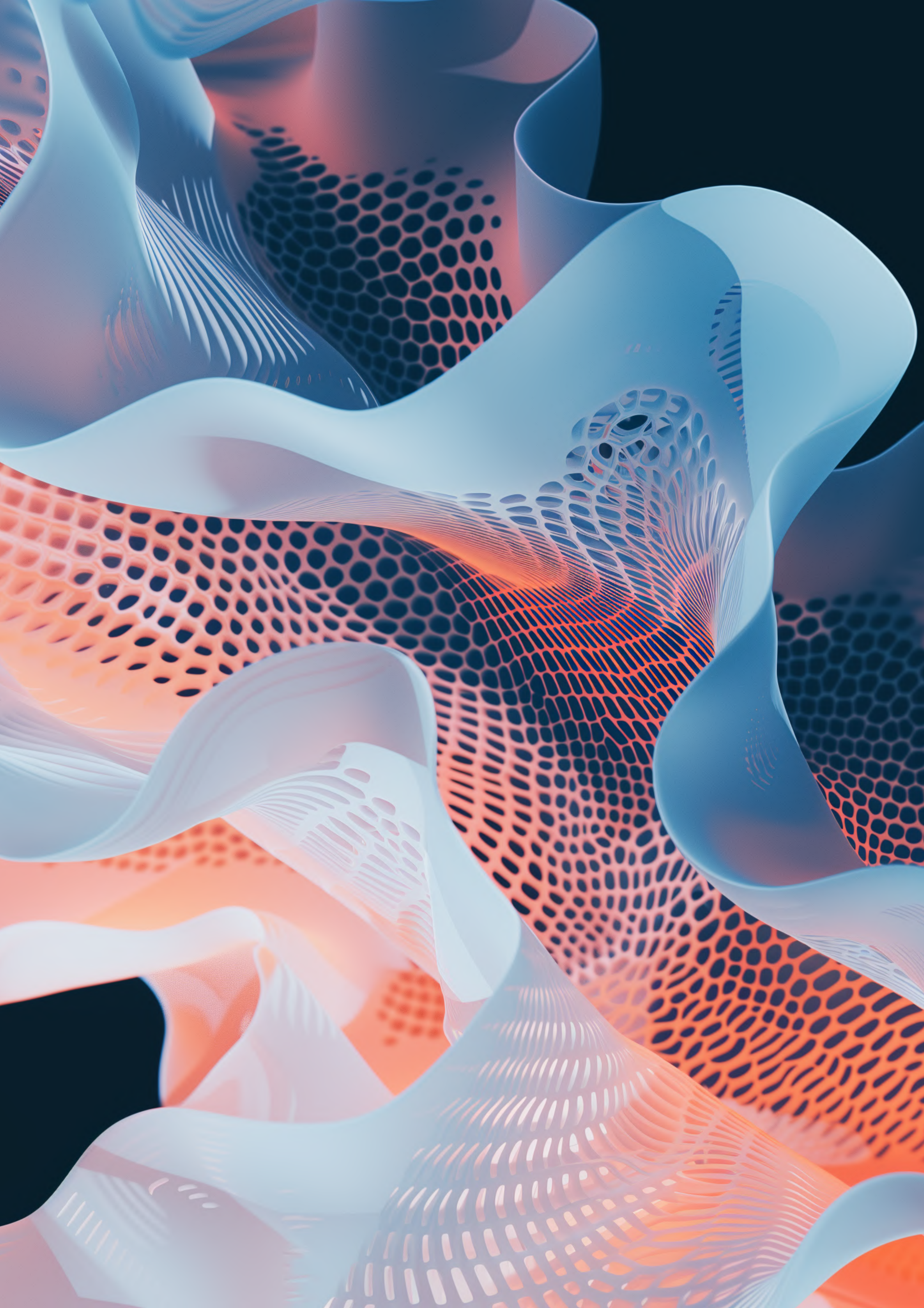
Эффективная защита медицинских данных

Практически любой медицинский сервис, использующий преимущество современных информационных технологий, начиная от облачных хранилищ и заканчивая медицинскими приложениями на различных устройствах, потенциально уязвим перед квантовой угрозой. Это связано с тем, что взаимодействие с сервисом сопряжено с выстраиванием безопасного канала связи. Некоторые криптографические примитивы, используемые при этом, могут быть взломаны с помощью квантового компьютера. Противостоять этому можно с помощью программных решений информационной безопасности на основе постквантовых алгоритмов шифрования.

Аппаратные решения на основе технологии квантовых коммуникаций и программные решения на основе постквантовых алгоритмов не противоречат друг другу и могут использоваться совместно для обеспечения комплексной защиты ИТ-инфраструктуры медицинской организации от атак настоящего и будущего.

Квантовые коммуникации и постквантовые алгоритмы — надежная защита медицинских данных от квантовой угрозы на всех уровнях

		Квантовые коммуникации	Постквантовые алгоритмы
Платформы	Комплексные ИТ-системы	✓	✓
Дата-центры	Критическая инфраструктура	✓	✓
Инфраструктура	Каналы коммуникации	✓	✓
Приложения	Мобайл, Веб, Десктоп, IoT		✓





Квантовые сенсоры

Технология

Сегодня прогресс в биомедицинских науках зачастую стимулируется разработкой новых инструментов с улучшенной чувствительностью и разрешающей способностью, благодаря которым становится возможным обнаружение слабых биологических сигналов.

Постепенные улучшения в ставших уже классическими методах диагностики (КТ, МРТ, ПЭТ) привели к огромному прогрессу в здравоохранении, но дальнейшее повышение чувствительности и разрешающей способности этих методов кажется сложным (а иногда и невозможным) с использованием стандартных подходов. Наиболее многообещающим направлением для нового поколения медицинской техники, основанной на более чувствительных измерительных системах, является область квантовой сенсорики.

Квантовые сенсоры – это принципиально новые устройства, использующие для измерения физических величин свойства квантовых систем, такие как особенности энергетических уровней в атомах, квантовая когерентность, квантовая запутанность, квантовая интерференция и сжатие квантового состояния. Использование квантовых состояний приводит к гораздо более высокой чувствительности квантовых датчиков относительно классических, вплоть до возможности измерения минимально возможных отклонений измеряемой величины. До недавнего времени квантовые сенсоры были представлены в основном в лабораториях, однако на сегодняшний день происходит их значительный трансфер из науки в индустрию, в частности, в медицину.

Применение в медицине

Диагностика на клеточном и молекулярном уровнях

Некоторые квантовые датчики (например, основанные на азото-замещенных вакансиях в алмазе) могут быть размером с один атом и, как следствие, обладают непревзойденной пространственной разрешающей способностью. Такие микроразмерные квантовые сенсоры могут использоваться для мониторинга биологических процессов внутри клеток, минимизируя воздействие на их работу за счёт своего размера. Их чувствительность и размер позволяют регистрировать температуру и магнитные поля отдельных клеток, что в свою очередь, может помочь в изучении метаболизма и исследовании электрической активности отдельных нейронов.

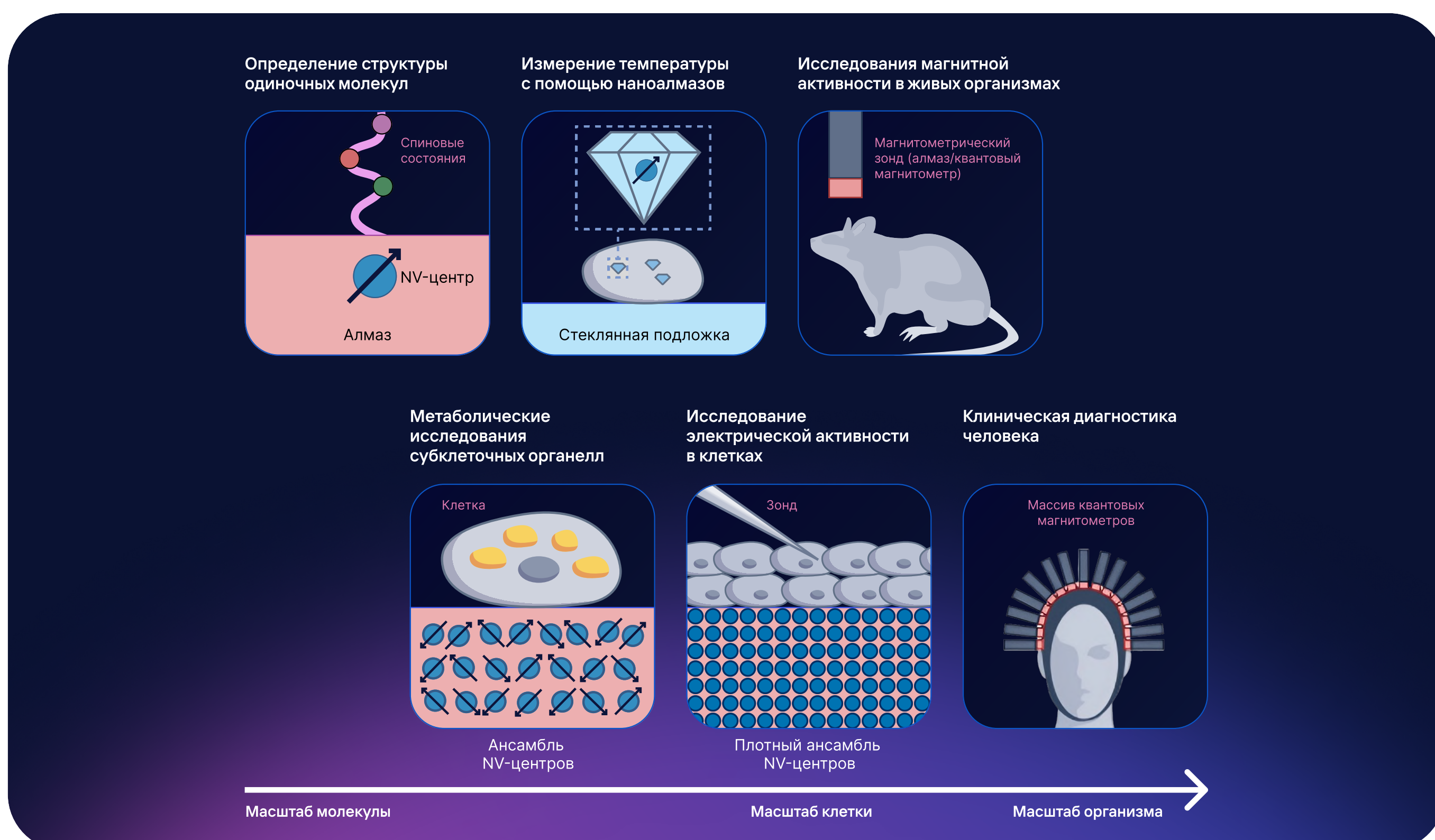
К примеру, недавнее исследование датских ученых показывает, что высокочувствительные датчики, использующие азотные центры окраски в алмазе, позволяют регистрировать слабое магнитное поле, индуцируемое ионными токами в аксонах мозолистого тела мозга мыши и так восстанавливать сигналы от распространения «потенциала действия» нейронов. Алмазные датчики позволяют измерять сигналы нервных клеток без повреждения ткани и с большой чувствительностью. Такой подход сделает возможным более точное изучение изменений, происходящих на самых ранних стадиях нейродегенеративных заболеваний, и поможет развитию новых методов их лечения.

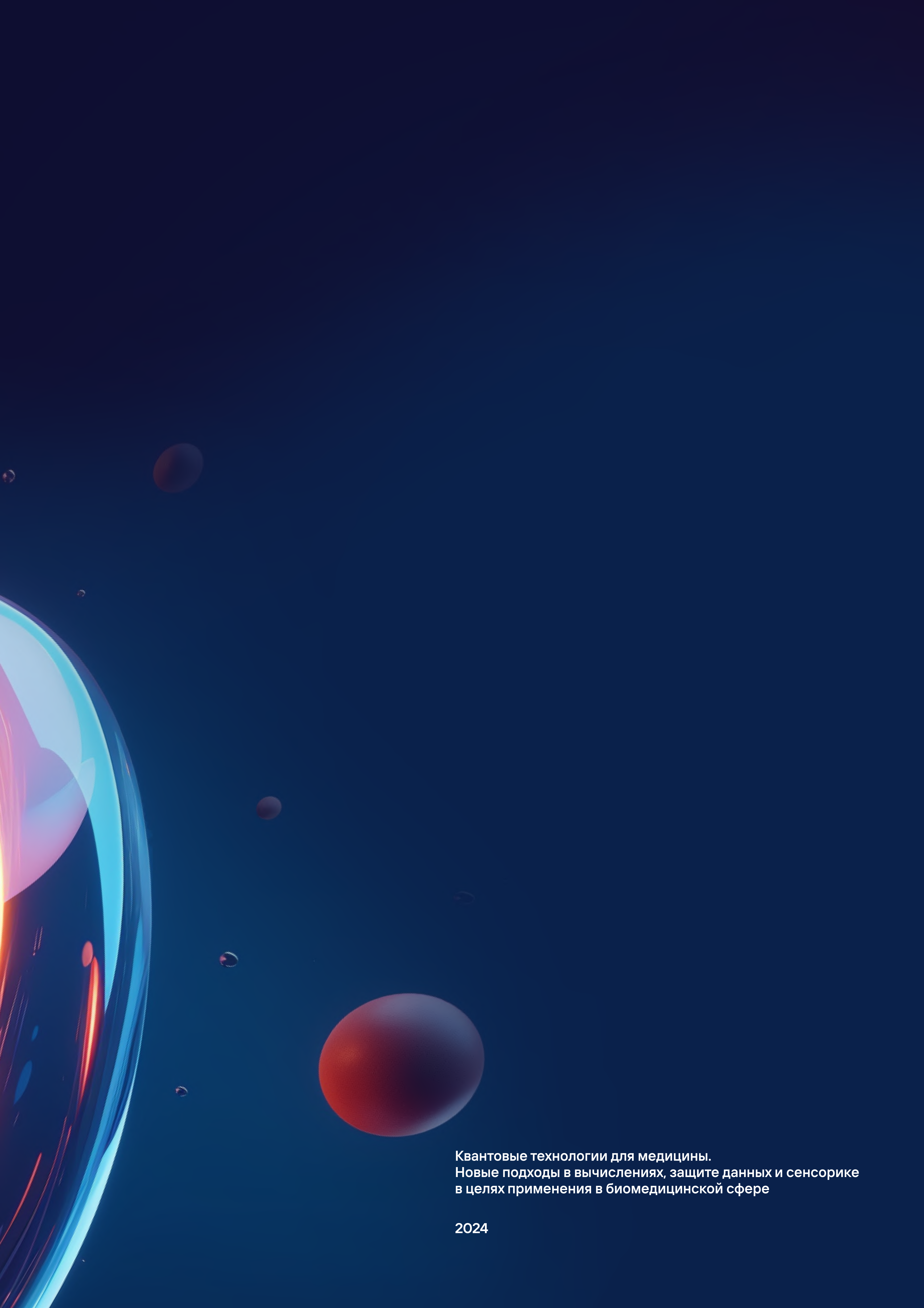
Магнитоэнцефалография

Квантовые магнитометры активно применяются в медицине для магнитоэнцефалографии (МЭГ), метода, основанного на регистрации магнитной компоненты электромагнитного излучения нейронов. В отличие от электроэнцефалографии, МЭГ имеет очень высокое временное и пространственное разрешение, что позволяет с более высокой точностью обнаруживать и локализовывать эпилептогенные зоны, а также помогать в выявлении на ранней стадии таких комплексных заболеваний, как шизофрения, аутизм, болезнь Альцгеймера и другие.

Адресная доставка лекарств

Ещё одной областью, где могут использоваться квантовые сенсоры, является адресная доставка лекарств. Это стратегия, при которой медикаменты доставляются прямо к определенной ячейке или ткани в организме, минимизируя воздействие на здоровые клетки. Такой метод позволяет снизить побочные эффекты лекарств и повысить их эффективность. Тераностика представляет собой симбиоз терапии и диагностики. Эта концепция предоставляет возможность одновременного определения и лечения заболевания. Например, носители для адресной доставки лекарств могут также включать в себя компоненты для визуализации, что позволяет отслеживать процесс лечения и оценивать его эффективность. Квантовые сенсоры могут решать проблемы с детектированием и визуализацией таких носителей.





Квантовые технологии для медицины.
Новые подходы в вычислениях, защите данных и сенсорике
в целях применения в биомедицинской сфере

2024