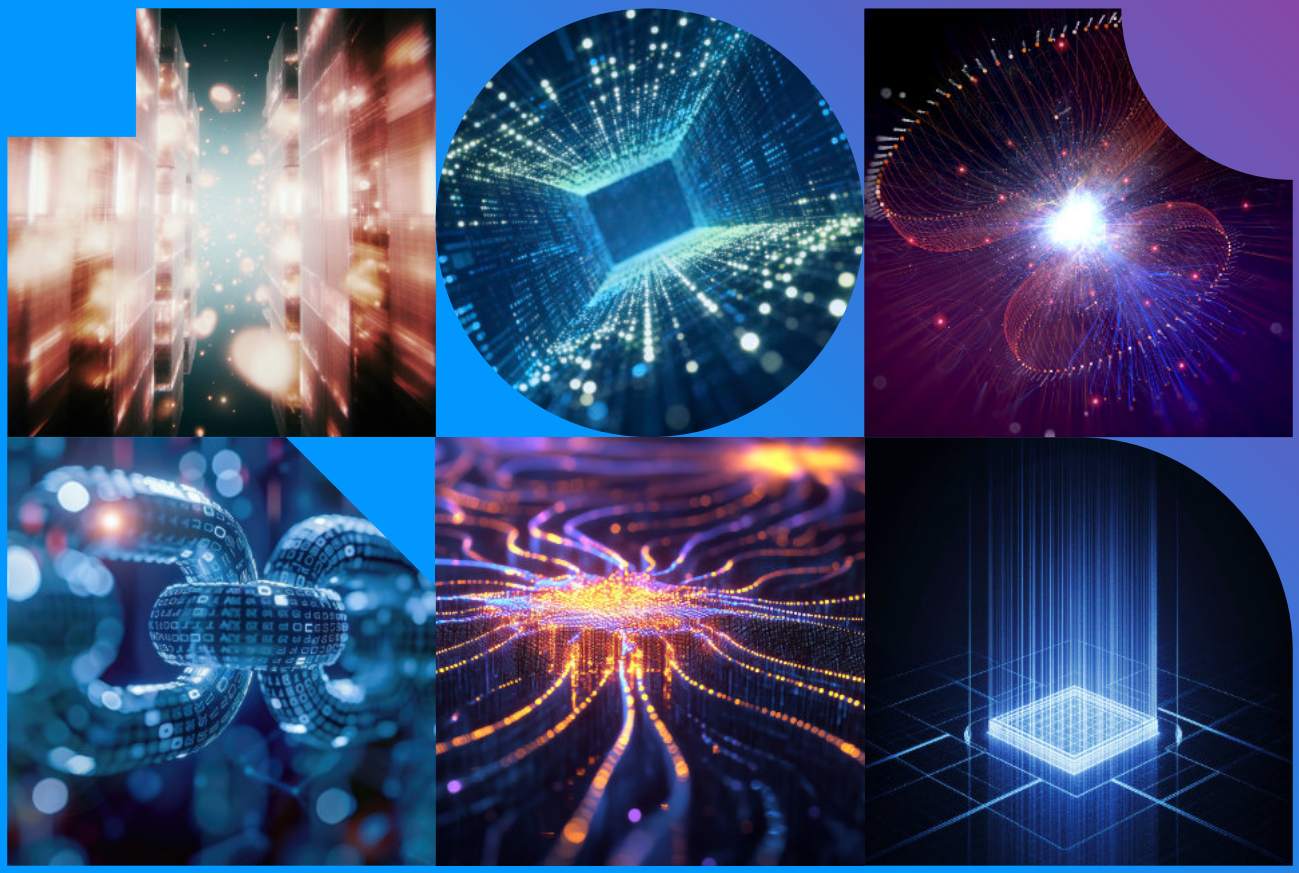
Перспективные сценарии применения квантовых и смежных технологий в сфере информационной безопасности



Ярослав Авдиев

Директор направления «Технологическое лидерство» АНО «Цифровая экономика»

Применение квантовых и смежных технологий открывает новые горизонты в обеспечении киберустойчивости цифровой инфраструктуры. В ближайшие годы квантовые технологии станут значимой точкой роста, а для их успешного развития и внедрения необходимо объединение усилий науки, бизнеса и государства.

В рамках деятельности Центра технологического лидерства 2030 АНО ЦЭ ведет активную работу с разработчиками, операторами и потенциальными заказчиками решений в области квантовых и смежных технологий в сфере информационной безопасности. В этом отчете мы представляем результаты анализа и практического применения решений, рекомендации по развитию квантовых и смежных технологий, а также эффекты от их внедрения. Сегодня крайне важно не только понимать потенциал этих решений, но и выстраивать системную стратегию их внедрения, чтобы обеспечить технологический суверенитет и безопасность цифрового пространства страны.

Дмитрий Зауэрс

Заместитель Председателя Правления АО «Газпромбанк»

С 2014 г. Газпромбанк поддерживает развитие квантовых технологий и первым в России среди финансовых организаций испытал средства квантовой криптографии и квантово-устойчивой защиты данных. Сегодня мы реализуем комплексный подход к применению квантовых и смежных технологий в информационной безопасности, сочетая пилотные проекты с практическими внедрениями в банковскую инфраструктуру и развивая новые виды защищенных каналов связи и криптозащиты.

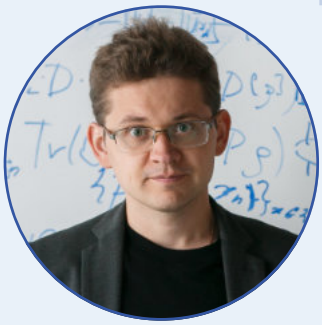
В данном исследовании представлены существующие решения, разработанные российскими компаниями, в том числе при участии Газпромбанка, которые применяются главным образом для создания новых, более надежных методов защиты информации и могут быть масштабированы для применения в различных отраслях.

Екатерина Солнцева

Директор по квантовым технологиям Госкорпорации «Росатом»

Как только стало понятно, что появление квантовых компьютеров – вопрос времени, весь мир сконцентрировался на очевидной угрозе для криптографии. Алгоритмы, запущенные на квантовых вычислителях большой мощности, потенциально смогут взломать используемые сегодня стандартные системы шифрования. Однако, мир справился с этим вызовом – нам уже понятно, как эти угрозы нивелировать с помощью квантового распределения ключей и постквантовой криптографии. А по мере развития квантовых технологий стало понятно, что они способны оказать прорывной эффект в развитии промышленности, медицины, логистики, финансов – принести колоссальную пользу экономикам мира. Поэтому сегодня перед бизнесом встал новый вызов – конкурентное преимущество будет у тех, кто раньше других научится извлекать пользу из квантовых технологий.

Ответственные компании уже начинают реализацию «плана квантовой готовности», включающего не только оценку будущих рисков и меры по их преодолению, но и прогнозирование квантовых возможностей и подготовку персонала к приходу промышленных квантовых компьютеров. В рамках дорожной карты развития квантовых вычислений «Росатом» совместно с партнерами содействует формированию в нашей стране суверенной научно-технологической экспертизы в этой области. Здесь мы видим общее поле работы с «Российскими железными дорогами», которые развивают квантовые коммуникации. В конечном итоге, наша общая цель – обеспечить применение квантовых технологий во всех ключевых отраслях российской экономики. Это одно из условий обеспечения будущего технологического суверенитета страны.



Алексей Федоров

Директор института физики и квантовой инженерии, Университет науки и технологий МИСИС

Квантовые технологии – это активно развивающееся направление, которое окажет существенное влияние на процессы обработки, передачи и защиты информации. Нами разрабатывается и пилотируется широкий спектр программных и программно-аппаратных решений для информационной безопасности на основе технологий квантового распределения ключей и постквантовой криптографии.

Внедрение технологий квантово-устойчивой защиты информации обусловлено рядом значимых факторов. Прежде всего, это растущая угроза атаки типа «сохрани сейчас – расшифруй потом», при которой злоумышленники уже сегодня собирают зашифрованные данные в расчёте на их расшифровку в будущем с помощью высокопроизводительных квантовых компьютеров. Во-вторых, необходимость адаптации квантово-устойчивых решений под реальные бизнес-требования, для обеспечения не только безопасности, но и практической применимости, совместимости и минимального влияния на текущие процессы.

Максим Острась

Генеральный директор
Российского квантового
центра

Текущий период в области квантовых технологий ознаменовывает существенный прогресс для отечественной квантовой индустрии. Происходит планомерное движение от исследования потенциальных возможностей к демонстрации практических результатов — от концептуальных разработок к экспериментальным образцам, а затем к продуктам, привлекающим внимание бизнеса. Сегодня главная цель состоит в ускорении и совершенствовании данного процесса трансформации. Гибридные квантово-классические алгоритмы, квантовая оптика, фотонные сенсоры, компоненты защищённой связи и многое другое — это уже не просто направления, это ростки новой технологической экономики, которая с каждым годом будет только расти.

Успех этой трансформации во многом зависит от готовности всех участников процесса — научных коллективов, инженеров, инвесторов и заказчиков — работать в едином ритме, понимая друг друга и выстраивая мосты между фундаментальной наукой и реальными потребностями рынка. Именно синергия компетенций, открытость к экспериментам и способность быстро адаптироваться к вызовам уже сегодня создают ту среду, в которой квантовые технологии становятся не просто амбициозным проектом, а естественной частью отечественной технологической повестки.

Партнеры отчета

минцифры_

ГАЗПРОМБАНК

РЖД

Ростелеком

РОСАТОМ

АСТРА

УНИВЕРСИТЕТ ИННОПОЛИС

РКЦ Российский Квантовый Центр

МФТИ

infotecs

QApp

ЦИР

СМАРТС КВАНТТЕЛЕКОМ

СПБ СИСТЕМЫ ПРАКТИЧЕСКОЙ БЕЗОПАСНОСТИ

S-Quantum

QRATE

КФТИ КазНЦ РАН

ИТМО

web3 tech

Сириус Научно-технологический университет

МТУСИ МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ

Казанский федеральный УНИВЕРСИТЕТ

CONSULTING

Оглавление

Введение

Цели и задачи отчета

Цель отчета

Способствовать продвижению и популяризации отечественных квантовых и смежных технологий и решений посредством:

- формирования отраслевой экспертизы по применению квантовых и смежных технологий в ИБ;
- серийного внедрения квантовых и смежных технологий в экономику;
- определения новых подходов к решению бизнес-задач и создания принципиально новых продуктов и услуг;
- заключения контрактов на решение бизнес-задач;
- содействия росту инвестиций в разработку и научные исследования по квантовым и смежным технологиям в сфере ИБ.

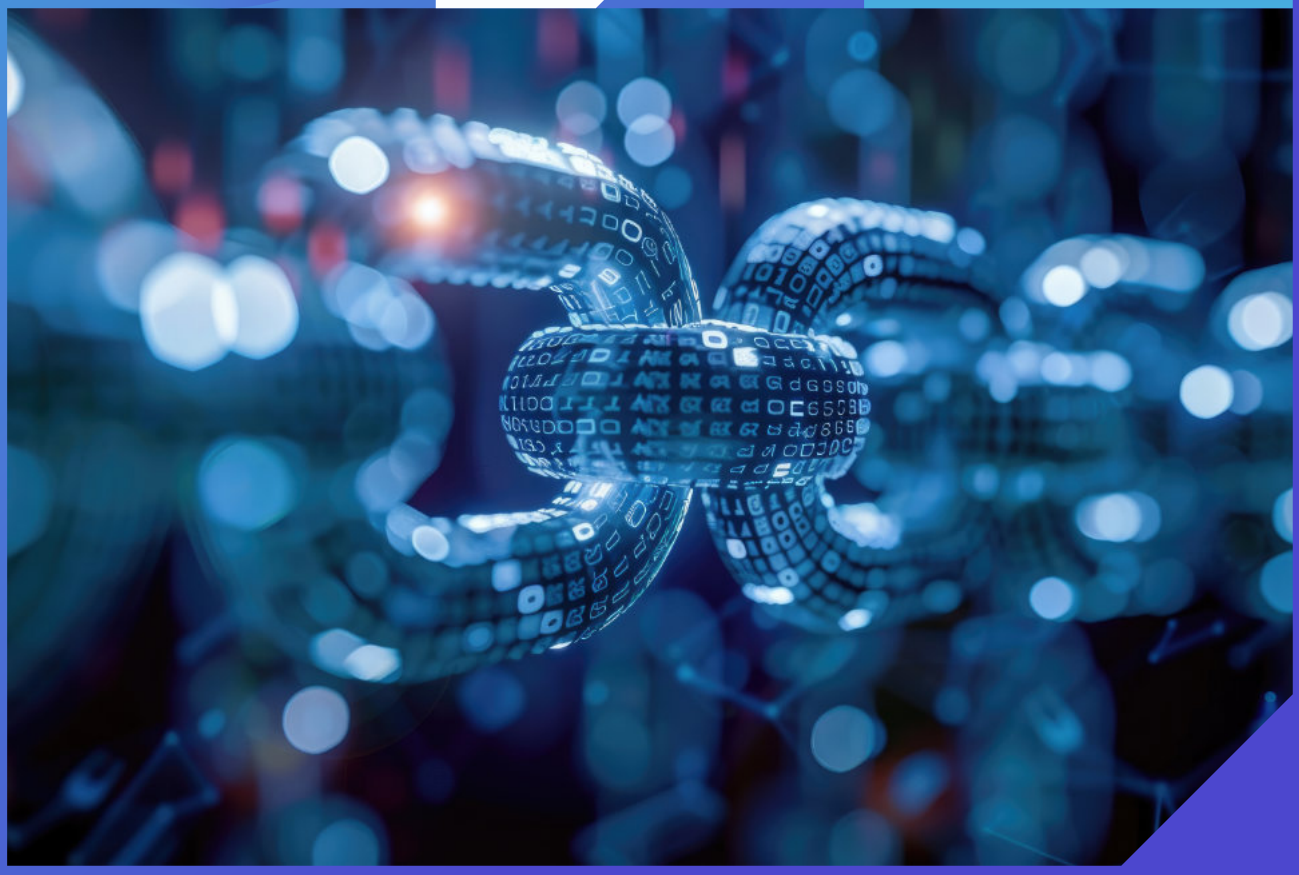
Задачи отчета

- Провести анализ российского и мирового опыта развития квантовых и смежных технологий в ИБ.
- Описать развитие системы ИБ с учетом применения квантовых и смежных технологий на уровне государства и организаций.
- Выявить тренды и сценарии применения квантовых и смежных технологий в сфере ИБ и описать барьеры.
- Проанализировать успешные кейсы и примеры пилотного применения квантовых и смежных технологий в сфере ИБ.
- Представить нормативно-правовую базу по квантовым и смежным технологиям.
- Описать экосистему развития квантовых и смежных технологий в России.

Целевая аудитория

- Компании — лидеры цифрового развития, предприятия различных отраслей экономики, заинтересованные в защите данных и готовые внедрять квантовые и смежные технологии.
- Федеральные органы исполнительной власти, главы субъектов РФ.
- Топ-менеджеры и эксперты в области информационной безопасности, квантовых и смежных технологий.
- Разработчики и заказчики решений в области квантовых и смежных технологий.
- Исследователи и представители академического сообщества, работающие на стыке ИБ, квантовых и смежных технологий.
- Широкий круг лиц, интересующихся развитием квантовых и смежных технологий и их применением.

Общая информация о развитии квантовых и смежных технологий в сфере ИБ



Обзор рынка и характеристика сферы информационной безопасности, вызовы и текущее состояние

Информационная безопасность (ИБ) Российской Федерации – состояние защищенности национальных интересов, при котором обеспечивается нейтрализация угроз информационной безопасности Российской Федерации[1].

Для чего нужна информационная безопасность

Информационная безопасность защищает системы от проникновения и от атак[2], что, в частности, обеспечивает стабильность государственных функций и поддерживает операционную эффективность бизнеса.

Чем информационная безопасность отличается от кибербезопасности

Информационная безопасность VS **Кибербезопасность**

Охватывает все виды защиты информации, независимо от формы (бумажной, устной, цифровой). Она связана с защитой информации во всех средах: цифровой, физической, организационной. Включает в себя кибербезопасность как компонент.

Представляет собой часть ИБ, фокусирующуюся на цифровом пространстве (данные и интернет-угрозы). Сосредоточена на цифровой информации и информационных системах, подключенных к сети (компьютеры, серверы, облака).

От каких угроз защищает ИБ

Внутренние

Угрозы, которые идут изнутри системы. Чаще всего в таких случаях речь идет об утечке данных или об их повреждении.

Внешние

Угрозы, которые приходят извне: попытка взлома системы через найденную уязвимость, DDoS-атака, вирусы.

72 %

компаний в мире утверждают, что за 2024 год возросло количество случаев кибермошенничества, фишинговых атак, а также краж личных данных, что стало главным киберриском для частных лиц[3].

Три принципа ИБ[4]

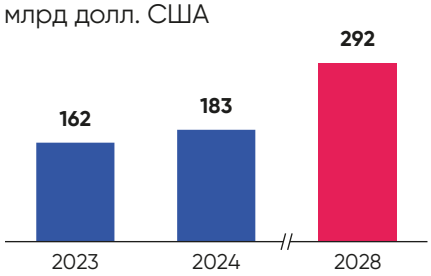
В каких сферах ИБ важнее всего

- Банки и финансы
- Дата-центры
- Государственные информационные системы
- Отрасли экономики
- Компании с большой Базой данных
- Электронная коммерция

[1] Проект новой реакции Доктрины информационной безопасности Российской Федерации.
[2] Защищает от взломов, DDoS-атак, в результате которых может и «лечь» сервер сайта, и произойти утечка данных.
[3] World Economic Forum Global Cybersecurity Outlook 2025.
[4] ГОСТ Р ИСО/МЭК 27001-2021.

Обзор рынка и характеристика сферы информационной безопасности, вызовы и текущее состояние

Объем мирового рынка ИБ[1], млрд долл. США



Основные драйверы роста мирового рынка ИБ:

Внедрение ИИ. Риски, связанные с использованием ИИ, потребуют от организаций инвестиций в безопасность приложений, в защиту данных и конфиденциальности, а также в защиту инфраструктуры.

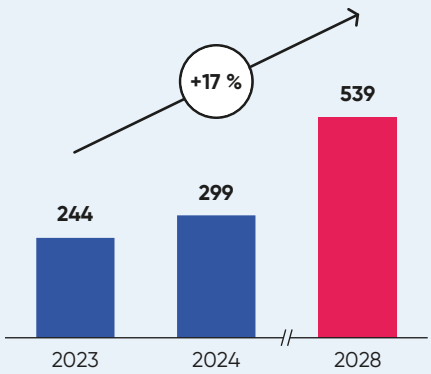
Внедрение облачных технологий. Будут способствовать росту сегментов программного обеспечения в области безопасности и сетевой безопасности предприятий.

Топ-10 стран по доле затрат на ИБ[2], 2024 год

183
млрд долл. США

- США (44 %)
- Китай (8 %)
- Великобритания (6 %)
- Япония (5 %)
- Германия (4 %)
- Франция (3 %)
- Австралия (2 %)
- Канада (2 %)
- Россия (2 %)
- Южная Корея (2 %)
- Прочие (22 %)

Объем российского рынка ИБ[3], млрд руб.



Основные драйверы роста российского рынка ИБ

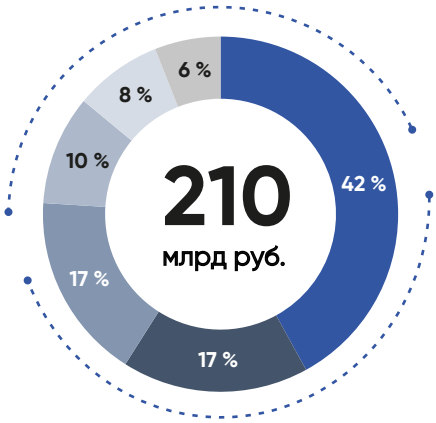
- Фокус на технологический суверенитет и развитие отечественных решений.
- Интеграция новых технологий для повышения устойчивости и защиты данных.
- Развитие стандартизации и появление новых требований, в том числе по защите персональных данных.
- Рост интенсивности[4] и изощренности кибератак.
- Увеличение количества киберпреступников.

[1] Gartner (2024, 2025).
[2] Forbes (2025), Б1 (2025).
[3] Б1 (2025).
[4] Вследствие, в частности, роста количества APT-атак (в т. ч. из недружественных стран) и роста количества инструментов атаки с ИИ.

Обзор рынка и характеристика сферы информационной безопасности, вызовы и текущее состояние

Структура российского рынка ИБ в 2024 году, % [3,4]

Структура российского рынка ИБ-продуктов в 2024 году, % [3]



- Сетевая и облачная безопасность
- Анализ, контроль, реагирование на угрозы ИБ
- Защита конечных точек
- Защита данных
- Управление доступом
- Управление рисками и навыками ИБ и пр.

В настоящее время все еще сохраняется зависимость от зарубежных ИБ-продуктов, особенно в сегменте «сетевая безопасность», который занимает наибольшую долю (свыше 40 %). Это создает стратегические риски, особенно для объектов КИИ[1], на которые приходится более половины ВВП страны.

294 млн руб. в среднем инвестировали в ИБ в 2025 году крупные российские компании. Это **на 29 % больше, чем в 2024 году**. В результате опроса среди более чем 100 крупных компаний России из разных отраслей выявлено:
89 % опрошенных компаний при разработке стратегии ИБ проводят анализ ключевых рисков в сфере ИБ, что показывает высокую степень зрелости в решении данной задачи[2].

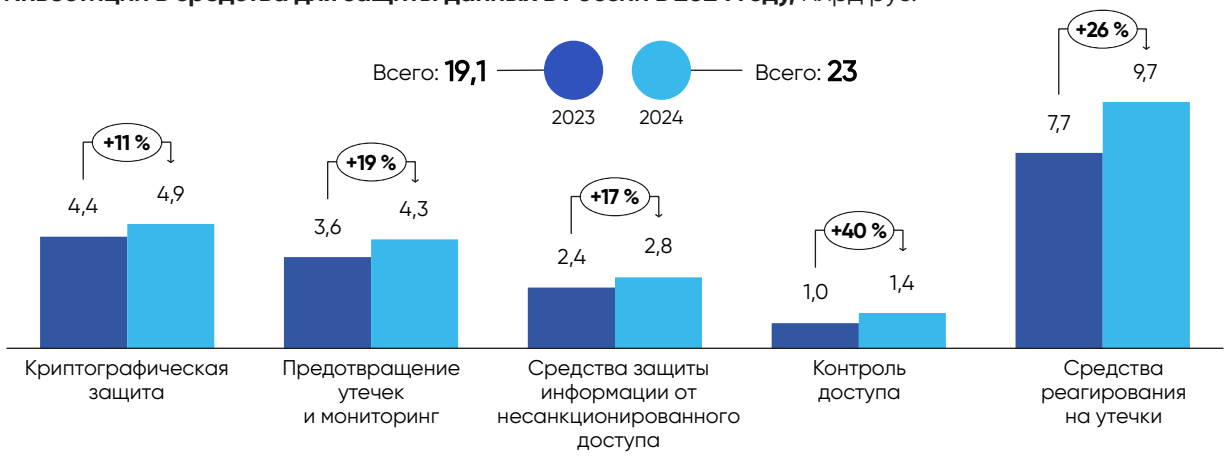
Тренды рынка ИБ-продуктов [3,4]

- Развитие экосистемных и платформенных решений в области ИБ
- Развитие и внедрение концепций Zero Trust[5]
- Встраивание ИИ в решения в области ИБ
- Развитие решений для обнаружения и реагирования на угрозы идентификации в B2B, B2C, B2B2C
- Повышение уровня совместимости отечественных ИТ и ИБ-решений
- Решения для безопасности подключенных устройств
- Информационная безопасность в архитектуре ИТ-решений
- Развитие ИБ-продуктов для облаков
- Обогащение данных об угрозах
- **Квантово-устойчивая защита информации**
  Развитие криптографии в эпоху квантовых вычислений

[1] Критическая информационная инфраструктура.
[2] Центр стратегических разработок (2025).
[3] Б1 (2025).
[4] Gartner (2023, 2024, 2025).
[5] Нулевое доверие.

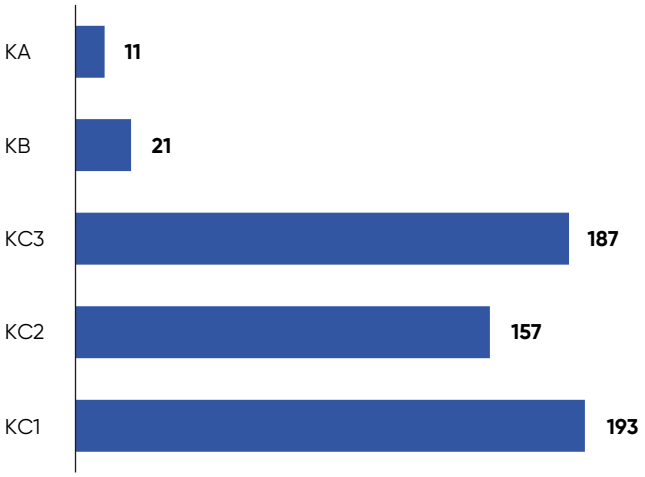
Обзор рынка и характеристика сферы информационной безопасности, вызовы и текущее состояние

Инвестиции в средства для защиты данных в России в 2024 году, млрд руб.[1]



Рост рынка объясняется увеличением спроса на решения по защите данных, обусловленного усиливающимися требованиями регуляторов. Это, в частности, штрафы до 500 млн руб. за повторную утечку персональной информации. Сегмент криптографии демонстрирует рост в связи с тем, что она является обязательной для госучреждений, банков и ряда других организаций.

Количество СКЗИ[2] в реестре ФСБ России на начало 2025 года, шт.[3]



Наиболее востребованными являются СКЗИ низких классов **(КС1, КС2 и КС3)**, так как более высокие классы, в соответствии с требованиями регулирующих органов, обязательны к применению для ограниченного числа специальных задач и объектов. **СКЗИ может обслуживаться организациями как самостоятельно, так и на основе сервисной модели, например, ГОСТ-VPN.**

В 2024 году затраты российских госорганов и госкорпораций на VPN составили 17,3 млрд руб. Это на 73 % больше по сравнению с 2023 годом, когда соответствующие расходы оценивались в 10 млрд руб. При этом количество тендеров увеличилось с 1413 до 14614. **Рост интереса** государственных структур к VPN **связан с необходимостью обеспечивать защиту данных и устойчивость ИТ-инфраструктуры** на фоне роста киберугроз.

[1] Информзащита (2025).
[2] Здесь и далее — средства криптографической защиты информации.
[3] Центр по лицензированию, сертификации и защите гостайны ФСБ России. Одно и то же СКЗИ может соответствовать сразу нескольким классам.
[4] Tadviser (2024).

Обзор рынка и характеристика сферы информационной безопасности, вызовы и текущее состояние

Появление квантовых технологий трансформирует сферу ИБ. Основная угроза заключается в способности квантового компьютера взламывать классические криптографические схемы — прежде всего, асимметричные алгоритмы, на которых строится инфраструктура электронной подписи, интернета вещей и инфраструктура открытых ключей. В то же время появляются новые средства защиты, такие как квантовое распределение ключей, в том числе устраняющие человеческий фактор.

Ключевые угрозы и вызовы, связанные с появлением квантовых технологий в сфере ИБ[1]

Взлом криптографии

Возможность взлома RSA (Rivest-Shamir-Adleman) — криптографического алгоритма с открытым ключом, а также других асимметричных схем.

Реализация принципа «собери сейчас — расшифруй потом».

Взлом электронной подписи.

Ослабление стойкости симметричных алгоритмов под действием квантовых атак, требующее увеличения длины ключей и адаптации архитектур шифрования, в том числе развертывания дополнительных вычислительных мощностей.

Теоретическое доказательство устойчивости постквантовых алгоритмов

Постквантовые алгоритмы сложны, не подтверждены, некоторые уже взломаны.

Информационный шум и мифы

Умышленная дезинформация о прогрессе в квантовых технологиях как элемент глобального противостояния.

Опасны как бездействие, так и иррациональные инвестиции, вызванные перегретыми ожиданиями.

Угроза для систем диспетчерского управления и сбора данных

При использовании только симметричных алгоритмов без сертификации система может быть более уязвима для перехвата.

Возможность компрометации сообщений в критически важных отраслях экономики.

Утечка и компрометация ключей

Человеческий фактор остаётся основной уязвимостью при генерации и загрузке ключей. КРК минимизирует участие человека в процессе и ускоряет процесс распределения криптографических ключей

Снижение порога допустимой нагрузки на ключ.

Актуализация моделей угроз и злоумышленников

Квантовые и смежные технологии требуют пересмотра моделей угроз и типов нарушителей.

Масштабирование квантовой криптографии

Сети квантового распределения ключей (КРК) имеют ограничения по дальности и скорости, требуют больших капитальных затрат и перестройки архитектур безопасности (там, где требуется замена асимметричным шифрам).

[1] Консолидированная позиция экспертного сообщества Центра технологического лидерства при АНО «Цифровая экономика» в рамках проведенных экспертных сессий и глубинных интервью.
[2] Здесь и далее по тексту — квантовое распределение ключей.

Предпосылки развития квантовых и смежных технологий в ИБ, ключевые показатели и аспекты, отражающие развитие квантовых технологий в ИБ

В последние годы наблюдается **существенный прогресс в области квантовых технологий в сфере ИБ**, который трансформирует подходы к обеспечению безопасности информации. **Квантовые технологии базируются на принципах квантовой физики**, которые принципиально отличаются от классических физических законов и позволяют реализовать уникальные методы обработки, передачи и защиты информации.

Ключевые направления развития квантовых и смежных технологий в сфере ИБ[1]

Квантовые вычисления

Применение: взлом существующих и генерация новых механизмов защиты.

Статус: активно исследуется и пилотируется.

Тип вычислений, использующий принципы квантовой физики для выполнения операций над данными. Квантовые вычисления обладают большим потенциалом в решении сложных вычислительных задач. **Высокопроизводительные квантовые компьютеры в руках злоумышленника смогут эффективно взламывать классические криптографические системы**[2].

Квантовые коммуникации

Применение: защита информации (обеспечение защищенной передачи данных).

Статус: активно внедряется.

Технология передачи информации посредством прямой передачи квантовых состояний или посредством квантовой запутанности. **Наиболее зрелая сфера квантовых коммуникаций — это метод квантового распределения ключей**, позволяющий двум сторонам обмениваться криптографическими ключами, **безопасность которых обеспечивается законами квантовой физики**, а не скомпрометированными алгоритмами.

Постквантовая криптография

Применение: обеспечение криптографической устойчивости.

Статус: активно исследуется и пилотируется.

Набор новых асимметричных алгоритмов, разработанных для защиты данных от атак, осуществляемых с использованием квантовых компьютеров. Основная цель — обеспечить безопасность криптографических систем в условиях, когда квантовые вычисления становятся доступными злоумышленнику и могут угрожать традиционным методам шифрования. **Важно: постквантовая криптография — это не квантовая технология, а новые алгоритмы шифрования**[3].

Квантовые сенсоры

Применение: инструмент защиты (обнаружение атак «физического уровня»).

Статус: на стадии исследований.

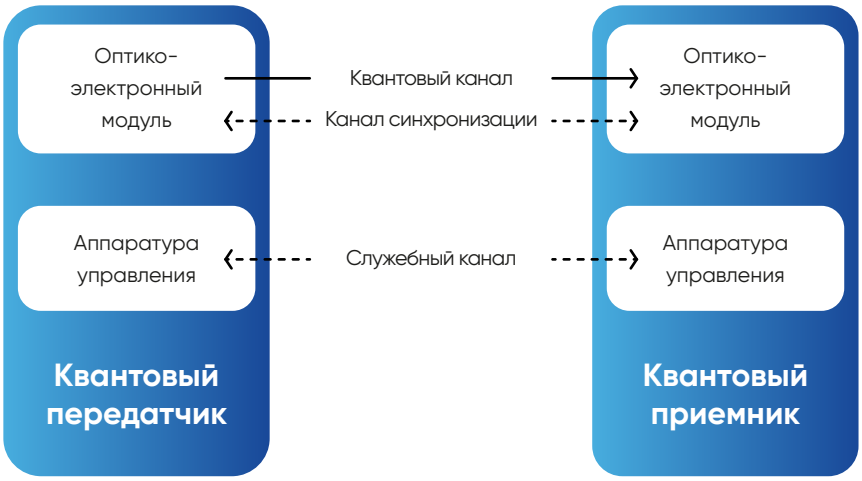
Измерительные приборы, использующие сверхчувствительные датчики на квантовых эффектах. Несмотря на раннюю стадию технологического цикла, рассматриваются как **перспективный инструмент обеспечения физического уровня информационной безопасности**. Их потенциал особенно высок в задачах детекции атак на аппаратное обеспечение и мониторинга критически важных объектов.

[1] Аналитический отчет «Перспективные сценарии применения квантовых и смежных технологий в отраслях» (2025).
[2] Например, алгоритм Шора способен разложить большие числа на множители за полиномиальное время, а алгоритм Гровера — ускоряет перебор симметричных ключей.
[3] Алгоритмы, реализованные на традиционных языках программирования и использующие классические вычислительные архитектуры.

Предпосылки развития квантовых и смежных технологий в ИБ, ключевые показатели и аспекты, отражающие развитие квантовых технологий в ИБ

Одним из ключевых направлений практической реализации квантовых технологий в сфере ИБ является создание защищенных каналов связи на основе квантовых коммуникаций. Согласно ПНСТ 829-2023, квантовая коммуникация предполагает передачу информации через квантовые каналы с использованием квантовых состояний объектов — чаще всего фотонов.

Типовая схема квантовой коммуникации



Структура включает:

- Квантовый передатчик — формирует и кодирует квантовый сигнал.
- Квантовый канал — оптоволокно или открытая среда.
- Квантовый приемник — регистрирует и декодирует сигнал.
- Каналы синхронизации и служебные каналы — передают управляющие сигналы по классическим сетям.

Такая архитектура лежит в основе **сетей квантового распределения ключей (КРК)**, обеспечивающих генерацию и безопасную доставку квантовых и производных от них **квантово-защищенных ключей (КЗК)** между узлами.

Дополнительно в КРК могут применяться:

Доверенные промежуточные узлы (ДПУ) — для ретрансляции ключей.

Квантовые повторители — для увеличения дальности без разрушения сигнала.

Модули управления ключами (МУК) — агрегируют и передают КЗК в СКЗИ[2].

Эти компоненты обеспечивают не только устойчивость и надежность КРК, но и их масштабирование, что позволяет строить квантовые сети сложной топологии (звезда, кольцо, дерево и др.).

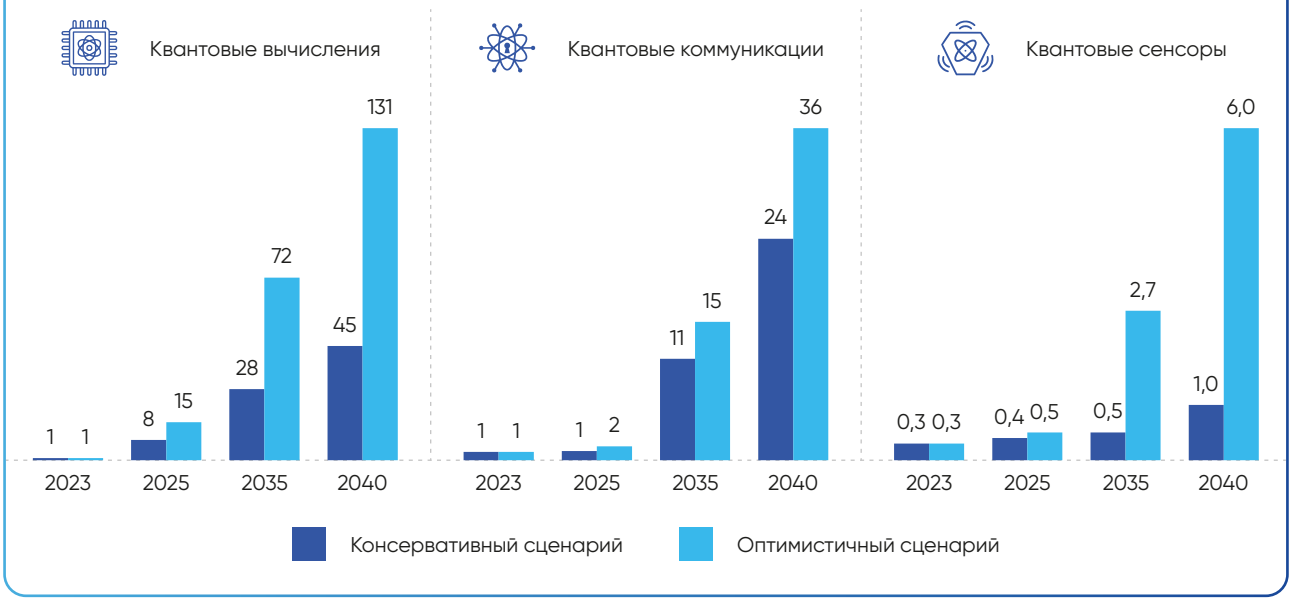
» Дополнительная защита достигается за счет фундаментальных законов физики: квантовый сигнал не может быть разделен, скопирован или усилен без разрушения, а классические каналы служат только для управления. Нарушение этих условий делает атаку мгновенно заметной.

» **Квантово-защищенные сети связи (КЗСС)** используют КРК для генерации ключей, которые затем применяются в СКЗИ. Защита может быть реализована с помощью квантового ключа (с перешифрованием данных в каждом узле) или на КЗК (с перешифрованием квантового ключа на узлах), что исключает компрометацию даже при наличии нарушителя, обладающего квантовым компьютером.

[1] ПНСТ 829-2023.
[2] Средство криптографической защиты информации.

Предпосылки развития квантовых и смежных технологий в ИБ, ключевые показатели и аспекты, отражающие развитие квантовых технологий в ИБ

Объем мирового рынка квантовых технологий[1], млрд долл. США



Инвестиции в квантовые технологии[1]

Новые инициативы (в/после 2024 года) | **Действующие инициативы (до 2024 года)**

Китай
$15,3 млрд

Увеличено государственное финансирование НИОКР в области квантовых технологий, с применением в безопасности, обороне и ИИ.

Германия
$5,2 млрд

Объявлено о вложении $2,25 млрд с целью создания универсального квантового компьютера: 100 кубитов к 2026 году и 500 кубитов в дальнейшем.

Великобритания
$4,6 млрд

Новая стратегия на 10 лет включает рост рынка, исследования и развитие кадров, с доп. инвестициями в $3,1 млрд. Дополнительно $130 млн в 2024 году.

США
$6 млрд

Национальная квантовая инициатива предусматривает $1,2 млрд за 5 лет на развитие квантовых технологий. Также в 2024–2025 годах выделили > $2,1.

Южная Корея
$2,4 млрд

Планирует вложить $2,3 млрд в квантовую науку и технологии к 2035 году с целью стать лидером в данной области.

Франция
$2,2 млрд

Заявлено о намерении занять лидирующую позицию в международной квантовой гонке, с инвестициями $1,3 млрд, объявленными в 2021 году.

Япония
$9,2 млрд

В 2025 году выделено $7,4 млрд на развитие технологий следующего. В 2021 году – $1,8 млрд.

Индия
$1,7 млрд

Национальная квантовая миссия (NQM) направлена на стимулирование НИОКР и создание инновационной экосистемы с финансированием $730 млн.

Канада
$1,4 млрд

Запущена Национальная квантовая стратегия (NQS) с инвестициями $360 млн в 2023 году. Дополнительно $52 млн в 2024 году.

Нидерланды
$1 млрд

Национальный фонд роста выделил $65 млн на Quantum Delta NL в 2023 году: ключевой элемент национальной инновационной экосистемы.

Россия[2]
$0,8 млрд

В 2021 году объявлено о $790 млн инвестиций в квантовые исследования на 5 лет – часть стратегии по технологическому развитию.

Израиль
$0,4 млрд

Запущена Израильская национальная квантовая инициатива (INQI) в 2018 году с первоначальным бюджетом около $390 млн.

[1] McKinsey (2025).
[2] Российский совет по международным делам.

Предпосылки развития квантовых и смежных технологий в ИБ, ключевые показатели и аспекты, отражающие развитие квантовых технологий в ИБ

6
млрд руб.
Объем российского рынка **квантовых вычислений** к 2030 году[1].

35–86
млрд руб.
Объем российского рынка **квантовых вычислений** к 2035 году[1].

30
млрд руб.
Объем российского рынка **квантовых коммуникаций** к 2030 году[2].

80
млрд руб.
Объем российского рынка **квантовых коммуникаций** к 2035 году[2].

39,9
млрд руб.
Объем финансирования сферы квантовых технологий в России в период 2020–2024 годов[3]

23,8
млрд руб.
Квантовые вычисления

16,1
млрд руб.
Квантовые коммуникации

Квантовая коммуникация играет ключевую роль в сфере ИБ.

Развитие квантовых технологий в области ИБ обусловлено научными и социально-экономическими предпосылками, а также предпосылками в сфере безопасности[4,5,6]

Научно-технологические предпосылки

- Развитие квантовой информатики и экспериментальной квантовой оптики.
- Миниатюризация и рост вычислительных мощностей.
- Прорывы в квантовой оптике и фотонике.

Социально-экономические предпосылки

- Геополитическая конкуренция.
- Государственные и частные инвестиции.
- Требования новых международных стандартов.
- Рост роли технологической ИТ- и ИБ-инфраструктуры как средства обеспечения глобального суверенитета.

Предпосылки в сфере безопасности

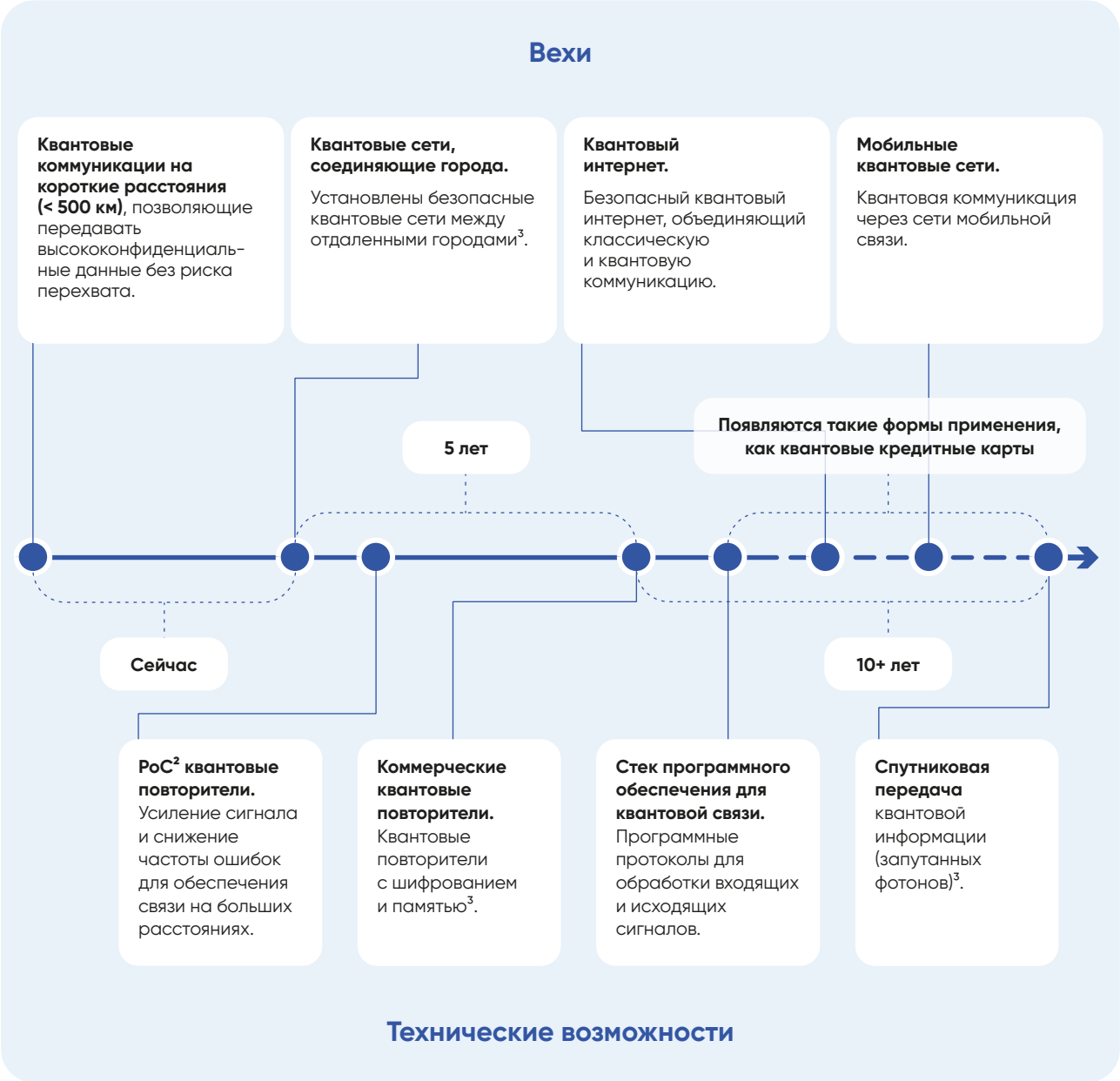
- Уязвимость классических криптографических алгоритмов и инфраструктуры перед квантовой угрозой.
- Повышение требований к защите данных с учетом роста не квантовых угроз.

[1] Предварительная оценка с учетом традиционной доли РФ в объеме аналогичных высокотехнологичных рынков.
[2] Индикативная оценка на основе результатов исследования компании «Иннопрактика».
[3] СП «Квант».
[4] N + 1 (2020).
[5] Gartner (2024, 2025).
[6] NIST (2025).

Предпосылки развития квантовых и смежных технологий в ИБ, ключевые показатели и аспекты, отражающие развитие квантовых технологий в ИБ

В ближайшей перспективе ожидается **активное развитие квантовых коммуникаций** как ответ на возрастающие риски для кибербезопасности, в том числе связанные с возможным появлением квантовых компьютеров, способных взламывать традиционные криптографические алгоритмы. **Квантовая криптография, в частности квантовое распределение ключей (КРК)**, рассматривается как перспективный способ обеспечения устойчивости к таким угрозам[1].

Основные этапы и технические возможности безопасной квантовой коммуникации[1]



[1] McKinsey (2024).
[2] (Proof of Concept) — это демонстрация практической осуществимости какой-либо идеи, метода или технологии с целью доказательства факта, что метод, идея или технология работают.
[3] Консолидированная позиция экспертного сообщества Центра технологического лидерства при АНО «Цифровая экономика» в рамках проведенных экспертных сессий и глубинных интервью.

Предпосылки развития квантовых и смежных технологий в ИБ, ключевые показатели и аспекты, отражающие развитие квантовых технологий в ИБ

Временной горизонт и условия перехода к квантовой устойчивости в ИБ-системах в крупных стратегически важных предприятиях России, государственных учреждениях / органах и остальных организациях[1]

	Крупные стратегически важные предприятия	Государственные учреждения/органы	Остальные организации
Горизонт внедрения	• 2025–2035 годы, в соответствии с государственными стратегиями и дорожными картами по квантовым коммуникациям. • Масштабное внедрение ожидается с 2027 по 2030 год, после нормативной адаптации и осознания угрозы квантового взлома. • Ранние показательные пилоты (например, на базе ОАО «РЖД») могут стартовать в 2026 году.	• 2025–2030 годы — вероятный период поэтапного перехода (при наличии нормативных требований). • В ряде организаций процесс уже запущен: идет обучение, пилотирование и эксплуатация оборудования. • В некоторых регионах уже выделяются крупные суммы, например, в Москве выделено 10 млрд руб. на создание защищенных каналов для поликлиник и школ.	• После 2030 года, возможный массовый рубеж — 2040 год. • В ряде мнений называются ориентиры даже до 2050 года (в случае B2C-сегмента), при отсутствии давления сверху или квантовых инцидентов.
Условия перехода	Переход будет происходить постепенно и директивно, при наличии: • нормативных требований; • утвержденных государственных стандартов; • инфраструктурной готовности (сети, оборудование, кадры).	• Директивное решение регулятора. • Нормативные требования и бюджетное финансирование. • Переход возможен в рамках институциональных программ, с участием интеграторов, особенно в инфраструктурных проектах (волоконные линии, спутниковая связь). • Потребность в защищенной передаче ключей на большие расстояния может подтолкнуть к приоритетному переходу для отдельных категорий органов.	• Внедрение будет происходить по мере доступности, зрелости технологии и появления рыночного или регуляторного драйвера. • В исторической ретроспективе аналогичный переход (например, к электронно-цифровой подписи) занял до 20 лет после принятия закона.
Ограничения и риски	• Недостаточное количество утвержденных стандартов. • Коммерческие подключения только начинают запускаться; полноценное развертывание требует высокой плотности узлов (100–200 точек / узел). • Крупные инвестиции пока не делаются в отсутствие реальных квантовых угроз.	• Технология требует серьезной инфраструктурной базы, что затрудняет быстрое масштабирование. • Отсутствие регуляторного документа делает массовый переход практически невозможным — пока все происходит на уровне пилотов. • Неравномерность зрелости между игроками: от высокоподготовленных (например, ОАО «РЖД») до инертных сегментов с низкой ИБ-культурой.	• Без нормативного давления мотивов для внедрения недостаточно. • Квантовая угроза пока воспримется как гипотетическая. • Ограниченная дальность текущих ККС[2]. • Ценность квантовых технологий в контексте ИБ пока не сформирована и не осознана большинством игроков рынка.

[1] Консолидированная позиция экспертного сообщества Центра технологического лидерства при АНО «Цифровая экономика» в рамках проведенных экспертных сессий и глубинных интервью.
[2] Квантовые каналы связи.

Анализ влияния развития квантовых и смежных технологий на традиционные методы шифрования и кибербезопасность

Современные криптографические методы

Асимметричное шифрование

Недостатки:

- Большие размеры ключей.
- Низкая производительность при работе с большими массивами данных.
- Необходимость в больших вычислительных мощностях.

Симметричное шифрование

Недостатки:

- Проблема распределения ключей.
- Ограниченная масштабируемость.

Хэширование

Недостатки:

- Уязвимость к коллизиям[1].
- Проблемы скорости и производительности.
- При недостаточном размере хэша возможно нарушение целостности.

Квантовые алгоритмы в возможной реализации квантовых атак

Алгоритм Шора позволяет эффективно решать задачи факторизации и дискретного логарифмирования, что ставит под угрозу все асимметричные криптосистемы.

Алгоритм Гровера ускоряет атаку на симметричные шифры и хэши, сокращая необходимое количество операций вдвое, что приводит к снижению допустимой нагрузки на ключи (это, в свою очередь, требует либо увеличения длины ключей, либо увеличения частоты смены ключей).

Возможные решения, основанные на квантовых и смежных технологиях

1. Постквантовая криптография[2]

В ответ на новые угрозы развивается постквантовая криптография — криптографические алгоритмы, устойчивые к атакам как классических, так и квантовых компьютеров. Важно отметить, что постквантовая криптография — это не квантовая технология, а новые алгоритмы шифрования данных, реализованные на традиционных языках программирования и использующие классические вычислительные архитектуры.

Преимущества и недостатки решений на базе постквантовой криптографии

Относительно низкая стоимость приобретения

Возможность интеграции без модификации аппаратной инфраструктуры

Поддержка популярных платформ и вычислительных архитектур

Государственные стандарты по постквантовой криптографии еще разрабатываются

Повышенные требования к реализации и оптимизации параметров алгоритмов

[1] Коллизия возникает, когда два разных входных сообщения производят одинаковое хэш-значение.
[2] SecurityLab.

Анализ влияния развития квантовых и смежных технологий на традиционные методы шифрования и кибербезопасность

2. Квантовое распределение ключей

Процедура выработки и распределения секретных ключей, реализуемая с помощью квантовых криптографических протоколов и квантовых каналов связи. Суть метода: две стороны, соединенные по аутентифицированному каналу связи, создают общий случайный ключ, который известен только им, и используют его для шифрования и расшифровывания сообщений. Решения на базе квантовых технологий, в частности квантового распределения ключей (КРК), могут эффективно сочетаться с решениями на базе других технологий в сфере информационной безопасности (ИБ).

Преимущества и недостатки КРК

Безопасность: попытка перехвата квантовых состояний нарушает их квантовые свойства, что оставляет следы присутствия.

Детектируемость атак: участники коммуникации обнаруживают попытки перехвата по ошибкам в передаваемых сигналах.

Устойчивость к квантовым компьютерам

Необходимость специфического и дорогого оборудования и инфраструктуры

Сложности с масштабированием

Ограниченная дальность передачи

3. Квантовые генераторы случайных чисел

Квантовые генераторы случайных чисел (КГСЧ) – устройства, которые используют принципы квантовой механики для создания истинно случайных чисел, не поддающихся предсказанию. В отличие от классических генераторов, которые полагаются на алгоритмические процессы, КГСЧ используют непредсказуемость квантовых явлений, например поведения фотонов или других частиц.

Преимущества и недостатки квантовых генераторов случайных чисел

Непредсказуемость генерируемых чисел

Устойчивость к атакам

Высокая скорость генерации и возможность облачного предоставления случайных чисел

Необходимость калибровки и настройки

Стоимость оборудования

Квантовые вычисления кардинально изменят ландшафт ИБ, делая уязвимыми существующие криптографические методы. Однако даже высокопроизводительные квантовые компьютеры смогут взломать далеко не все: неуязвимыми останутся симметричные шифры, решетчатые шифры, многомерная криптография, криптография на основе кодов и квантовые генераторы случайных чисел.

Преимущества внедрения квантовых и смежных технологий в ИБ в долгосрочной перспективе

Долгосрочная защита конфиденциальных данных

Квантовые и смежные технологии позволяют создать системы, способные противостоять актуальным угрозам настоящего и будущего, таким как взлом современных криптографических алгоритмов с помощью квантовых компьютеров. Это особенно важно для информации, требующей длительного хранения, например, коммерческой тайны, инженерной тайны, персональных данных.

Повышение доверия и конкурентоспособности

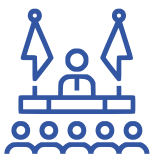
Исследования и ранние пилотные внедрения квантовых технологий демонстрируют приверженность организации к передовым методам защиты данных, что может повысить доверие клиентов и партнеров. Кроме того, это может предоставить конкурентное преимущество на рынке, особенно в отраслях, где безопасность информации является приоритетом.

Интеграция с другими передовыми технологиями

Квантовые и смежные технологии могут быть эффективно интегрированы как друг с другом, так и с другими инновационными направлениями, такими как искусственный интеллект и машинное обучение, для создания более мощных и адаптивных систем безопасности. Это открывает новые горизонты для разработки комплексных решений в области кибербезопасности.

Следование передовым мировым научным трендам

Создание магистральных и межуниверситетских сетей квантовых коммуникаций, использующих квантовое распределение ключей, обеспечивает защищенную передачу данных. Такие сети уже реализуются в различных странах, демонстрируя потенциал для масштабирования и интеграции в существующую инфраструктуру.



Глобальное перераспределение власти и киберсуверенитет

Квантовая безопасность станет ключевым фактором геополитического и экономического влияния. Страны и корпорации, обладающие квантово-устойчивой инфраструктурой, получат преимущество в киберконфликтах и международной торговле. Технологии квантово-устойчивой защиты информации станут частью национального технологического суверенитета.

Преимущества внедрения квантовых и смежных технологий в ИБ в долгосрочной перспективе

Как организации могут противодействовать новым угрозам?

Технология	Описание	+	−
Обнаружение угроз с помощью ИИ	Использование машинного обучения для анализа закономерностей и обнаружения аномалий	Автоматизированное обнаружение угроз в режиме реального времени	Высокие вычислительные затраты, возможность ложных срабатываний
Архитектура нулевого доверия	Проверка каждого пользователя и устройства в каждой точке доступа	Минимизация поверхности атаки, усиление контроля	Сложная реализация в больших сетях
Технологии обмана	Развертывание поддельных средств для введения в заблуждение атакующих и сбора информации	Предоставляет разведывательную информацию о методах атаки	Ресурсоемкие, риск обнаружения атакующими
Поведенческая аналитика	Мониторинг поведения пользователей и организаций на предмет необычных действий	Обнаружение внутренних угроз, передовых аномалий	Требуются большие массивы данных и постоянный мониторинг
Шифрование данных	Защита данных путем их кодирования для хранения и передачи	Защита конфиденциальной информации от утечки	Сложность управления ключами
Обмен информацией об угрозах	Совместный обмен данными об угрозах между организациями	Принятие обоснованных решений и проактивная защита	Конфиденциальность. Вопрос доверия между организациями
Планы реагирования на инциденты	Предустановленные протоколы реагирования на кибер-инциденты	Сокращение времени простоя, организованные усилия по восстановлению	Требуется регулярное обновление и тестирование
Основы киберустойчивости	Сочетает стратегии предотвращения, обнаружения и восстановления	Обеспечивает непрерывность и адаптируемость бизнеса	Интеграция с существующими системами может быть затруднена

Анализ мирового и российского опыта развития квантовых и смежных технологий в сфере ИБ

Выявление основных трендов развития ИБ

Глобальный переход к квантово-устойчивой коммуникации

Описание тренда

В горизонте около десяти лет ожидается появление высокопроизводительного квантового компьютера, который будет способен угрожать классическим криптографическим системам. Решения на базе квантовых и смежных технологий позволят, как ожидается, сделать системы ИБ устойчивыми к данной угрозе. Осознавая это, компании уже сейчас направляют средства на разработку, внедрение (в том числе в рамках пилотных проектов) решений на основе квантового распределения ключей, постквантовой криптографии и др., которые должны успешно защитить ценную информацию перед атаками с применением как классических, так и квантовых компьютеров.

Примеры

Российские компании (такие как ИнфоТеКС, СМАРТС- Квантелеком, КуРэйт) перешли к серийному производству систем КРК.

Google тестировал постквантовые алгоритмы в Chrome наряду с классическими (в рамках гибридного обмена ключами).

Развитие различных видов развертывания устойчивых квантовых сетей

Описание тренда

В защищенной с помощью квантовых технологий передаче информации будут заинтересованы все большее и большее количество организаций. Это влечет за собой появление сложноорганизованных сетей, которые бы объединяли множество участников, передающих и получающих информацию, защищенную с помощью квантовой криптографии (многоузловые квантовые сети, гибридные квантовые сети, квантовый интернет и др.).

Примеры

На 2025 год общая протяженность создаваемой ОАО «РЖД» и партнерами линии квантовой коммуникационной сети составила 7012 км. К 2030 году протяженность должна составить не менее 15 тыс. км. Экосистема развития квантовых коммуникаций насчитывает более 180 участников.

Первый экспериментальный прототип квантового интернета уже создан в китайской столице: в 2023 году с помощью развернутого квантового канала связи протяженностью 64 км продемонстрировали рекордную скорость передачи данных (7,1 кбит/с).

Источник: аналитика O2Consulting, консолидированная позиция экспертного сообщества Центра технологического лидерства при АНО «Цифровая экономика» в рамках проведенных экспертных сессий и глубинных интервью.

Выявление основных трендов развития ИБ

Оптимизация и улучшение характеристик устойчивой квантовой связи

Описание тренда

Сочетание квантовых и смежных технологий с передовыми цифровыми технологиями выведет на принципиально новый уровень решения на базе данных технологий. В частности, комбинирование квантовых и смежных технологий с умными устройствами интернета вещей открывает новый уровень эффективности (за счет появления квантовых датчиков, квантово-устойчивых каналов связи и др.). Кроме того, криптографические решения на базе квантовых и смежных технологий все больше будут использоваться в блокчейн-системах, а также в облачных вычислениях. С другой стороны, квантовый компьютер выведет на новый уровень качества современный ИИ, что найдет свое применение в ИБ-предиктивной аналитике.

Примеры

По состоянию на 2025 год АО «ИнфоТеКС» удалось добиться снижения стоимости новой платформы ViPNet КУКС примерно на 30 %.

В 2025 году китайским ученым в течение 168 часов беспрерывной работы удалось обеспечить устойчивую передачу квантовых данных со скоростью 2,38 кбит/с.

Интеграция квантовых технологий с прочими цифровыми технологиями, в том числе в сфере ИБ

Описание тренда

Сочетание квантовых технологий с передовыми цифровыми технологиями выведет на принципиально новый уровень решения на базе данных технологий. В частности, комбинирование квантовых технологий и умных устройств (IoT, IIoT) открывает новый уровень эффективности интернета вещей (за счет появления квантовых датчиков, квантово-устойчивых каналов связи и др.). Кроме того, квантовые криптографические решения все больше будут использоваться в блокчейн-системах, а также при предоставлении услуг облачных вычислений. С другой стороны, квантовый компьютер выведет на новый уровень качества современный ИИ, что найдет свое применение в ИБ-предиктивной аналитике.

Примеры

Компании Web3 Tech и QApp разработали блокчейн-платформу «Конфидент» — прототип квантово-устойчивого блокчейна на отечественных постквантовых алгоритмах.

В рамках проекта EU OpenQKD квантовое распределение ключей применяется для защиты данных, передаваемых при функционировании умной сети электроснабжения.

Источник: аналитика O2Consulting, консолидированная позиция экспертного сообщества Центра технологического лидерства при АНО «Цифровая экономика» в рамках проведенных экспертных сессий и глубинных интервью.

Выявление основных трендов развития ИБ

Поддержка развития квантовых технологий

Описание тренда

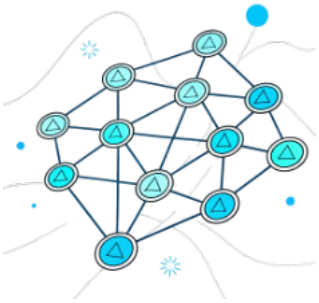
Развитие квантовых технологий, как и других передовых высоких технологий, требует поддержки со стороны государства. На сегодняшний день множество стран предпринимают различные шаги, направленные на развитие этой сферы. Помимо финансирования исследований и поддержки малых инновационных компаний, принимаются госпрограммы (в том числе затрагивающие процессы ИБ) и проводится стандартизация алгоритмов, протоколов, необходимая для широкого применения решений на базе квантовых технологий, в том числе в сфере ИБ.

Примеры

В 2019 году началась реализация дорожных карт развития высокотехнологичных областей «квантовые коммуникации» и «квантовые вычисления», которые, в том числе, затрагивают сферу ИБ.

В 2024 году Национальный институт стандартов и технологий США (NIST) представил первые три стандарта, определяющие алгоритмы постквантового шифрования, стойкие к угрозе взлома квантовым компьютером.

Формирование сервисной модели услуг квантово-устойчивой связи



Описание тренда

Создаваемые в настоящее время федеральные магистральные сети защищенной квантовой связи являются основой для постепенно формирующихся более широких сетей, частью которых (на более низких уровнях) станут существующие телекоммуникационные компании и конечные пользователи квантовой связи, которые будут приобретать услугу по подключению к федеральным магистральным сетям через вышеуказанные телекоммуникационные компании.

Примеры

ОАО «РЖД» с 2026 года планирует предоставлять услуги внешним абонентам (через операторов и интеграторов), предлагая квантово-защищенные коммуникации и сервисную поддержку для ключевых отраслей экономики.

China Telecom Quantum Group представила первую в мире систему связи, устойчивую к атакам квантовых компьютеров. Система разворачивается в 16 городах Китая, обслуживая сотни госструктур и корпораций через специализированные сервисы.

Источник: аналитика O2Consulting, консолидированная позиция экспертного сообщества Центра технологического лидерства при АНО «Цифровая экономика» в рамках проведенных экспертных сессий и глубинных интервью.

Выявление основных трендов развития ИБ

Горизонт активного проявления технологий и процессов, влияющих на тренды

до 5 лет	5–10 лет	10+ лет
1. Глобальный переход к квантово-устойчивой коммуникации		
Квантовое распределение ключей*	Квантовая цифровая подпись*	
Постквантовая криптография*		
Квантовый генератор случайных чисел*		
2. Развитие различных видов развертывания устойчивых квантовых сетей		
Оптоволоконные квантовые коммуникации	Квантовый повторитель	Квантовый интернет
Гибридные квантовые сети*	Квантовая память	Спутниковая квантовая связь
	Атмосферная квантовая связь	
3. Оптимизация и улучшение характеристик устойчивой квантовой связи		
Миниатюризация (уменьшение размера и веса квантовых программно-аппаратных комплексов)	Снижение потерь, уровня шумов в квантовых каналах связи	Увеличение дальности передачи квантовой информации
Автоматизация (исключение человеческого фактора) при распределении ключей	Снижение потребления ресурсов	Повышение скорости передачи данных
	Снижение стоимости развертывания квантовых сетей	
4. Интеграция квантовых технологий с прочими цифровыми технологиями, в том числе в сфере ИБ		
	Квантово-защищенное распределенное хранение данных	
	Квантовые финансы	
	Квантово-устойчивый интернет вещей	
	Квантово-устойчивые облачные вычисления	
	Квантовый искусственный интеллект	
5. Поддержка суверенитета квантовых технологий		
Принятие различных госпрограмм, а также госстандартов в сфере квантовых технологий		
Новые образовательные программы		
6. Формирование сервисной модели услуг квантово-устойчивой связи		
	Квантовая коммуникация как телеком-услуга, доступная широкому кругу пользователей	

* — может участвовать в формировании нескольких трендов.

Источник: аналитика O2Consulting, консолидированная позиция экспертного сообщества Центра технологического лидерства при АНО «Цифровая экономика» в рамках проведенных экспертных сессий и глубинных интервью.

Исследование международного опыта развития квантовых и смежных технологий в ИБ

Китай

Государственное регулирование и инициативы

- **Cryptography Law of the People's Republic of China (Закон КНР «О криптографии»)** регулирует не только классические, но и квантовые технологии шифрования. В нормативных документах отражено обязательное использование китайских криптосредств и работа с госстандартами в области ИБ.
- **14-й пятилетний план (2021–2025)** включает квантовую ИБ как один из ключевых приоритетов. Государство активно инвестирует в квантовые кластеры и формирует замкнутую экосистему в этой сфере.

Ключевые проекты в области квантовых технологий в сфере ИБ

- Китай в 2017 году **создал первую в мире квантовую межгородскую линию связи** между Пекином и Шанхаем (BSBN). Это одна из крупнейших в мире реализаций КРК (распределения квантовых ключей)[1].
- В 2017 году физики из Китая и Австрии **с помощью спутника «Мо-Цзы» (Micius, QUESS) провели первый сеанс межконтинентальной квантовой видеосвязи**, защищенной от взлома при помощи шифровальных ключей, переданных через спутник.
- **Китай сообщил в 2023 году о планах масштабного квантового интернета**, основанного на квантовых спутниках и наземных узлах. Это потенциально крупнейшая система такого рода в мире.

Инструменты поддержки и стимулирования

1. **Пекинский комитет по управлению зонами экономического и технологического развития опубликовал документ с мерами поддержки развития квантовых технологий и промышленности.** Финансирование разделено по нескольким направлениям[2]:

- **Направление 1.** Предприятиям рекомендуется сосредоточиться на ключевых технологиях, таких как программные и аппаратные продукты квантовых вычислений, облачные платформы, сети квантовой связи и алгоритмы безопасности и др. Финансирование нацелено на прорывные НИОКР.
- **Направление 2.** Финансируются консорциумы: вуз – НИИ – индустрия – заказчики (совместные НИОКР / инвестиции / инкубация) при условии если продукт / услуга в квантовой сфере получил статус «новый».
- **Направление 3.** Поддержка построения гетерогенных квант-классических облаков/центров (мульти-технологические маршруты, стек ПО / компиляторы и др.).

2. **Зона развития высоких технологий Восточного озера Optics Valley в г. Ухань выпустила документ Quantum Twelve[3] с мерами поддержки для квантовой сферы.** Документ нацелен на развитие квантовых технологий, в том числе квантово-защищенной связи. Финансирование направлено на:

- создание концептуально-демонстрационных и среднеиспытательных (пилотных) платформ для квантовой связи и квантового сенсинга;
- поддержку компаний, которые внедряют проекты вузов / НИИ (проект должен быть включен в перечень задач Зоны).

[1] Chinese Academy of Sciences
[2] Пекинский комитет по управлению зонами экономического и технологического развития
[3] Quantum Twelve

Исследование международного опыта развития квантовых и смежных технологий в ИБ

США

Государственное регулирование и инициативы

- **CHIPS & Science Act (2022)** содержит целую главу, посвященную квантовым технологиям и безопасности. Закон предусматривает выделение финансирования на исследование, разработку и внедрение PQC-решений.
- **Меморандум OMB M-23-02 (2022)** требует от всех федеральных ведомств за два года (и ежегодно в дальнейшем до 2035 года) составить инвентаризацию уязвимой криптографии и план перехода на PQC.
- **National Quantum Initiative Act (2018)**. Закон, определяющий цели и приоритеты на 10 лет для ускорения развития квантовых информационных наук и технологий.
- **Национальная квантовая инициатива (NQI) (2023) и National Cybersecurity Strategy (2023)** приоритизируют миграцию на квантоустойчивую криптографию к 2035 году.

Ключевые проекты в области квантовых технологий в сфере ИБ

- США активно продвигают **стандарты постквантовой криптографии (PQC)**. В августе 2024 года в США официально утвердили федеральные стандарты FIPS 203, FIPS 204 и FIPS 205, основанные на алгоритмах CRYSTALS-KYBER (ML-KEM), CRYSTALS-Dilithium (ML-DSA) и SPHINCS+ (SLH-DSA). Стандарт FIPS 206 (на базе Falcon) находится в разработке[1].
- Нью-Йоркский университет и Qunnect **проложили 10-мильную (16-километровую) связь квантовой сети (GothamQ)** между Бруклинской военно-морской верфью и кампусом Нью-Йоркского университета в Манхэттене[2].
- **DARPA запустила программу QuANET** — «квантовая надстройка» для оборонных сетей, с упором на масштабируемую КРК и квантовую аутентификацию. Программа QuANET направлена на расширение существующей программной инфраструктуры и сетевых протоколов квантовыми свойствами[3].

Инструменты поддержки и стимулирования

1. **Программа исследований инноваций малого бизнеса финансируемая NIST (Small Business Innovation Research, SBIR, Phase I/II)**[4]. Финансированию подлежит малый бизнес из различных сфер, в том числе сферы квантовых технологий, с целью противодействия новым угрозам безопасности, возникающим в связи с развитием квантовых технологий.
2. **Программа финансирования малых предприятий NSF (America's Seed Fund)**[5], которая поддерживает исследования во всех областях науки и техники. Национальный научный фонд финансирует малые предприятия, в том числе в сфере квантовых информационных технологий, кибербезопасности и аутентификация (включая постквантовую криптографию и гомоморфное шифрование).

[1] NIST
[2] New York University
[3] DARPA
[4] NIST (SBIR)
[5] NSF

Исследование международного опыта развития квантовых и смежных технологий в ИБ

Сингапур

Государственное регулирование и инициативы

- **National Quantum Strategy, NQS** (Национальная квантовая стратегия) (2024). Она рассчитана на пять лет и призвана укрепить позиции Сингапура как одного из ведущих центров по разработке и внедрению квантовых технологий.
- **Агентство кибербезопасности Сингапура (CSA)** планирует с 2025 года начать выпуск **руководств по квантовой безопасности (Guidelines on Quantum Security) для бизнеса**.

Ключевые проекты в области квантовых технологий в сфере ИБ

- В 2024 году сингапурский **оператор Singtel запустил National Quantum-Safe Network Plus (NQSN+)** — первую в Юго-Восточной Азии национальную квантово-безопасную сеть. Цель проекта — защитить предприятия от квантовых угроз, которые ожидаются в ближайшие 5–10 лет[1].

Инструменты поддержки и стимулирования

1. **Квантовый трек FSTI от Управления денежного обращения Сингапура (Monetary Authority of Singapore, MAS)**[2]. Программа FSTI Quantum Track создана в рамках Программы развития технологий и инноваций в финансовом секторе (FSTI 3.0) и направлена на поддержку инноваций в области квантовых технологий и ИИ. Трек состоит из пакета грантов для поддержки:

- **Технологические центры**. Создание функций квантовых вычислений и инноваций в области безопасности. Направление открыто для финансовых учреждений и глобальных технологических компаний, которые намерены создать Центр передового опыта в области квантовых вычислений и безопасности в Сингапуре.
- **Технологические инновации**. Стратегические проекты, которые изучают возможности использования квантовых технологий для решения значимых проблем и реализации вариантов их использования в промышленности и учреждениях.
- **Безопасность**. Ускорение пилотов, повышающих кибербезопасность. Предназначено обеспечить возможность проведения экспериментов и ускорить разработку пилотных проектов, связанных с квантовыми технологиями, для повышения безопасности в сфере финансовых услуг. Пилотные проекты, исследующие такие подходы, как постквантовая криптография и квантовое распределение ключей, способствуют развитию квантово-безопасной криптографии и защите критически важных данных компаний.
- **Развитие талантов**. Инициативы по развитию талантов, направленные на поощрение корпоративной культуры, ориентированной на квантовые технологии, в финансовых учреждениях.

[1] Singtel
[2] Monetary Authority of Singapore

Исследование международного опыта развития квантовых и смежных технологий в ИБ

Европейский союз

Государственное регулирование и инициативы

Quantum Europe Strategy[1]. Стратегия направлена на превращение Европы в квантовый центр посредством содействия формированию устойчивой, суверенной квантовой экосистемы. Стратегия фокусируется на пяти взаимосвязанных областях:

- Исследования и инновации.
- Квантовые инфраструктуры.
- Укрепление квантовой экосистемы.
- Космические и квантовые технологии двойного назначения (безопасность и оборона).
- Quantum Skills: создание разнообразной рабочей силы мирового класса посредством скоординированного образования, обучения и мобильности талантов по всему ЕС.

Ключевые проекты в области квантовых технологий в сфере ИБ

- **Quantum Internet Alliance (2018–2026)**. Разрабатываются архитектура и прототипы для будущего квантового интернета, включая защищенную межузловую коммуникацию, квантовые ретрансляторы и распределенную криптографию. Проект объединяет ведущие европейские академические и промышленные центры и фокусируется на создании фундаментальной инфраструктуры для масштабируемой квантовой связи[2].
- **Система EuroQCI**. Создание общеевропейской квантовой коммуникационной инфраструктуры с использованием КРК. Система будет состоять из наземного сегмента, основанного на волоконно-оптических сетях связи, связывающих стратегически важные объекты на национальном и трансграничном уровнях, и космического сегмента на основе спутников. Она станет неотъемлемой частью новой космической защищенной системы связи ЕС[3].

Инструменты поддержки и стимулирования

1. **Программа EIC STEP Scale Up[4] является частью инициативы The Strategic Technologies for Europe Platform (STEP)**, предлагающей финансовую поддержку в виде инвестиций стартапам, малым и средним предприятиям, а также компаниям средней капитализации. Цель программы — масштабировать инновации в стратегических технологических секторах Европы, особенно в области квантовых технологий и полупроводников. Программа STEP Scale Up, которой управляет Фонд EIC , направлена на устранение дефицита финансирования высокорисковых инноваций, которые не могут быть полностью профинансированы другими инвесторами.
2. **Программа EIC Accelerator[5], в том числе EIC Accelerator Open[6]** (не имеют заранее определенной темы: этот конкурс предназначен для инноваций в любой области технологий, а также инноваций, которые затрагивают различные научные, технологические, отраслевые и прикладные области). **EIC Accelerator** — это финансирование, осуществляемое в рамках программы Horizon Europe, направленное на поддержку стартапам, малым и средним предприятиям, которым необходимо быстрое масштабирование деятельности до TRL 9. Принимаются заявки от новаторов из всех государств-членов ЕС и стран, участвующих в программе Horizon Europe. **Особое внимание уделяется стартапам, а также малым и средним предприятиям, возглавляемым женщинами**.
3. **Грантовый конкурс Transition to post-quantum Public Key Infrastructures[7] (Переход к постквантовым инфраструктурам открытых ключей) в рамках программы Digital Europe. Цель конкурса** — решить проблемы эффективной интеграции алгоритмов постквантовой криптографии в инфраструктурах открытых ключей.
4. **Программа Horizon Europe[8]** — рамочная программа ЕС по НИОКР на 2021–2027 годы с бюджетом 93,5 млрд евро. Рассчитана на поддержку исследований и инноваций, повышение конкурентоспособности ЕС, в том числе по цифровой/киберповестке. В рамках этой программы реализуются 3 подпрограммы, связанные с квантовыми технологиями в ИБ: **Грантовый конкурс Security evaluations of Post-Quantum Cryptography (PQC) primitives[9], Грантовый конкурс Integration of PQC algorithms into high-level[10], Грантовый конкурс Security of implementations of PQC algorithms[11]**.

[1] European Commission
[2] QIA
[3] EuroQCI
[4] EIC STEP Scale Up
[5] EIC Accelerator
[6] EIC Accelerator Open
[7] Transition to post-quantum Public Key Infrastructures
[8] Horizon Europe
[9] Security evaluations of Post-Quantum Cryptography (PQC) primitives
[10] Integration of PQC algorithms into high-level protocols
[11] Security of implementations of PQC algorithms

Исследование международного опыта развития квантовых и смежных технологий в ИБ

Великобритания

Государственное регулирование и инициативы

- **Timelines for Migration to Post-Quantum Cryptography** Национального центра кибербезопасности (NCSC) Великобритании — национальный план миграции к постквантовой криптографии (PQC) до 2035 года.
- **National Quantum Strategy** — Национальная квантовая стратегия Великобритании (2023). Одна из целей — создание инфраструктуры для квантово-безопасной связи, в том числе через квантовые сети, например UK Quantum Network (UKQN).

Ключевые проекты в области квантовых технологий в сфере ИБ

- Великобритания создала **квантовую сеть UK Quantum Network (UKQN)**, которая охватывает Бристоль и Кембридж и соединена четырьмя длинными оптоволоконными каналами с тремя промежуточными узлами. Сеть использует два типа схем квантового распределения ключей (КРК): «невзламываемые» ключи шифрования, скрытые внутри частиц света, и распределенную запутанность, которая связывает квантовые частицы. Расстояние между Бристолем и Кембриджем по оптоволоконной сети — более 410 километров[2].
- **UKQN служит «открытым полигоном» для SME-компаний,**[1] которые могут подключаться и тестировать КРК-решения на реальной инфраструктуре. UKQN предоставляет лишь временный доступ к КРК-линии, необходимый для проведения тестов[2].

Инструменты поддержки и стимулирования

1. **Пилотный проект Innovate UK Quantum Missions**[3]. Конкурс призван вывести Великобританию на передовые позиции в области квантовых инноваций, предоставляя значительные — гранты на новаторские проекты в области квантовых вычислений и квантовых сетей.
2. **Программа EIC Accelerator также доступна для Великобритании** поскольку страна принимает участие в программе Horizon Europe (см. блок Европейский союз). Финансирование направлено стартапам, малым и средним предприятиям, которые занимаются разработкой, внедрением и масштабированием инновационных решений на поздних стадиях, демонстрирующих высокий потенциал для прорыва.

[1] Small and Medium-sized Enterprises — «малые и средние предприятия».
[2] Quantum Communications Hub.
[3] Innovate UK «Quantum Missions».

Исследование международного опыта развития квантовых и смежных технологий в ИБ

Германия

Государственное регулирование и инициативы

- **Инициатива QuNET**, финансируемая Федеральным министерством образования и исследований Германии (BMBF) направлена на разработку безопасных и устойчивых ИТ-сетей с использованием квантовых технологий.
- **Проект QUANTITY** – совместная инициатива Германского аэрокосмического центра (DLR) и Федерального ведомства по информационной безопасности (BSI) по квантовому криптоанализу.
- **BSI выпускает серии руководств:** Quantum-safe cryptography (2021), техническое руководство TR-02102-1 (Cryptographic Mechanisms: Recommendations and Key Lengths). В нем упоминаются FrodoKEM и Classic McEliece.
- **Kryptografie quantensicher gestalten.**

Ключевые проекты в области квантовых технологий в сфере ИБ

- **В рамках инициативы QuNET**, совместной программы Общества Fraunhofer, Немецкого аэрокосмического центра и Общества Макса Планка, осуществлено несколько проектов[1]:

1. В 2021 году реализована квантовая защищенная видеоконференция между двумя федеральными агентствами.
2. В 2024 году установлен лазерно-оптический канал связи между исследовательским самолетом DLR DO 228 CFFU и мобильной наземной станцией QuBUS от Fraunhofer IOF.
3. В 2025 году планируется соединить световые частицы, передаваемые через воздух, с ионом-ловушкой.

- В 2025 году **BSI сертифицировал первую в мире смарт-карту** с встроенным PQC-алгоритмом (FrodoKEM)[2].

Инструменты поддержки и стимулирования

1. **Для страны актуальны все инструменты поддержки и стимулирования, указанные в блоке «Европейский союз».**
2. **Программа Transfer und Netzintegration der Quantenkommunikation[3] (Перенос и внедрение квантовой связи в сети)**, финансируемая Федеральным министерством образования и исследований, направлена на поддержку исследований в области квантовых коммуникации в сфере ИТ-безопасности. **Гранты предоставляются в качестве безвозвратных субсидий посредством проектного финансирования.**

[1] QuNET.
[2] BSI.
[3] BMBF.

Исследование международного опыта развития квантовых и смежных технологий в ИБ

Франция

Государственное регулирование и инициативы

- **Специального «квантового» закона нет: требования ИБ задаются ANSSI** (Национальное агентство по кибербезопасности Франции) и выполняются в рамках общеевропейского регламента EuroQCI.
- **Национальная стратегия квантовых технологий Франции (2021)**. В рамках стратегии была запущена программа PROQCIMA.
- **Консорциум RESQUE (RÉSilience Quantique или квантовая устойчивость)** — объединение шести французских компаний и организаций для разработки постквантовых решений в области информационной безопасности. Они будут работать над разработкой постквантового криптографического решения, способного защитить коммуникации, инфраструктуру и сети предприятий и местных органов власти от будущих атак, осуществляемых с помощью квантовых компьютеров.

Ключевые проекты в области квантовых технологий в сфере ИБ

- **ParisRegionQCI** — проект по созданию сети квантовой связи для тестирования решений безопасной коммуникации. Сеть ParisRegionQCI соединяет несколько квантовых узлов, представленных партнерами проекта: от Plateau de Saclay (Thales, Institut d'Optique, Télécom Paris) до лаборатории LIP6 Университета Сорбонны в центре Парижа, через сайт Orange Gardens в Шатийоне[1].
- **Первая страна в ЕС**, где оператор связи (Orange) развернул **КРК-сеть для государственных нужд** (проекты ANSSI).

Инструменты поддержки и стимулирования

1. **Для страны актуальны все инструменты поддержки и стимулирования, указанные в блоке «Европейский союз».**
2. **Программа Développement des technologies innovantes critiques 4e édition[2] (Развитие критически важных инновационных технологий, IV издание), финансируемая Bpifrance[3]**. Помощь предоставляется в виде субсидий на проекты с уровнем готовности не менее 4 и с ожидаемым уровнем 7 (к концу проекта).

   Цель программы: разработка инновационных и суверенных решений, основанных на технологиях кибербезопасности, а также поддержка проектов по разработке новых подходов и средств защиты данных на протяжении всего их жизненного цикла (в т. ч. постквантовые инструменты).
3. **Программа ASTRID[4]**, запущенная в 2025 году Французским национальным агентством исследований (ANR) в партнерстве с Агентством оборонных инноваций (AID), национальным департаментом, прикрепленным к Французскому агентству оборонных закупок (DGA).

   Цель программы — поддержка развития научных работ, которые получили финансовую поддержку от Министерства вооруженных сил. Проекты должны касаться как гражданских, так и военных областей, в том числе квантовых технологий, кибербезопасности и пр.

[1] Orange
[2] Développement des technologies innovantes critiques 4e édition
[3] Bpifrance
[4] ASTRID

Исследование международного опыта развития квантовых и смежных технологий в ИБ

Нидерланды

Государственное регулирование и инициативы

- **Government-wide Quantum Cryptography Policy Framework (2025)** — новый обязательный стандарт шифрования для всех центральных органов власти. Суть инициативы: помочь организациям разработать эффективные политики в области криптографии, заранее подготовиться к потенциальным угрозам и принять необходимые меры.
- **Программа Quantum Delta NL**, которая при поддержке Фонда восстановления и устойчивости (RRF EU) создает национальную экосистему для квантовых инноваций.

Ключевые проекты в области квантовых технологий в сфере ИБ

- В 2024 году **международная исследовательская группа под руководством QuTech** (исследовательский центр, основанный в сотрудничестве TU Delft и Netherlands Organisation for Applied Scientific Research (TNO) **создала квантовую связь на расстоянии 25 км между голландскими городами Делфт и Гаага**. Команда разработала полностью независимые рабочие узлы и интегрировала их с развернутым оптоволоконным интернетом. Руководитель группы Рональд Хансон отметил, что расстояние в 25 км является рекордным для квантовых процессоров и это первый случай соединения таких процессоров в разных городах[1].

Инструменты поддержки и стимулирования

1. **Для страны актуальны все инструменты поддержки и стимулирования, указанные в блоке «Европейский союз».**
2. **Программа Quantum Delta NL SME[2]** — целевая грантовая линия для МСП внутри Quantum Delta NL (финансируется National Growth Fund) направлена на проекты по кибербезопасности, квантовым технологиям.

[1] Science Advances.
[2] Quantum Delta NL SME.

Исследование международного опыта развития квантовых и смежных технологий в ИБ

Швейцария

Государственное регулирование и инициативы

- **National Cyber strategy** (Национальная киберстратегия Швейцарии) (2023). Швейцария укрепляет свой статус глобального лидера в области знаний, образования и инноваций, в частности в сфере кибербезопасности. Страна самостоятельно оценивает киберугрозы в цепочках поставок, предвидит технологические достижения и быстро реагирует.
- **Швейцарская квантовая инициатива (SQI) (2022)** – мера поддержки исследований и инноваций, принятая Федеральным советом Швейцарии. Цель инициативы – укрепить позиции в области квантовых технологий и повысить ее конкурентоспособность на международном уровне.

Ключевые проекты в области квантовых технологий в сфере ИБ

- **ID Quantique (IDQ)**, мировой лидер в области квантово-безопасных решений безопасности, в 2021 году **запустила новую серию своего продукта четвертого поколения Cerberis XG** – первое решение из серии, направленное на обеспечение высочайшего уровня безопасности. Продукция используется правительствами, предприятиями, промышленными клиентами и академическими исследовательскими лабораториями в более чем 60 странах и на всех континентах. Усовершенствованные надежные компоненты безопасности, такие как обнаружение несанкционированного доступа, защищенный модуль памяти, а также новейшая технология QRNG от IDQ (чип IDQ20MC1 QRNG), которая обеспечивает доказанную случайность для всех связанных криптохранилищ[1].

Инструменты поддержки и стимулирования

1. **Программа BRIDGE Quantum Call 2025[2], финансируемая Swiss National Science Foundation (SNSF) и Swiss Innovation Agency (Innosuisse), направлена на продвижение прикладных исследований и инноваций в области квантовых технологий.**

   Цель программы – поддержка исследователей, которые работают по направлениям: квантовая коммуникация, квантовые вычисления, квантовое моделирование, квантовое зондирование и квантовая метрология.

2. **Для страны также доступны европейские программы Horizon Europe и Digital Europe.**

[1] ID Quantique.
[2] BRIDGE Quantum Call 2025.

Исследование международного опыта развития квантовых и смежных технологий в ИБ

Япония

Государственное регулирование и инициативы

- **Sixth Science, Technology and Innovation Basic Plan** (Шестой базовый план развития науки, техники и инноваций)
- **Vision of Quantum Future Society** (Концепция развития общества в эпоху квантовых технологий) (2022)
- **Quantum Technology Innovation Strategy Roadmap (2022)**
- **Integrated Innovation Strategy** (Комплексная инновационная стратегия) (2024)
- **Quantum Technology and Innovation Strategy** – QTIS (Стратегия исследований и разработок в области квантовых технологий) (2020)
- **Strategy of Quantum Future Industry Development** (Стратегия развития квантовой индустрии) (2023)

Ключевые проекты в области квантовых технологий в сфере ИБ

- **Cybertrust Japan**, ведущий центр сертификации в Японии, **интегрировал решение Quantum Origin от Quantinuum для генерации квантово-устойчивых ключе**й в свою платформу аутентификации IoT-устройств[1].

Инструменты поддержки и стимулирования

1. **Программа NEDO: K-Program (Программа развития ключевых технологий экономической безопасности), финансируемая New Energy and Industrial Technology Development Organization (NEDO), агентство правительства Японии[2].**

   Цель – повышение ситуационной осведомленности для сбора и анализа информации в киберпространстве, совершенствование оборонительных возможностей устройств и систем от кибератак, а также разработка и внедрение технологий и сред оценки для этих возможностей и технологий. Кроме того, разрабатываются квантовые информационно-коммуникационные технологии для обеспечения высокого уровня безопасности критически важной инфраструктуры.

2. **Открытый конкурс предложений по исследованиям и разработкам в области информационно-коммуникационных технологий (проект «Приоритетные ИКТ-технологии»), Министерство внутренних дел и коммуникаций (MIC)[3]**. В 2025 году приоритетная тема сформулирована как: «Исследования и разработки для раннего социального внедрения коммуникационной сети на основе квантовой криптографии (КРК-сети)». Проект направлен на: (1) продвижение технологии распределения квантовых ключей, (2) развитие технологии управления ключами в сети распределения квантовых ключей и (3) высокую функциональность квантовой криптографической сети связи и демонстрация интеграции.

[1] Quantinuum.
[2] NEDO.
[3] Приоритетные ИКТ-технологии.

Исследование международного опыта развития квантовых и смежных технологий в ИБ

Канада

Государственное регулирование и инициативы

- **National Quantum Strategy** (Национальная квантовая стратегия) (2023). Цель — определить будущее квантовых технологий в Канаде и создать тысячи рабочих мест. Три основных направления стратегии:

1. Квантовые вычисления и программное обеспечение. Сделать Канаду мировым лидером в разработке, внедрении и использовании этих технологий.
2. Квантовые коммуникации. Обеспечить Канаду национальной защищенной сетью квантовой связи и средствами постквантовой криптографии.
3. Квантовые сенсоры. Поддерживать канадских разработчиков и первопроходцев в использовании новых квантовых сенсорных технологий.

Ключевые проекты в области квантовых технологий в сфере ИБ

- **Open Quantum Safe (liboqs)** — проект с открытым исходным кодом, направленный на поддержку перехода к квантово-устойчивой криптографии. В 2024 году проект стал частью Альянса постквантовой криптографии (PQCA) Linux Foundation[1].

Инструменты поддержки и стимулирования

1. **Гранты** должны быть направлены на продвижение одной или нескольких миссий NQS путем разработки любой из следующих областей квантовых технологий или их комбинации: квантовые алгоритмы/шифрование, включая постквантовую криптографию, квантовые коммуникации, квантовые вычисления, квантовые материалы, квантовое зондирование. **Финансируются The Natural Sciences and Engineering Research Council of Canada (NSERC)[2]**:

- **Alliance Consortia Quantum** поддерживает развитие крупномасштабного сотрудничества канадских исследований в области квантовой науки и техники и обеспечивает сотрудничество между исследователями из университетов и организациями из частного, государственного или некоммерческого секторов.
- **Alliance International Catalyst Quantum** поддерживает канадских исследователей в развитии международного сотрудничества с другими исследователями из академического сектора в области квантовой науки и квантовых технологий.
- **Alliance International Collaboration Quantum** поддерживают канадских исследователей, сотрудничающих по проектам с международными исследователями из академического сектора.

2. **Программа Quantum Commercialization Program[3]**, финансируемая DIGITAL (Global Innovation Cluster) в рамках Национальной квантовой стратегии Канады совместно с отраслевыми партнерами и NGen Canada, направлена на коммерциализацию и внедрение квантовых технологий через пилотные проекты у реальных заказчиков. Критерий — решение конкретных бизнес-задач и выход на рынок. Направление Quantum Communications нацелено на обеспечение конфиденциальности и кибербезопасности страны через национальную сеть защищенных квантовых коммуникаций.

[1] Open Quantum Safe.
[2] NSERC.
[3] Quantum Commercialization Program.

Исследование международного опыта развития квантовых и смежных технологий в ИБ

Австралия

Государственное регулирование и инициативы

- **Cyber Security Strategy (2023–2030)**. В стратегии говорится о необходимости перехода к quantum-resilient encryption (квантово-устойчивой криптографии) для критически важных операторов к 2030 году. Она предусматривает поэтапный подход к реализации мер по кибербезопасности: от базовых усилий (2023–2025) до масштабирования киберустойчивости (2026–2028) и достижения глобального лидерства (2029–2030). В рамках второго этапа (2026–2028) планируется ускорить внедрение технологий, устойчивых к квантовым угрозам, и обеспечить безопасность систем шифрования.
- **National Quantum Strategy** (Национальная квантовая стратегия) (2023). Основная цель — к 2030 году сделать Австралию лидером в мировой квантовой индустрии.

Ключевые проекты в области квантовых технологий в сфере ИБ

- **Компания QuintessenceLabs выпустила PCIe-модуль qStream™ 100 — квантовый генератор случайных чисел 8 Гбит/с**. Модуль qStream™ 100 позволяет добавлять функцию генерации случайных чисел в существующие аппаратные HSM-хранилища ключей, что повышает безопасность криптографических операций. Также qStream™ 100 может напрямую интегрироваться с системой управления ключами и политиками QuintessenceLabs Trusted Security Foundation (TSF)[1].

Инструменты поддержки и стимулирования

1. **Программа Critical Technologies Challenge Program (CTCP)[2,3]** — федеральный грант, спонсируемый Департаментом промышленности, науки и ресурсов Австралии (DISR), который тестирует и доводит до демонстратора рыночно-ориентированные решения с использованием квантовых технологий для задач национальной значимости, в том числе ИБ. Программа реализуется в два раунда, каждый из которых состоит из двух этапов. Этап 1 — технико-экономическое обоснование, этап 2 — демонстрационный.
2. **Национальный доменный регулятор .au осуществляет финансирование исследований и разработок (Research & Development Program)** для двух проектов по защите шифрования, используемого системой доменных имен (DNS) от угрозы квантовых вычислений[4].
3. **Грант NIDG (National Intelligence Discovery Grants), финансируемый Office of National Intelligence (ONI)[5]**, содержит 9 направлений, в том числе гомоморфное и квант-базированное шифрование, новые квантовые технологии для поддержки мер безопасности и др.

[1] QuintessenceLabs.
[2] CTCP (Round 1/1).
[3] CTCP (Round 1/2).
[4] auDA.
[5] NIDG.

Исследование международного опыта развития квантовых и смежных технологий в ИБ

Израиль

Государственное регулирование и инициативы

- **Израильская национальная квантовая инициатива (INQI)**. Цель инициативы — содействовать сотрудничеству между научными кругами, промышленностью и государственными учреждениями для ускорения квантовых исследований, разработок и приложений. В рамках INQI, в частности, создан Израильский центр квантовых вычислений.

Ключевые проекты в области квантовых технологий в сфере ИБ

- **Компания QuantLR**, занимающаяся квантовым распределением ключей (КРК), **интегрировала свои технологии с сетевыми решениями NVIDIA для создания защищенного квантовыми технологиями дата-центра**. В рамках проекта система КРК QuantLR подключила и передала ключи шифрования двум сетевым интерфейсным картам (NIC) NVIDIA ConnectX-6. Для этого использовали интерфейс программирования приложений (API) на основе ETSI REST.
- **Компания HUB Security** предоставит Министерству обороны Израиля **новое решение квантовой безопасности для защиты конфиденциальной информации** в облачной среде. Компания сотрудничает с QuantLR.

Инструменты поддержки и стимулирования

1. **Для страны доступна европейская программа Horizon Europe.**
2. **В рамках трека MAGNET**[1], финансируемого Израильским управлением инноваций (Israel Innovation Authority), в мае 2025 года был предложен грант в области прикладных исследований среди консорциумов, в том числе консорциума Post-Quantum Communication (PQC)[2]. Его цель — разработка прорывных технологий для решения проблем безопасности, шифрования и приватности в эпоху квантовых вычислений.

[1] MAGNET
[2] PQC

Исследование международного опыта развития квантовых и смежных технологий в ИБ

Южная Корея

Государственное регулирование и инициативы

- **National Quantum Strategy (2023)**. Цель стратегии — к 2035 году занять лидирующее положение в глобальной квантовой экономике.

Ключевые проекты в области квантовых технологий в сфере ИБ

- **Национальная «квантово-безопасная» сеть, построенная** в 2022 году: SK Broadband и ID Quantique связали 48 государственных ведомств по 800-километровому кольцу, внедрив КРК как штатную услугу шифрования. Цель проекта — защита чувствительной информации и коммуникаций между важными государственными учреждениями.
- **Nokia и SK Broadband в августе 2024 года развернули квантовобезопасную выделенную линию для Корейской гидроатомной электростанции** (Korea Hydro и Nuclear Power (KHNP). Цель проекта — улучшить безопасность данных и защитить сеть KHNP от существующих и возникающих киберугроз, в том числе кибератак на основе квантовых вычислений. Южная Корея — одна из немногих стран с КРК в энергосекторе[1].

Инструменты поддержки и стимулирования

1. **Госпрограмма «Поддержка пилотной миграции к постквантовой криптографии 2025»[2,3] в трех отраслях: энергетика / здравоохранение / госадминистрирование** нацелена на обеспечение безопасности процедуры перехода на криптографические системы в каждом секторе промышленности, а также на проверку совместимости и взаимодействия с существующими системами. Заказчик — MSIT (Миннауки и ИКТ), оператор — KISA.
2. **Госпрограмма «ICT R&D 2025 (квантовый блок)[4]: «Расширение промышленного внедрения квантовой криптографической связи и разработка технологий следующего поколения»** нацелена на снижение стоимости и масштабирование КРК-сетей , а также на R&D следующего поколения квантовой криптографии. Заказчик — MSIT (Министерство науки и ИКТ), оператор — IITP. В 2025 году предусмотрены две линии — «Индустриальное внедрение квантовой криптографии» (2 проекта) и «Следующее поколение квантовой криптографии» (2 проекта).

[1] Nokia
[2] Поддержка пилотной миграции к постквантовой криптографии 2025
[3] KISA
[4] ICT R&D 2025

Исследование международного опыта развития квантовых и смежных технологий в ИБ

Индия

Государственное регулирование и инициативы

- **Стандарт на общие требования к квантовым генераторам случайных чисел (QRNG)**
- **Центр электросвязи (TEC) выпустил стандарты** «Квантовая система распределения ключей» и «Квантово-безопасные и классические криптографические системы».
- **National Quantum Mission** (2023–2031) предусматривает:
  - Разработку квантовых компьютеров промежуточного масштаба 50–1000 физических кубитов за 8 лет на различных платформах.
  - Спутниковую безопасную квантовую связь между наземными станциями в диапазоне 2000 км в пределах Индии, дальнюю безопасную квантовую связь с другими странами, междугороднее распределение квантового ключа на расстоянии более 2000 км.

Ключевые проекты в области квантовых технологий в сфере ИБ

- В 2022 году **DRDO и IIT Delhi продемонстрировали КРК по волокну**, которое заключалось в установке безопасной квантовой связи между городами Праяградж и Виндхьячал на расстоянии более 100 км. Для этого использовали оптическое волокно коммерческого качества. Кроме того, ученые разработали источник одиночных фотонов для квантовой связи в свободном пространстве со скоростью более 4 млн фотонов в секунду[2].
- Индия **развивает отечественные фотонные источники и детекторы (SNSPD на LNOI)** — ставка на полную технологическую независимость в «железе» для КРК[1].

Инструменты поддержки и стимулирования

1. **Грантовая государственная программа от Ministry of Electronics & IT (MeitY) по кибербезопасности[2]**, нацеленная на инновации и разработку местных технологий, ведущих к их коммерциализации. Основные направления: безопасность оборудования, кибербезопасность в КИИ, шифрование и криптография (в том числе системы и протоколы, готовые к квантовой кибербезопасности), безопасность транспортных средств и др.
2. **Telecom Technology Development Fund (TTDF) — грантовая поддержка Минсвязи Индии (DoT)** для НИОКР и пилотов в телеком-технологиях. В 2024 году под TTDF запущены два профильных направления для квантовой ИБ[3]: **QEA — Quantum Encryption Algorithm** (конкурс на разработку «индийского квантового алгоритма шифрования»), и **Quantum Standardization & Testing Labs** (конкурс на создание/развитие лабораторий стандартизации и испытаний для квантовой связи — интероперабельность, надежность, безопасность).

[1] Ministry of Defence.
[2] MeitY.
[3] TTDF.

Исследование международного опыта развития квантовых и смежных технологий в ИБ

ОАЭ

Государственное регулирование и инициативы

- **Совет по кибербезопасности ОАЭ разрабатывает новые политики по кибербезопасности**. Нововведения должны охватывать «облачные вычисления и безопасность данных», «безопасность Интернета вещей» и «центры операций по кибербезопасности». По информации на февраль 2025 года, глава Совета кибербезопасности ОАЭ, доктор Мухаммед Аль Кувейти, заявил, что политика в сфере криптографии будет реализована в первом квартале 2025 года. Кроме того, Совет работает над разработкой новых стандартов кибербезопасности, чтобы повысить эффективность соблюдения установленных требований учреждениями и мер безопасности.

Ключевые проекты в области квантовых технологий в сфере ИБ

- В 2024 году **Technology Innovation Institute (TII) и Космическое агентство ОАЭ показали первую национальную КРК-схему:** наземная линия + оптическая станция ADQOGS в Абу-Даби для будущей спутниковой раздачи ключей. Первая в арабском мире и крупнейшая в регионе MENA. С ее помощью обеспечивается безопасная оптическая связь и соединение ОАЭ с глобальной квантовой сетью[1].

Инструменты поддержки и стимулирования

1. **В ОАЭ нет объявленных государственных грантов / субсидий / налоговых льгот, направленных на квантовые технологии в сфере информационной безопасности.** Однако правительство нацелено развивать квантовые технологии через инфраструктуру и пилотные площадки:

- ADGM, ADGM Academy (ADGMA), Технологический инновационный институт (TII), Hub71 и ASPIRE совместно запустили первый в стране испытательный стенд для квантово-безопасных коммуникаций. Инициатива будет изучать способы передачи сверхбезопасных данных с использованием квантовых технологий. Сеть действует как «живая лаборатория» для высокозащищенных от несанкционированного доступа средств связи в эпоху нарастающей киберугрозы и утечки конфиденциальности данных[2].

[1] Technology Innovation Institute
[2] ADGM

Основные результаты и планы реализации «Дорожных карт» развития высокотехнологичных областей «Квантовые коммуникации» и «Квантовые вычисления» в части ИБ[1]

Реализация дорожной карты «Квантовые коммуникации» до 2030 года

Развитие цифровой экономики и растущие угрозы в сфере ИБ требуют не просто усиления существующих средств защиты, а перехода к принципиально новым технологическим платформам. Квантовые коммуникации становятся одним из таких решений: они обеспечивают недостижимый ранее уровень защищенности передачи данных, устойчивый к взлому даже при появлении квантовых вычислений.

Ключевые вызовы:

- Создание индустрии квантовых коммуникаций и рынка сервисов.
- Достижение технологического суверенитета (магистральные, абонентские, атмосферные сети).
- Реализация технологического потенциала в виде продуктов.
- Обеспечение развития экосистемы: нормативные акты, стандарты, кадры, кооперация.

В рамках дорожной карты «Квантовые коммуникации» до 2030 года создаются сети нового поколения, развивается рынок услуг и ведется работа по нормативному и кадровому обеспечению. Уже сейчас ведется масштабное тестирование квантовых решений в критической инфраструктуре и разрабатываются новые сервисы на базе квантовой передачи ключей.

Результаты к 2024 году		Цели к 2030 году
Создано более **7000** км магистральной квантовой сети.	**Магистральная инфраструктура**	**15 000** км магистральной сети, созданы клиентские мультивендорные сети.
Разработано **18** образцов оборудования квантовых коммуникаций (**5** опытных и **13** экспериментальных).	**Технологии**	Более **10** перспективных технологий области квантовой связи.
Подано **78** заявок на регистрацию РИД, **46** статей приняты к публикации.	**Коммерциализация продуктов**	В **3** раза больше созданных результатов интеллектуальной деятельности (более **150** патентов).
Подготовлено **700+** специалистов в **30+** вузах.	**Кадры**	**100 %** кадровой обеспеченности, **x2** рост экосистемы квантовых коммуникаций.
Создан Центр квантовых технологий ОАО «РЖД».	**Масштабируемость услуг**	Сервис оператора связи с SLA и биллингом, более **4** млн пользователей информационных систем.
Выполняется **25** НИОКР, включая создание оборудования, компонентной базы, перспективных технологий.	**Развитие линейки устройств**	Коммерциализация сервисов, обеспечена локализация **80 %** номенклатуры критически важных оптических компонентов.
Правительством РФ утверждена Концепция регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года.	**Нормативная база**	Сформирована система нормативного регулирования отрасли и технической стандартизации (принято более **35** НПА и стандартов).

[1] ОАО «РЖД»

Основные результаты и планы реализации «Дорожных карт» развития высокотехнологичных областей «Квантовые коммуникации» и «Квантовые вычисления» в части ИБ[1]

Реализация дорожной карты по квантовым вычислениям: от тестов — к экономике и ИБ

Современные вызовы в области кибербезопасности требуют комплексного подхода, включающего технические решения и разработку новых стандартов защиты информации. Развитие квантовых вычислений и квантового ИИ открывает новые возможности для защиты данных от киберпреступников. В мире уже осуществляются тестирование новых подходов: от квантовых моделей машинного обучения для обнаружения кибератак до полностью гомоморфных схем шифрования с использованием квантовых алгоритмов. Из-за несовершенства существующих квантовых вычислительных устройств преждевременно говорить о внедрении подобных решений в цифровую инфраструктуру, однако в ближайшем будущем они с большой вероятностью станут неотъемлемой частью систем защиты информации

Ключевые вызовы:

- Фокус на информационную безопасность
- Переход от прототипов к промышленным вычислителям
- Создание инфраструктурной и научной базы
- Ликвидация технологического разрыва с мировыми лидерами

В рамках реализации дорожной карты «Квантовые вычисления» исследования в ИБ в 2020–2024 гг. не проводились. В актуализированном проекте на 2025–2030 гг. предусмотрено выполнение мероприятий по разработке и актуализации комплекса предложений и мер по обеспечению информационной и кибербезопасности при осуществлении квантовых вычислений

Результаты к 2024 году		Цели к 2030 году
Разработаны прототипы квантовых процессоров на **50** кубитов, фотонный чип — **35** кубитов, сверхпроводники — **16** кубитов	**Кубиты**	Создание квантового процессора на **300** кубитов
Создано **34** квантовых алгоритма	**Алгоритмы**	Более **85** квантовых алгоритмов
Выполнены **7** проектов в **5** организациях по оптимизации и моделированию	**Пилотные проекты**	Проверка не менее **100** научных гипотез, внедрение в реальный сектор
Разработана облачная платформа для тестового доступа	**Доступность технологий**	**10 000** пользователей квантового сервиса, облачная платформа с УГТ **9**
Квантовые вычислители — экспериментальные образцы	**УГТ**	УГТ **7** для процессора, УГТ **9** для облачной платформы
Общий бюджет: около **24** млрд руб.	**Финансирование**	**29,3** млрд руб. (из них **14,6** млрд руб. — федеральный бюджет)
Центры у ГК «Росатом», АНО «Платформа национальной технологической инициативы», Московский государственный университет имени М. В. Ломоносова, Российский квантовый центр	**Центры компетенций**	**85+** организаций участвуют в проверке гипотез и внедрении решений

[1] ГК «Росатом»

Рекомендации по обеспечению мер поддержки и стимулирования развития квантовых и смежных технологий в России (на основании внутреннего и внешнего бенчмарка)

В условиях стремительного развития сферы квантовых и смежных технологий и связанными с ними угроз, ведущие страны мира реализуют комплексные меры поддержки с целью обеспечения ИБ. Эти меры охватывают нормативную, образовательную, исследовательскую и индустриальную сферы. Принятие указанных мер в России позволит занять передовые позиции в глобальной гонке, связанной с квантовыми технологиями, обеспечить непрерывную защиту критической инфраструктуры, а также выйти в число лидеров в сфере ИБ. По результатам изучения практик стран-лидеров сформулированы рекомендации по их внедрению в Российской Федерации.

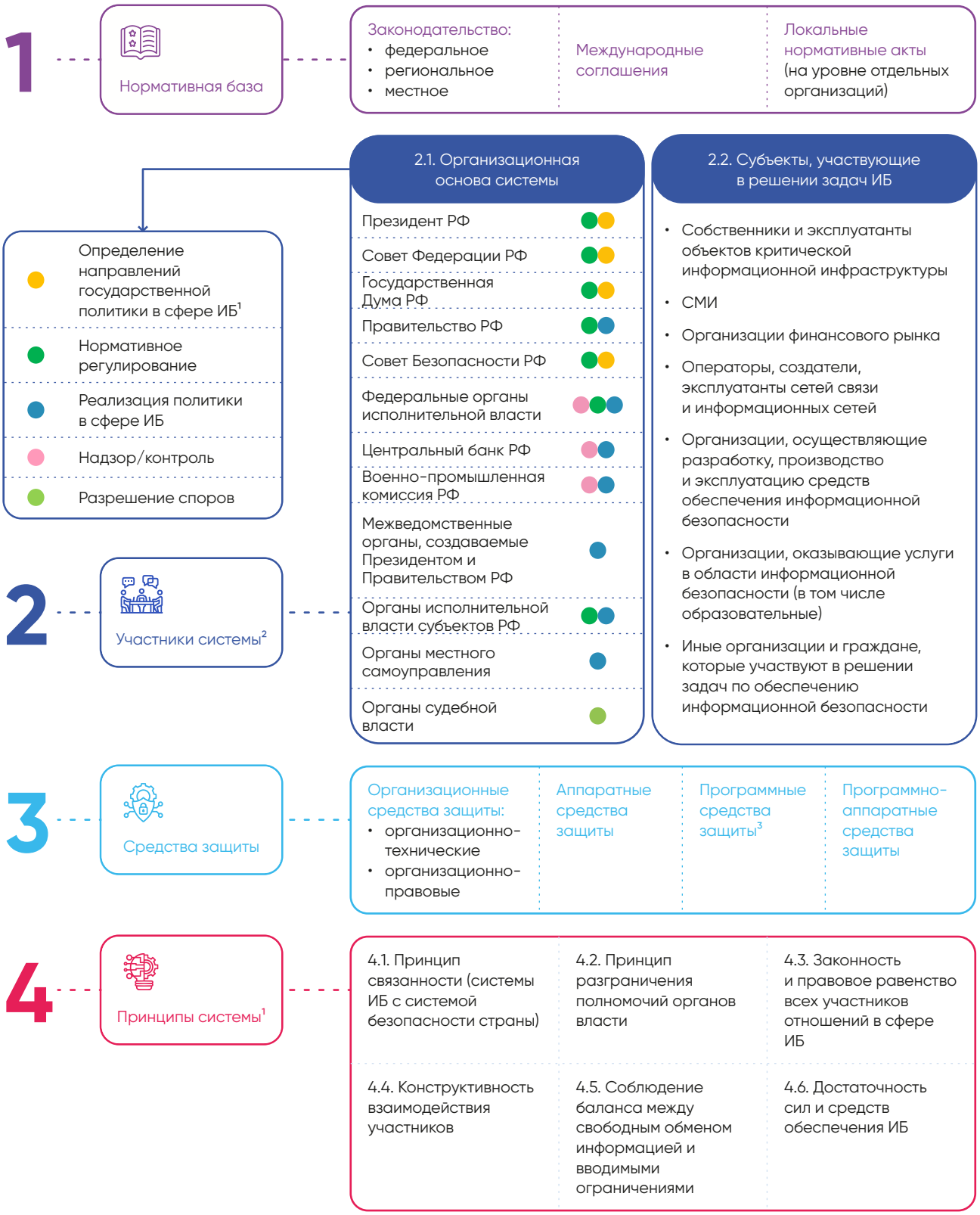
- Предоставление адресных мер поддержки[1] (в т. ч. на уже внедренные технологии, которые описаны и сданы в контролирующие органы) в целях обеспечения масштабирования решений.
- Установление регуляторных требований к отказоустойчивости ИБ-систем с учетом квантовой угрозы. Внедрение обязательного аудита систем на устойчивость к квантовым атакам.
- Создание квантовых кластеров – локальных площадок, где собираются компании, исследовательские центры, другие организации для практики и обмена опытом в сфере квантовых технологий (с прикреплением индустриальных партнеров для пилотирования решений).
- Создание национальной ассоциации развития квантовых технологий (функции по координации, обеспечению «открытого диалога», определению тематик НИОКР, поддержке разработки и внедрения решений на базе КТ (на примере НКЛ в области КВ, КК и КС).
- Установление экспериментальных правовых режимов (ЭПР), способствующие эффективной разработке и внедрению квантовых технологий.
- Включение квантовых ИБ-решений в обязательный перечень для критической инфраструктуры компаний, организаций госсектора.
- Создание программы поддержки стартапов и масштабирования производства/оказания услуг в сфере квантовых технологий в ИБ (на примере программы акселерации Росатома для КВ).
- Создание программ с заинтересованными странами по совместной разработке и тестированию квантовых решений с учетом механизмов для миграции иностранных ИБ- и квантовых специалистов.
- Создание полигонов для тестирования решений в условиях, близких к реальным.
- Создание отраслевых дорожных карт для внедрения квантовых и смежных технологий в сфере ИБ (в том числе разработка карт технологических кооперации).

[1] 1) Кредитование проектов внедрения КТ по субсидируемой процентной ставке. 2) Гранты в форме субсидий на реализацию научными центрами прорывных исследований в сфере КТ. 3) Субсидии на компенсацию части затрат на проведение НИОКР по квантовым технологиям в рамках реализации инновационных проектов. 4) Налоговое стимулирование в сфере КТ (преимущества по налогу на прибыль для организаций, которые создают, приобретают и внедряют продукты и услуги , относящиеся к КТ). Источник: Консолидированная позиция экспертного сообщества Центра технологического лидерства при АНО «Цифровая экономика» в рамках проведенных экспертных сессий и глубинных интервью.

Развитие системы ИБ с помощью квантовых и смежных технологий на уровне организаций

Принципы построения системы организации ИБ на уровне государства и бизнеса

Принципы построения системы информационной безопасности на уровне государства



[1] Информационная безопасность.
[2] Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента РФ от 05.12.2016 № 646.
[3] Как локальные, так и облачные.

Принципы построения системы информационной безопасности на уровне бизнеса

1. Цели создания системы ИБ[1] на уровне бизнеса

- Защита конфиденциальной информации (как от внешних, так и внутренних угроз)
- Обеспечение подлинности и актуальности информации
- Обеспечение целостности информации
- Обеспечение прозрачности и постоянного совершенствования процессов ИБ
- Обеспечение сохранности, доступности и подотчетности информации
- Эффективное управление рисками в сфере ИБ

2. Последовательность этапов создания системы ИБ на уровне бизнеса

Этап 1. Проведение аналитики

- Оценка текущего уровня ИБ[2] в компании
- Выявление уязвимых (с т. з. ИБ) мест в бизнес-процессах
- Определение достаточности внутренних компетенций для построения СИБ[2]
- Исследование зарубежных и российских лучших практик построения СИБ
- Определение оптимальной бизнес-модели компании, соответствующей требованиям ИБ
- Оценка рисков построения СИБ
- Разработка требований к оптимальной конфигурации СИБ

Этап 2. Формирование документов для построения системы

- Формирование дорожной карты построения СИБ
- Формирование алгоритма процессов СИБ
- Формирование организационной структуры в соответствии с требованиями выстраиваемой СИБ
- Формирование корпоративной политики ИБ компании на базе российского и зарубежного опыта (в том числе принятие ЛНА[3])

Этап 3. Построение системы

- Выбор наиболее подходящих решений и технических средств обеспечения в сфере ИБ
- Корректировка внутренних процессов компании в соответствии с выбранными решениями и планируемой СИБ (при необходимости)
- Пилотное тестирование построенной СИБ
- Корректировка СИБ по результатам пилотного тестирования[4]
- Полноценный запуск СИБ
- Проведение обучения сотрудников компании по использованию и обслуживанию решений в рамках новой СИБ

Этап 4. Контроль и совершенствование системы[5]

- Техническое обслуживание СИБ
- Постоянный аудит функционирования СИБ и устранение выявленных недостатков
- Непрерывный мониторинг появления новых и совершенствования текущих киберугроз
- Поиск новых и усовершенствование текущих решений, позволяющих оптимизировать и повысить эффективность СИБ
- Обучение сотрудников компании противодействию новым угрозам в сфере ИБ

[1] Информационная безопасность.
[2] Система информационной безопасности.
[3] Локальные нормативные акты.
[4] При необходимости.
[5] На постоянной основе.

Основные условия для внедрения квантовых и смежных технологий в систему ИБ в рамках организации

Перед внедрением квантовых технологий в систему ИБ любой организации, необходимо провести сложную и достаточно капиталоемкую подготовку, в том числе:

Со стороны организации

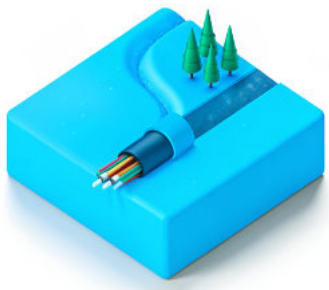
- Разработка или адаптация существующих (масштабируемых) квантово-устойчивых алгоритмов
- Защита инфраструктуры — подготовка сетей и системы к переходу к квантово-устойчивым технологиям, в том числе:
  - Создание устойчивых и надежных квантовых каналов связи, что требует значительных затрат и ресурсов
  - Адаптация существующих систем безопасности и разработки, что потребует значительного обновления инфраструктуры
- Обучение сотрудников новым методам защиты

Со стороны государства

- Разработка стандартов и подходов к ИБ при использовании квантовых технологий (в том числе на базе международного сотрудничества)
- Разработка и утверждение норм регулирования применения квантовых технологий в ИБ

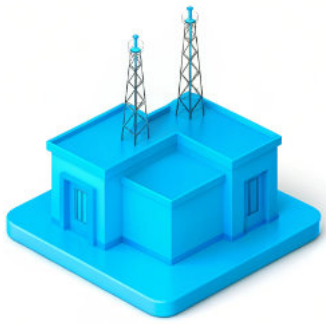
Существует несколько видов оптических линий связи, в которые могут быть интегрированы квантовые сети:

ВОЛС



ВОЛС (волоконно-оптическая линия связи) — это система передачи данных, в которой в качестве среды используется оптическое волокно, включая пассивные компоненты (кабель, кросс, сплиттеры) и активные (лазеры/модуляторы, приемники, усилители).

АОЛС



АОЛС (атмосферная оптическая линия связи) — вид связи, позволяющий передавать данные между объектами в атмосфере, имея оптическое соединение без использования оптоволокна. Эффективна на дистанции до ~3 км, но чувствительна к погодным условиям.

БОЛС

БОЛС (беспроводные оптические лазерные системы) — это космические лазерные каналы, использующие электромагнитные волны оптического диапазона (как правило, инфракрасные) для передачи данных между объектами через атмосферу.

Основные условия для внедрения квантовых и смежных технологий в систему ИБ в рамках организации

Базовые условия для развертывания квантовых сетей: среда передачи ВОЛС (волоконно-оптическая линия связи)

ТЕХНИЧЕСКИЕ АСПЕКТЫ

- **Минимизация уровня оптических потерь** — при передаче по оптоволокну часть квантового сигнала теряется. Для работы сетей необходимо, чтобы уровень потерь был минимальным, так как превышение допустимого значения резко сокращает дальность (обычно до менее 100 км).
- **Обеспечение стабильной скорость передачи** — из-за шумов и особенностей детекторов скорость ограничена килобитами в секунду. Условием внедрения является обеспечение стабильной пропускной способности, достаточной для практического обмена квантовыми ключами.
- **Обеспечение совместимости с существующей инфраструктурой**.

ЭКОНОМИЧЕСКИЕ АСПЕКТЫ

- **Доступная стоимость развертывания** — реализация квантовой сети требует значительных затрат на оборудование, монтаж и обслуживание.
- **Целесообразность** применения квантовых технологий для решения задач организации того или иного типа (присутствие положительного экономического эффекта).

ВЛИЯНИЕ ОКРУЖАЮЩЕЙ СРЕДЫ

- **Соблюдение изоляции от погодных влияний** — волокно находится под землей или в герметичных каналах. Ни дождь, ни снег, ни ветер не оказывают заметного влияния на качество квантового сигнала. Это делает ВОЛС наименее зависимой от внешней среды технологией.

ПРАВОВЫЕ АСПЕКТЫ

- **Соблюдение требований законодательства** о сертификации оборудования, соблюдение норм электромагнитной совместимости, а также правил безопасности при монтаже и эксплуатации. Также могут потребоваться согласования с операторами связи и муниципальными властями. Регулирование близко к существующим правилам телеком-инфраструктуры.

ПРИМЕРЫ УСПЕШНЫХ ПРОЕКТОВ

- **Пилотный участок магистральной квантовой сети (ПУ МКС)** — в 2019–2022 годах Университетом ИТМО создана и запущена первая в России квантовая магистраль, протянувшаяся на 700 км (с применением доверенных узлов), обеспечивающая генерацию квантовых ключей и защиту данных в реальных условиях эксплуатации[1].
- **Проект международной исследовательской группы QuTech** — в 2024 году на расстоянии 25 км между голландскими городами Делфт и Гаага была создана квантовая связь при интеграции независимых рабочих узлов с развернутым оптоволоконным интернетом[2].

[1] ПРОквант.

[2] TU Delft.

Основные условия для внедрения квантовых и смежных технологий в систему ИБ в рамках организации

Базовые условия для развертывания квантовых сетей: среда передачи АОЛС (атмосферная оптическая линия связи)

ТЕХНИЧЕСКИЕ АСПЕКТЫ

- **Обеспечение совместимости длин волн** — используют ближний ИК-диапазон (~1550 нм) и видимый свет, но длины волн могут отличаться, что требует дополнительных оптических преобразователей.
- **Обеспечение защиты оборудования** — приемопередатчики размещают в защищенном, обогреваемом корпусе, а объектив приемника закрывают блендой для защиты от прямых солнечных лучей.
- **Обеспечение адаптивной настройки системы** — мощность передатчика и чувствительность приемника корректируются на основе статистических данных и текущих параметров среды.

ЭКОНОМИЧЕСКИЕ АСПЕКТЫ

- **Оптимизация стоимости и сложности оборудования** — требуется закупка сложных лазерных передатчиков, оптических трекеров, усилителей и систем коррекции атмосферных искажений. Установка на здания и вышки требует дополнительных инженерных согласований и устойчивых площадок. Хотя это дешевле спутников, стоимость выше, чем у ВОЛС.

ВЛИЯНИЕ ОКРУЖАЮЩЕЙ СРЕДЫ

- **Снижение затухания сигнала** — погодные явления (туман, дождь) вызывают ослабление сигнала из-за рассеяния на частицах в атмосфере и поглощения фотонов молекулами воздуха.
- **Учет атмосферной турбулентности** — она влияет на распространение оптического луча, изменяя или отклоняя его, а также расширяя оптический пучок.
- **Минимизация солнечной засветки** — естественное освещение может влиять на прием сигнала, особенно при высокой интенсивности фонового излучения.

ПРАВОВЫЕ АСПЕКТЫ

- **Соблюдение ограничений по использованию оптических и инфракрасных источников** — в том числе лазеров, влияющих на авиацию. Также требуются разрешения на установку на высотных зданиях и использование спектра. Однако использование оборудования АОЛС не требует каких-либо проектных, согласовательных, лицензионных мер и оплаты за использование радиочастотного спектра, так как применяет те частоты, на которые не требуется разрешение.

ПРИМЕРЫ УСПЕШНЫХ ПРОЕКТОВ

- **Эксперимент по беспроводной передаче квантового ключа шифрования в открытом пространстве** — ученые Московского технического университета связи и информатики (МТУСИ) и специалисты компаний ООО «КуРэйт» и «Мостком» провели эксперимент по передаче ключа на 180 и 3100 метров с использованием АОЛС[1].
- **Гибридная технология передачи квантовых ключей** — АО «СМАРТС» совместно с Университетом ИТМО при поддержке Минобрнауки России, в одном из испытаний передавали квантовую информацию по оптоволокну, а затем по атмосферному оптическому каналу длиной 30–40 м. Это позволило использовать одновременно АОЛС и оптоволокно, что повысило точность взаимного позиционирования передатчика и приемника[2].

[1] N + [1]

[2] АО «СМАРТС»

Основные условия для внедрения квантовых и смежных технологий в систему ИБ в рамках организации

Базовые условия для развертывания квантовых сетей: среда передачи БОЛС (беспроводные оптические лазерные системы)

ТЕХНИЧЕСКИЕ АСПЕКТЫ

- **Минимизация инфраструктурных ограничений** – современные линии связи, например оптоволоконные кабели, не позволяют создать квантовые сети по всей России с учетом особенностей климата и географии. В связи с этим требуются спутниковые линии квантовой связи.
- **Обеспечение передачи фотонов на большие расстояния** – одиночные фотоны меняют свои состояния или поглощаются средой, поэтому сложно передать квант по оптоволоконному кабелю на расстояние свыше 200 км.

ЭКОНОМИЧЕСКИЕ АСПЕКТЫ

- **Минимизация стоимости разработки** – необходимость в специализированном оборудовании, таком как криогенные системы и высокоточные измерительные приборы, делает проектирование и развертывание квантовых систем экономически затратным, особенно на начальном этапе.
- **Обеспечение интеграции с существующей инфраструктурой**, которая не предназначена для квантовых сигналов и требует значительных модификаций или создания полностью новой инфраструктуры.

ВЛИЯНИЕ ОКРУЖАЮЩЕЙ СРЕДЫ

- **Снижение влияния атмосферных условий на космические каналы связи** – в космосе погодных условий нет, но атмосферное окно в нижней части канала (между станцией и спутником) подвержено облачности, инверсии температур, влажности. Наземные станции не могут принимать сигнал в условиях сильного дождя или плотной облачности.
- **Снижение влияния внешней среды** – в городских условиях на оптоволоконные кабели влияют перепады температур, что может вызывать ошибки при передаче данных.

ПРАВОВЫЕ АСПЕКТЫ

- **Формирование правового института** – необходимость создания механизма, который регулирует использование квантовых коммуникаций в существующих сетях связи и при создании новых сетей.
- **Разработка национальных стандартов**, которые устанавливают требования к сетям квантовых коммуникаций, оборудованию и ПО.
- **Сертификация оборудования** – для сохранения высокого уровня информационной безопасности требуется система сертификации оборудования, включая сертификацию отдельных его элементов.

ПРИМЕРЫ УСПЕШНЫХ ПРОЕКТОВ

- Российские ученые осуществили первый в России эксперимент по квантово-криптографической передаче данных между Россией и Китаем. Использование китайского квантового коммуникационного спутника «Мо-цзы» обеспечило передачу зашифрованных ключей на расстоянии свыше 3 800 км. С помощью специально разработанной российскими специалистами наземной станции был выполнен обмен зашифрованными изображениями размером 256×64 пикселей с партнерской станцией в Наньшане, Китай, продемонстрировав значимый прогресс в области международной квантовой коммуникации[1].

[1] SecurityLab

Обеспечение когерентности и согласования состояний в квантовых системах

Типы когерентности и согласования

- **Для квантовой связи** — требуется временная и фазовая когерентность источников фотонов и детекторов, чтобы обеспечивать корректное совпадение битов ключа.
- **Для квантовых вычислений** — согласование фаз и частот локальных осцилляторов, управляющих кубитами, для обеспечения устойчивости суперпозиции.
- **Для систем квантового распределения ключей (КРК)** — согласовывают аппаратуру, чтобы аппаратура получателя определяла, в какой момент времени прикладывать напряжение к фазовому модулятору.

Примеры инженерных решений

- **Устройство для систем КРК на боковых частотах в топологии типа «звезда»** содержит модуль отправителя с импульсным источником когерентного излучения и светоделителем, который разделяет излучение на оптический канал и квантовый канал, которые подключаются к модулю получателя через волоконно-оптический тракт.
- **Система одиночных фотонов с помощью атомной квантовой памяти** — фотоны генерируются в случайное время, один из них сохраняется в квантовой памяти с запоминающим импульсом, а второй поступает в линию задержки оптического волокна, после чего фотон, сохраненный в памяти, извлекается синхронно с фотоном, поступившим в линию задержки, с помощью второго, поискового, импульса.
- **Волоконно-оптический интерферометр** применяется в системах КРК для интерференции и компенсации фазы импульсов.
- **Квантовый повторитель** — промежуточный узел, который позволяет пошагово распространять запутанность по сегментам сети.

Перспективы развития

- **Создание квантовых сетей с когерентной связью** — например, сетей, которые будут поддерживать глобальное покрытие околоземного космического пространства и иметь несколько узлов с тысячами кубитов (атомов) в каждом, что обеспечит стабильность частоты на уровне в сто раз лучше классических аналогов.
- **Развитие квантовых повторителей (ретрансляторов)** — промежуточных узлов, которые сами являются квантовыми системами с памятью, позволит пошагово распространять запутанность по сегментам сети, что важно для создания масштабного квантового интернета.
- **Применение квантовой памяти** позволит хранить и обрабатывать квантовую информацию.

Подходы к внедрению квантовых технологий в существующие системы информационной безопасности

Этапы подготовки организаций к рискам кибербезопасности, связанных с квантовыми вычислениями

1 этап

Выполнение количественной оценки риска

- Определение и классификация данных с высоким уровнем риска, которые могут стать целью атак по принципу «собери сейчас, расшифруй позже».
- Замена протоколов шифрования для данных с длительным сроком хранения (например, контрактные документы, интеллектуальная собственность).

2 этап

Переход на крипто-гибкость

- Внедрение гибких криптосистем для возможности перехода в любой момент на квантово-устойчивое шифрование.
- Сотрудничество с поставщиками услуг кибербезопасности, которые уже экспериментируют с алгоритмами постквантовой криптографии.

3 этап

Инвестиции в решения, устойчивые к квантовым воздействиям

- Внедрение КРК для защиты обмена ключами.
- Использование квантовых генераторов случайных чисел для создания абсолютно случайных ключей шифрования.
- Обновление аппаратных модулей безопасности для поддержания квантово-устойчивых криптографических алгоритмов.

4 этап

Мониторинг стандартов и их соответствия

- Постоянный мониторинг стандартов в области постквантовой криптографии для обеспечения соответствия новейшим протоколам квантовой безопасности.
- Работа с экспертами по кибербезопасности для формирования плана перехода на квантово-безопасные технологии.

Принципы

Уделение первостепенного внимания информированности и просвещению персонала в области квантовых технологий, чтобы ключевые заинтересованные стороны понимали потенциальные последствия и возможности.

Инвестиции в исследованиях и разработках для изучения квантовых технологий и их применения в своей отрасли.

Сотрудничество между государственным и частным секторами может ускорить разработку стандартов и рекомендаций, обеспечивающих безопасное и эффективное применение квантовых технологий.

Переход на квантово-устойчивые методы шифрования должен стать частью долгосрочных стратегий кибербезопасности для защиты от будущих квантовых угроз.

Формирование кадров, владеющих навыками квантовых вычислений и шифрования, что потребует инвестиций в программы подготовки и обучения.

Построение безопасной системы передачи данных в организации

Характеристики безопасной системы передачи данных[1]

Для обеспечения устойчивой и надежной передачи данных организациям требуется система, обладающая ключевыми характеристиками. Эти свойства защищают от актуальных и перспективных угроз — включая атаки, утечку данных, несанкционированный доступ и др.

1 

Конфиденциальность — свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов. Доступ к данным предоставляется только сотрудникам, имеющим на это разрешение.

Зачем: защищает данные от утечек, шпионажа, внутреннего злоупотребления.

2 

Целостность — свойство сохранения правильности и полноты активов. Сохранность заданного системой объема и вида информации.

Зачем: предотвращает подмену, повреждение или несанкционированное изменение данных.

3 

Доступность данных — свойство быть доступным и готовым к использованию по запросу авторизованного субъекта. Возможность оперативного, беспрепятственного доступа к необходимым сведениям.

Зачем: исключает задержки и недоступность критических данных.

4 

Подлинность — свойство, гарантирующее, что субъект или ресурс идентичен заявленному источнику.

Зачем: предотвращает подделку источников, фальсификацию.

5 

Достоверность — свойство соответствия предусмотренному поведению и результатам.

Зачем: исключает ошибки, ложные значения, устаревшие сведения.

6 

Неотказуемость — способность удостоверять имевшее место событие или действие и их субъекты так, чтобы это событие или действие и субъекты, имеющие к нему отношение, не могли быть поставлены под сомнение.

Зачем: обеспечение безопасности коммуникации, в частности в вопросах, касающихся права и финансов.

7 

Подотчетность — ответственность субъекта за его действия и решения. Возможность узнать, кто сейчас работает с информацией, вносит в нее изменения.

Зачем: обеспечивает аудит, расследование инцидентов, юридическую защиту.

[1] ГОСТ Р ИСО/МЭК 27000-2012

Проектирование квантово-безопасной сети

Ключевые подходы и компоненты, позволяющие выстраивать квантово-устойчивые и безопасные системы передачи данных в организации после принятия профильных государственных стандартов и сертификации решений.

Ввод в промышленную эксплуатацию будет возможен после принятия новых государственных стандартов по постквантовой криптографии и последующей сертификации решений

1. Гибридные криптографические системы

Большинство организаций не могут сразу заменить всю свою инфраструктуру безопасности, поэтому гибридный подход является лучшим решением:

- Использование гибридного TLS (безопасность транспортного уровня), который сочетает в себе традиционное шифрование (RSA, ECC) с постквантовой криптографией. Применяется на этапе перехода, пока стандарты постквантовой криптографии не утверждены повсеместно.
- Работа с поставщиками облачных услуг, предлагающими гибридные квантово-устойчивые решения.

2. Архитектура безопасности с нулевым доверием

Ни одному пользователю или устройству не доверяют автоматически, гарантируя непрерывную аутентификацию и строгий контроль доступа, поэтому применяются следующие меры:

- Использование многофакторной аутентификации с квантовыми генераторами случайных чисел для создания непредсказуемых ключей.
- Сегментирование сетей с помощью микросегментации, ограничивая доступ даже внутри корпоративных систем, чтобы предотвратить горизонтальное перемещение.
- Внедрение постквантовой идентификации, которая объединяет биометрическую безопасность с квантово-безопасными методами аутентификации.

3. Безопасные квантовые сети

Организации, работающие с конфиденциальными или ценными данными (финансовые, медицинские, государственные), должны инвестировать в квантовое распределение ключей и квантово-защищенные VPN:

- Переход на квантово-безопасное облачное хранилище, которое шифрует данные с помощью криптографии на основе решеток.
- Внедрение VPN с квантовой защитой, обеспечив обмен ключами шифрования с помощью квантового распределения ключей для предотвращения кибершпионажа.

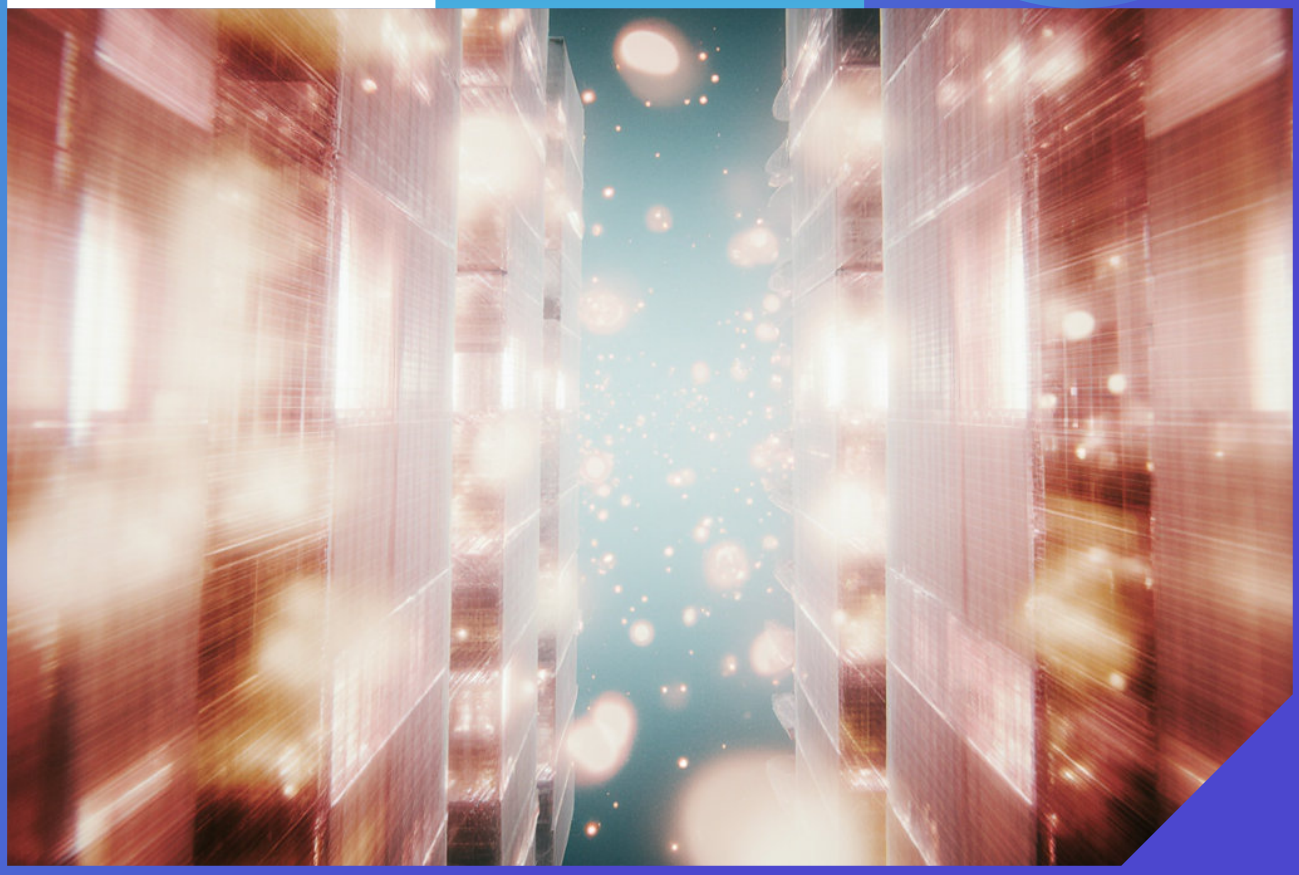
4. Полный квантово-безопасный стек

Комбинация физических и математических методов защиты приводит к тому, что:

- Квантовое распределение ключей обеспечивает надежное распределение ключей.
- Постквантовая криптография защищает алгоритмическую часть передачи и хранения.

Такой гибрид обеспечивает сквозную безопасность от фотона до протокола.

Практические аспекты внедрения квантовых и смежных технологий в системы ИБ в российских компаниях



Кейсы (сценарии применения) квантовых и смежных технологий в ИБ с описанием эффектов пилотного внедрения/апробации решений с использованием квантовых технологий в ИБ, методология отбора кейсов

МЕТОДОЛОГИЯ ОТБОРА КЕЙСОВ

1. Применение квантовых и смежных технологий в решении указанных задач может потенциально обеспечить большую эффективность по сравнению с существующими методами.

2. Сценарии направлены на решение реальной бизнес-задачи в исследуемой сфере.

3. Сценарии содержат количественные и/или качественные показатели эффективности внедрения квантовых и смежных технологий. Эффекты подтверждаются сравнением с традиционными методами по заранее определенным референсным метрикам (производительность, надежность, безопасность, экономическая выгода и т. д.).

4. В сценариях указаны ориентировочные сроки внедрения решения и стоимость.

5. Технология должна быть независимой от зарубежных разработок, обеспечивая технологическое лидерство и технологический суверенитет, устойчивость инфраструктуры и возможность дальнейшего развития отечественных решений.

Сервис шифрования каналов связи на основе магистральной квантовой сети

Технология

Квантовые коммуникации

Бизнес-процесс

- Исследование потребностей и подготовительные работы
- Закупка, внедрение и настройка оборудования
- Техническое обслуживание и мониторинг

Стоимость внедрения

По запросу

Срок внедрения

6–7
месяцев

Тип инсталляции

-

Экспорт решения

В перспективе

УГТ **9**

Наличие сертификации и аттестации:

- ФСТЭК России ☑
- ФСБ России ☑

Класс защищенности ИС по ФСТЭК России

≥ К2

Класс сертификации ФСБ России

КС3

Поставщик

ОАО «РЖД»

Проблема

- Повышение уязвимости информационных систем на фоне роста количества и сложности кибератак
- Зависимость от человеческого фактора при генерации и передаче криптографических ключей и чувствительных данных
- Рост вычислительных мощностей и объема трафика, усиливающие потребность в защите данных от растущих угроз

Потенциальные заказчики

- Государственные структуры
- ЦОДы
- ТЭК
- Атомная промышленность
- Военно-промышленный комплекс
- Химическая промышленность
- Транспорт
- Телеком операторы и др.
- Финансовый сектор

Решение

Разработанная линейка шифраторов позволяет осуществлять защиту информационных сервисов отдельных предприятий и высокоскоростных магистральных каналов передачи данных между центрами обработки данных и Государственными информационными системами.

Также обеспечивается сервисная поддержка проектов, в том числе выработка оптимального технического решения и подготовка необходимого пакета документов, размещение и настройка требуемого оборудования, техническая поддержка и мониторинг сети. Так, в режиме 24/7 функционирует Центр управления и мониторинга квантовой сети ОАО «РЖД», а также линейные отделы эксплуатации в городах присутствия сети.

Сервис предоставляется на основе магистральной квантовой сети ОАО «РЖД», протяженность которой составляет более 7000 км.

Эффекты

Исключение человеческого фактора при генерации и передаче криптографических ключей и чувствительных данных	Снижение затрат на оборудование и персонал	Безопасность передаваемых данных на десятилетия и круглосуточная служба поддержки во всех регионах присутствия магистральной квантовой сети

Сервис усиленной защиты каналов связи (КРК Квантовый ГОСТ VPN)

Технология

Квантовые коммуникации

Бизнес-процесс

- Обеспечение ИБ

Стоимость внедрения

от 10
млн руб.

Срок внедрения

от 1
месяца

Тип инсталляции

IaaS

Экспорт решения

Нет

УГТ 8–9

Наличие сертификации и аттестации:

ФСБ России

Уровень доверия в соответствии со ФСТЭК России

–

Класс сертификации ФСБ России

КС3

Поставщик

Ростелеком

ПАО «Ростелеком»

Потенциальные заказчики

- Государственные органы и компании с государственным участие
- Финансовые учреждения
- Центры обработки данных

Проблема

Угроза человеческого фактора в генерации, распространении и загрузке ключевой информации. В будущем угроза квантового компьютера.

Решение

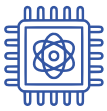
Сервис квантового распределения ключей — это максимально высокий уровень защиты каналов связи с помощью СКЗИ с использованием технологии квантового распределения ключей. Защита передачи данных в частных выделенных каналах связи с использованием отечественных сертифицированных алгоритмов шифрования и квантового распределения секретных ключей.

Эффекты

Минимизация влияния человеческого фактора при работе с ключами шифрования	Устранение угрозы информационной безопасности в долгосрочной перспективе	Надежная защита передаваемой информации

Набор инструментов разработчика, SDK «Сириус-Q. Решатель QUBO» для создания квантово-устойчивых национальных блокчейн-экосистем и платформ на основе QUBO-решателя семейства SB

Технология



Квантовые вычисления

Бизнес-процесс

- Обеспечение ИБ
- ИТ-обеспечение и связь

Стоимость внедрения

0,2–1	10
млн руб.	млн руб.
Лицензия	**НИОКР/ПАК**

Срок внедрения

1	2
год	года
Лицензия	**ПАК**

Тип инсталляции

SaaS, Paas, Iaas

Экспорт решения

Да

УГТ **6,7**

Наличие сертификации и аттестации:

- ФСТЭК России
- ФСБ России

Уровень доверия в соответствии со ФСТЭК России

4

Класс сертификации ФСБ России

–

Поставщик

УНИВЕРСИТЕТ ИННОПОЛИС

Сириус Научно-технологический университет

АНО ВО «Университет Иннополис, НТУ «Сириус»

Потенциальные заказчики

ФЕДЕРАЛЬНАЯ ТЕРРИТОРИЯ «СИРИУС»

Федеральная территория «Сириус»

Проблема

Сложность оптимизационных задач обеспечения квантовой устойчивости национальных блокчейн-экосистем и платформ является экспоненциальной по времени. Использование же технологии квантового отжига позволяет кратно сократить время, необходимое для нахождения точного решения таких задач, для практически релевантных размерностей

Решение

Создание и использование машин, основанных на различных физических принципах, специально предназначенных для решения задач оптимизации. Предлагаемое решение основано на методе квантового отжига и расширенной модели Р. Поттса.

Приводится аргументация, что эффективность квантовых алгоритмов связана с особенностями структуры энергетического профиля: наличием в термодинамическом пределе областей с большой плотностью локальных минимумов. Задача оптимизации ставится в форме задачи квадратичной бинарной оптимизации без ограничений (QUBO) либо в эквивалентной ей форме задачи Изинга. Это позволяет определять глобальные минимумы энергетического ландшафта, отражающие поведение блокчейн-систем в условиях квантовых атак Шора и Гровера и их известных модификаций, а также оптимальные процессы самовосстановления упомянутых блокчейн-систем, препятствуя их переходу в необратимые катастрофические состояния и отказу в облуживании в целом.

Эффекты

Увеличение точности моделирования динамики поведения блокчейн-систем в условиях квантовых атак злоумышленников

Получение оптимальной конфигурации средств защиты и самовосстановления для различных состояний блокчейн-платформ и экосистем

Набор инструментов разработчика, SDK «Сириус-Q. КНАА-2-ЭЦП» для реализации постквантовых криптографических примитивов и готовых интерфейсов в национальных блокчейн-экосистемах и платформах

Технология

Постквантовая криптография

Бизнес-процесс

- Обеспечение ИБ
- ИТ-обеспечение и связь
- Управление рисками

Стоимость внедрения

0,2–1	7
млн руб.	млн руб.
Лицензия	**НИОКР/ПАК**

Срок внедрения

1	2
год	года
Лицензия	**ПАК**

Тип инсталляции

SaaS, Paas, Iaas

Экспорт решения

Да

УГТ **6,7**

Наличие сертификации и аттестации:

- ФСТЭК России
- ФСБ России

Уровень доверия в соответствии со ФСТЭК России

4

Класс сертификации ФСБ России

–

Поставщик

УНИВЕРСИТЕТ ИННОПОЛИС

Сириус Научно-технологический университет

АНО ВО «Университет Иннополис, НТУ «Сириус»

Потенциальные заказчики

ФЕДЕРАЛЬНАЯ ТЕРРИТОРИЯ «СИРИУС»

Федеральная территория «Сириус»

Проблема

Проблема обеспечения устойчивости к компьютерным атакам злоумышленников с применением квантового компьютера. К 2030-м годам ожидается появление «практически релевантных» квантовых компьютеров, способных осуществлять взлом классических криптопримитивов RSA/ECC.

Решение

Создание и переход на национальные постквантовые криптопримитивы и электронную подпись на основе разделов математики, потенциально содержащих сложные вычислительные задачи, для которых в настоящее время не известны эффективные алгоритмы решения на классических и квантовых вычислителях. В частности, на постквантовые алгебраические алгоритмы ЭЦП на основе вычислительной трудности решения больших систем степенных уравнений, отличающиеся применением вспомогательных скрытых групп для устранения потенциальных атак на основе эквивалентных секретных ключей.

Эффекты

Повышение потенциально достижимого уровня криптографической стойкости

Повышение производительности алгебраических алгоритмов ЭЦП с двумя скрытыми коммутативными группами

Развертывание квантового генератора случайных чисел в структуре платформы Astra Облако

Технология

Квантовые сенсоры

Бизнес-процесс

- Обеспечение ИБ облачной платформы
- Разработка и развертывание облачных приложений
- Криптографическая защита облачных данных

Стоимость внедрения

от 10
млн руб.

ПАК

Срок внедрения

от 4
месяцев

ПАК

Тип инсталляции

On-premise, IaaS

Экспорт решения

Нет

УГТ **8**

Наличие сертификации и аттестации:

- ФСТЭК России ✓
- ФСБ России ✓

Класс защищенности ИС по ФСТЭК России

–

Класс сертификации ФСБ России

–

Поставщик

ООО «КуРэйт»,
ООО «РусБИТех-Астра»

Потенциальные заказчики

- Поставщики облачных услуг
- Банковские организации, работающие в облачной инфраструктуре
- Государственные структуры, внедряющие облачные решения
- Промышленные компании, мигрирующие в облако

Проблема

Традиционные псевдослучайные генераторы в облачной среде создают предсказуемые последовательности, что делает системы уязвимыми для атак.

Недостаток истинной случайности в облачных платформах приводит к компрометации шифрования, слабой аутентификации и возможности воспроизведения криптографических ключей, что нарушает безопасность данных и даёт злоумышленнику внешний контроль над результатами генерации.

Решение

Интеграция квантового генератора случайных чисел в структуру платформы Astra Облако.

КГСЧ использует флуктуации фазы электромагнитного поля в резонаторе полупроводникового лазера для генерации истинно случайных последовательностей со скоростью выше 300 Мбит/сек.

Система интегрируется с магазином приложений AIC, обеспечивая генерацию уникальных идентификаторов, первичных паролей пользователей и криптографических ключей для облачных сервисов.

Эффекты

Повышение стойкости облачных платформ от атак злоумышленников	Обеспечение истинной случайности для всех приложений в облаке	Снижение рисков компрометации пользовательских данных до минимума

Защита телефонной связи с использованием квантово-криптографической технологии

Технология

Квантовые коммуникации

Бизнес-процесс

- ИБ
- ИТ-обеспечение и связь

Стоимость внедрения

от 35
млн руб.

ПАК

Срок внедрения

от 1
месяца

ПАК

Тип инсталляции

On-premise, IaaS

Экспорт решения

Нет

УГТ **9**

Наличие сертификации и аттестации:

ФСТЭК России ✓

ФСБ России ✓

Уровень доверия в соответствии со ФСТЭК России

–

Класс сертификации ФСБ России

КС3

Поставщик

infotecs

АО «ИнфоТеКС»

Потенциальные заказчики

- Государственные и коммерческие учреждения
- Телеком-операторы

Проблема

- Высокие риски влияния человеческого фактора (умышленного и неумышленного) на конфиденциальность коммуникаций (телефония, сообщения, видеотелефония, файлы) в современных условиях
- Современные и потенциальные угрозы криптоанализа
- Использование одного телефона в открытом и закрытом сегментах сети

Решение

ViPNet QTS Lite — программно-аппаратный комплекс для защищенной IP-телефонии с использованием квантового распределения ключей. Обеспечивает защиту коммуникаций (видео, голос, сообщения, файлы) от криптоугроз, автоматизированную работу с криптографическими ключами и интеграцию с IP-телефонией, включая звонки между защищенными и обычными телефонами. Квантовые технологии лежат в основе протоколов выработки одинаковых ключей для территориально разнесенных абонентов защищаемой информационной системы. Работа квантовой криптографической системы выработки и распределения ключей (ККС ВРК) автоматизирована и исключает доступ к ключам, в том числе и администратора системы защиты. Решение отличает возможность построения полной системы криптографической защиты сети на оборудовании ViPNet, в том числе на существующих сетях. Все продукты взаимно увязаны и интегрированы в единую систему комплексной безопасности сети. Обеспечена возможность размещения абонентских аппаратов в категорированных помещениях.

Реализованные проекты: МГУ им. М.В. Ломоносова, ПАО «Газпром», АО «ИнфоТеКС», ТУСУР, Московский инновационный кластер «Ломоносов».

Эффекты

Исключение человеческого фактора и автоматизация работы системы криптографической защиты информации	Возможность размещения в категорированных помещениях	Исключение доступа третьих лиц к звонкам и переписке Устойчивость к современным и перспективным средствам криптоанализа

Защита магистральных каналов связи с применением квантово-криптографической технологии

Технология

Квантовые коммуникации

Бизнес-процесс

- ИБ
- ИТ-обеспечение и связь
- Удержание клиентов и лояльность
- Эксплуатация и обеспечение работы инфраструктуры
- Тарификация услуг и отдельных событий

Стоимость внедрения

от 45
млн руб.

ПАК

Срок внедрения

от 3
месяцев

ПАК

Тип инсталляции

On-premise, IaaS

Экспорт решения

Нет

УГТ **9**

Наличие сертификации и аттестации:

ФСТЭК России ✓

ФСБ России ✓

Уровень доверия в соответствии со ФСТЭК России

-

Класс сертификации ФСБ России

КС3

Поставщик

infotecs

АО «ИнфоТеКС»

Потенциальные заказчики

- Компании, работающие с конфиденциальной информацией, в том числе операторы персональных данных
- Операторы ГИС и ЗОКИИ
- Телеком-операторы
- Государственные и финансовые учреждения

Проблема

- Высокие риски влияния человеческого фактора (умышленного и неумышленного) на безопасность информационных систем в современных условиях
- Современные и перспективные методы криптоанализа, включая технологии квантовых вычислений и искусственного интеллекта
- Потребность роста производительности труда
- Стоимость реализации передовой системы криптографической защиты

Решение

ViPNet QTS использует квантово-криптографические технологии для защиты магистральных каналов связи на расстояниях до 100 км и более (с использованием промежуточных узлов), а также для сложных сетевых конфигураций. Обеспечивает создание защищенной VPN, автоматизированную работу с криптографическими ключами, интеграцию с существующими сетями ViPNet. Квантовые технологии лежат в основе протоколов выработки одинаковых ключей для территориально разнесенных абонентов защищаемой информационной системы. Работа квантовой криптографической системы выработки и распределения ключей (ККС ВРК) автоматизирована и исключает доступ к ключам, в том числе и администратора системы защиты. Решение АО «ИнфоТеКС» отличает возможность построения полной системы криптографической защиты сети на оборудовании ViPNet, в том числе на существующих сетях. Все продукты взаимно увязаны и интегрированы в единую систему комплексной безопасности сети.
Реализованные проекты: ОАО «РЖД», АО «ИнфоТеКС», МУКС (НИЦ «Курчатовский институт», МГУ им. М.В. Ломоносова, МТУСИ), «Большой университет Томска».

Эффекты

Повышение автоматизации криптографических систем и уровня защиты данных в магистральных каналах связи	Исключение человеческого фактора и автоматизация работы системы криптографической защиты информации за счет безопасной и автоматизированной выработки и распределения ключей	Устойчивость к современным и перспективным средствам криптоанализа

Квантовая защита каналов связи с технологией DWDM

Технология

Квантовые коммуникации

Бизнес-процесс

- ИБ
- ИТ-обеспечение и связь
- Удержание клиентов и лояльность
- Эксплуатация и обеспечение работы инфраструктуры

Стоимость внедрения

от 30
млн руб.

Готовый продукт с лицензией

Срок внедрения

от 3
месяцев

Внедрение системы КРК

Тип инсталляции

On-premise, IaaS

Экспорт решения

Нет

УГТ **6**

Наличие сертификации и аттестации:

ФСТЭК России ✓

ФСБ России ✓

Уровень доверия в соответствии со ФСТЭК России

–

Класс сертификации ФСБ России

–

Поставщик

infotecs

АО «ИнфоТеКС»

Потенциальные заказчики

- Компании, работающие с конфиденциальной информацией, в том числе операторы персональных данных
- Операторы ГИС и ЗОКИИ
- Телеком-операторы
- Государственные и финансовые учреждения

Проблема

- Высокие риски влияния человеческого фактора на безопасность информационных систем в современных условиях
- Современные и перспективные методы криптоанализа, включая технологии квантовых вычислений и ИИ
- Потребность роста производительности труда
- Стоимость реализации передовой системы криптографической защиты
- Ограничения по наличию и прокладке выделенного волокна для квантового канала, требуемого современными квантовыми криптографическими системами выработки и распределения ключей (ККС ВРК), в условиях городской застройки, вводов на территории технологических парков и деловых центров и соответствующие издержки при внедрении

Решение

ViPNet QTS DWDM снимает ограничения по необходимости прокладки или выделения отдельного квантового канала и обеспечивает абсолютно бесшовную интеграцию в существующие сети, а также:

- Реализует все преимущества ККС ВРК
- Совместима со средствами криптографической защиты ViPNet
- Работает в существующих ВОЛС по технологии DWDM
- Расстояние между двумя узлами до 50 км
- Расстояние между объектами не ограничено при использовании промежуточных узлов

Квантовые технологии лежат в основе протоколов выработки одинаковых ключей для территориально разнесенных абонентов защищаемой информационной системы. Работа квантовой криптографической системы выработки и распределения ключей (ККС ВРК) автоматизирована и исключает доступ к ключам, в том числе и администратора системы защиты. Решение АО «ИнфоТеКС» отличает возможность построения полной системы криптографической защиты сети на оборудовании ViPNet, в том числе на существующих сетях.

Эффекты

Отсутствие необходимости прокладки или выделения отдельного волокна для квантового канала, возможность работы в существующих DWDM сетях	Исключение человеческого фактора и автоматизация работы системы криптографической защиты информации за счет безопасной и автоматизированной выработки и распределения ключей	Возможность достижения абсолютной стойкости

Защита сети связи на базе произвольной телекоммуникационной инфраструктуры

Технология

Квантовые коммуникации

Бизнес-процесс

- ИТ-обеспечение и связь
- Информационная безопасность

Стоимость внедрения

от 45
млн руб.

ПАК

Срок внедрения

от 3–5
месяцев

ПАК

Тип инсталляции

On-premise, IaaS, KaaS

Экспорт решения

Нет

УГТ **8**

Наличие сертификации и аттестации:

ФСТЭК России ✓

ФСБ России ✓

Уровень доверия в соответствии со ФСТЭК России

–

Класс сертификации ФСБ России

КС3

Поставщик

СМАРТС КВАНТТЕЛЕКОМ

ООО «СМАРТС-Кванттелеком»

Потенциальные заказчики

- Операторы сотовой связи
- Интернет-провайдеры
- Банки
- Государственные структуры
- Любые крупные коммерческие организации, владеющие собственной информационной инфраструктурой

Проблема

Актуальные угрозы ИБ, являющиеся катализатором как растущих финансовых и репутационных рисков, так и угроз национальной безопасности.
К таким угрозам ИБ относятся:

- Развитие квантовых вычислений, способных скомпрометировать ныне используемые на практике алгоритмы шифрования данных
- Человеческий фактор, присущий устоявшейся процедуре распределения ключей шифрования в симметричных криптосистемах

Решение

Квантовая криптографическая система выработки и распределения ключей Qualion, сопряженная с линейкой средств криптографической защиты информации (СКЗИ). Позволяет реализовать канал связи, защищенный с использованием квантовых ключей, на расстоянии до 100 км и на произвольном расстоянии с использованием квантово-защищенных ключей, сформированных по принципу доверенных промежуточных узлов. В автоматическом режиме вырабатывает и обновляет ключи шифрования в СКЗИ, исключая финансовые и временные затраты на периодическое обслуживание СКЗИ и человеческий фактор из процедуры смены ключей. Вырабатывает ключи для симметричных криптосистем, устойчивых к атакам с использованием квантовых вычислителей.

Защищенные VPN-соединения с использованием квантовых и квантово-защищенных ключей могут реализовываться через произвольную сетевую топологию на базе коммутаторов и маршрутизаторов различных производителей. В качестве сопряженных шифраторов для защиты данных может использоваться целая линейка устройств с производительностью от 50 Мбит/с до 100 Гбит/с.

Эффекты

Снижение затрат на обслуживание СКЗИ за счет отсутствия необходимости в периодическом обновлении ключей в СКЗИ	Исключение человеческого фактора из процедуры распределения ключей за счет автоматизации	Защита от потенциальных угроз при появлении квантового компьютера

Защита выделенных каналов связи высокой пропускной способности

Технология

Квантовые коммуникации

Бизнес-процесс

- ИТ-обеспечение и связь
- Информационная безопасность

Стоимость внедрения

от 35
млн руб.

ПАК

Срок внедрения

от 3-5
месяцев

ПАК

Тип инсталляции

On-premise, IaaS

Экспорт решения

Нет

УГТ **8**

Наличие сертификации и аттестации:

- ФСТЭК России
- ФСБ России

Уровень доверия в соответствии со ФСТЭК России

–

Класс сертификации ФСБ России

КС3

Поставщик

СМАРТС КВАНТТЕЛЕКОМ

ООО «СМАРТС-Кванттелеком»

Потенциальные заказчики

- Операторы сотовой связи
- Интернет-провайдеры
- Банки
- Государственные структуры
- Любые крупные коммерческие организации, владеющие собственной информационной инфраструктурой

Проблема

В условиях растущего объема передаваемых данных и появления новых угроз безопасности информации высокоскоростные каналы связи между ЦОД особенно нуждаются в надежных решениях для защиты данных, поскольку их компрометация может привести к утечке всех агрегируемых данных. Актуальные угрозы ИБ ведут к финансовым и репутационным рискам. К таким угрозам относятся:

- Развитие квантовых вычислений, способных скомпрометировать ныне используемые на практике алгоритмы шифрования данных
- Человеческий фактор, присущий устоявшейся процедуре распределения ключей шифрования в симметричных криптосистемах

Решение

Квантовая криптографическая система (КВАКС) – является интегрированным решением, объединяющим квантовую криптографическую систему выработки и распределения ключей (ККС ВРК) и средство криптографической защиты информации (СКЗИ) в едином корпусе для защиты выделенных каналов связи. В автоматическом режиме вырабатывает и обновляет ключи шифрования в СКЗИ, исключая финансовые и временные затраты на периодическое обслуживание СКЗИ и человеческий фактор из процедуры смены ключей. Вырабатывает ключи для симметричных криптосистем, устойчивых к атакам с использованием квантовых вычислителей.

Особенностью решения является возможность использования СКЗИ, защищающего канал связи в составе оптической транспортной сети, что приводит к существенному снижению сетевых задержек в каналах передачи данных. Интегрированные СКЗИ имеют производительность 10 Гбит/с, при необходимости может быть использована платформа с производительностью 100 Гбит/с.

Эффекты

Снижение затрат на обслуживание СКЗИ за счет отсутствия необходимости в периодическом обновлении ключей в СКЗИ	Исключение человеческого фактора из процедуры распределения ключей за счет автоматизации	Защита от потенциальных угроз при появлении квантового компьютера

Защита удостоверяющего центра

Технология

Постквантовая криптография

Бизнес-процесс

- Обеспечение ИБ
- ИТ-обеспечение и связь
- Оценка риска
- Обслуживание и ведение банковских счетов

Стоимость внедрения

4–8	10–15
млн руб.	млн руб.
Лицензия	**НИОКР**

Срок внедрения

1	6-12
месяц	месяцев
Лицензия	**НИОКР**

Тип инсталляции

Пилотная поставка программного квантово-устойчивого решения в ограниченный контур информационной системы бизнес-клиента

Экспорт решения

Нет

УГТ 6

Наличие сертификации и аттестации:

ФСТЭК России

ФСБ России

Уровень доверия в соответствии со ФСТЭК России

-

Класс сертификации ФСБ России

-

Поставщик

QApp

ООО «КуАпп»

Потенциальные заказчики

- Финансовый сектор
- Медицинские и фармацевтические организации
- Образовательные и научные организации
- Корпоративный сектор
- (включая ИТ, промышленные компании, телеком-операторы)
- Государственные органы

Проблема

Удостоверяющий центр организации является ключевым звеном, на котором строится доверие как внутри компании, так и у внешних партнеров. Угроза его компрометации с применением квантовых компьютеров создаст новые риски, так как стандартные методы защиты могут оказаться недостаточными. Это повышает необходимость поиска новых решений для защиты критически важной информации и предотвращения финансовых и репутационных потерь.

Решение

Квантово-устойчивый удостоверяющий центр с поддержкой отечественных постквантовых алгоритмов в инфраструктуре открытых ключей поможет крупным организациям снизить до минимума успешность атак с применением квантовых компьютеров и минимизировать риск утечки информации.

Постквантовые криптографические алгоритмы основаны на специальном классе математических задач, расшифровка которых не представляется возможной с применением классических и квантовых вычислителей.

Эффекты

Повышение стойкости к криптографическим атакам с применением как классических, так и квантовых компьютеров

Снижение риска подделки транзакций в инфраструктуре цифрового рубля

Технология

Постквантовая криптография

Бизнес-процесс

- Обеспечение ИБ
- ИТ-обеспечение и связь
- Оценка риска
- Выявление мошенничества

Стоимость внедрения

4–8 млн руб.	12–20 млн руб.
Лицензия	**НИОКР**

Срок внедрения

1 месяц	6–12 месяцев
Лицензия	**НИОКР**

Тип инсталляции

Пилотная поставка программного квантово-устойчивого решения в ограниченный контур информационной системы бизнес-клиента

Экспорт решения

Нет

УГТ 3

Наличие сертификации и аттестации:

ФСТЭК России

ФСБ России

Уровень доверия в соответствии со ФСТЭК России

–

Класс сертификации ФСБ России

–

Поставщик

QApp

ООО «КуАпп»

Потенциальные заказчики

- Банк России
- Финансовые организации

Проблема

В модели цифрового рубля блокчейн и электронная цифровая подпись (ЭЦП) обеспечивают авторизацию и целостность транзакций. Однако классические ЭЦП уязвимы перед квантовой угрозой, возможен риск подделки транзакций злоумышленником.

Решение

Организационные и технические меры, направленные на перевод инфраструктуры цифрового рубля на квантово-устойчивые механизмы поддержания конфиденциальности и целостности данной системы. Использование технологий, устойчивых к квантовым атакам, повысит безопасность цифрового рубля: применение постквантовых подписей для аутентификации делает невозможным подделку транзакций, а защита каналов передачи данных может быть обеспечена постквантовыми механизмами инкапсуляции ключа.

Эффекты

Повышение стойкости к криптографическим атакам с применением как классических, так и квантовых компьютеров

Защита систем дистанционного банковского обслуживания

Технология

Постквантовая криптография

Бизнес-процесс

- Обеспечение ИБ
- Внутренний аудит и контроль
- Оценка риска
- Выявление мошенничества
- Учет, налогообложение и отчетность

Стоимость внедрения

4–8 млн руб.	**10–15** млн руб.
Лицензия	**НИОКР**

Срок внедрения

1 месяц	**6-9** месяцев
Лицензия	**НИОКР**

Тип инсталляции

Пилотная поставка программного квантово-устойчивого решения в ограниченный контур информационной системы бизнес-клиента

Экспорт решения

Нет

УГТ **7**

Наличие сертификации и аттестации:

ФСТЭК России

ФСБ России

Уровень доверия в соответствии со ФСТЭК России

–

Класс сертификации ФСБ России

–

Поставщик

QApp

ООО «КуАпп»

Потенциальные заказчики

- Банковские организации
- Операторы платежных систем

Проблема

Холдинговые компании, являющиеся клиентами крупных банков, централизуют финансовые операции дочерних структур и направляют платежные поручения через систему дистанционного банковского обслуживания. Однако используемые традиционные криптографические алгоритмы уязвимы к квантовой угрозе, что требует перехода на квантово-устойчивые решения для защиты финансовых данных.

Решение

Квантово-устойчивая защита каналов передачи данных между информационными системами напрямую подключенных организаций позволит значительно снизить риски утраты целостности и раскрытия конфиденциальной информации, содержащейся в платежных поручениях компаний.

Эффекты

Повышение стойкости к криптографическим атакам с применением как классических, так и квантовых компьютеров

Защита киберфизических систем

Технология

Постквантовая криптография

Бизнес-процесс

- ИБ
- ИТ-обеспечение и связь
- Управление рисками

Стоимость внедрения

4–8	15–20
млн руб.	млн руб.
Лицензия	**НИОКР**

Срок внедрения

1	9–12
месяц	месяцев
Лицензия	**НИОКР**

Тип инсталляции

Пилотная поставка программного квантово-устойчивого решения в ограниченный контур информационной системы бизнес-клиента

Экспорт решения

Нет

УГТ 3

Наличие сертификации и аттестации:

ФСТЭК России

ФСБ России

Уровень доверия в соответствии со ФСТЭК России

–

Класс сертификации ФСБ России

–

Поставщик

QApp

ООО «КуАпп»

Проблема

Киберфизические системы (в состав которых входят различные АСУ ТП: промышленный интернет вещей, роботизация, умный транспорт, ЖКХ и агросистемы, беспилотные авиационные системы и др.) становятся неотъемлемым ключевым элементом цифровой экономики. Однако с их развитием растет и уязвимость к кибератакам: злоумышленники могут перехватить данные с датчиков, подделать команды управления, вывести из строя критически важные узлы. Эти угрозы многократно возрастают с применением злоумышленниками мощных квантовых вычислителей.

Потенциальные заказчики

- Разработчики киберфизических устройств

Решение

Применение постквантовой криптографии обеспечит защиту каналов связи и аутентификации устройств киберфизических систем от атак с применением как классических, так и квантовых компьютеров.

- Для систем интернета вещей: использование квантово-устойчивого обмена ключами (постквантовые механизмы инкапсуляции ключей) и квантово-устойчивой цифровой подписи управляющих команд, обеспечение контроля целостности передаваемого низкоуровневого программного обеспечения
- Для БАС и умного транспорта: обеспечение подлинности сообщений навигации и телеметрии
- Для медицинских, ЖКХ-систем: квантово-устойчивая защита персональных данных и критически важных измерений от подделки и подмены

Эффекты

Повышение стойкости к криптографическим атакам с применением как классических, так и квантовых компьютеров

Защита корней доверия

Технология

Постквантовая криптография

Бизнес-процесс

- Обеспечение ИБ
- ИТ-обеспечение и связь
- Оценка риска
- Выявление мошенничества

Стоимость внедрения

4–8	35–45
млн руб.	млн руб.
Лицензия	**НИОКР**

Срок внедрения

1	12-18
месяц	месяцев
Лицензия	**НИОКР**

Тип инсталляции

Пилотная поставка программного квантово-устойчивого решения в ограниченный контур информационной системы бизнес-клиента

Экспорт решения

Нет

УГТ **4**

Наличие сертификации и аттестации:

ФСТЭК России

ФСБ России

Уровень доверия в соответствии со ФСТЭК России

–

Класс сертификации ФСБ России

–

Поставщик

QApp

ООО «КуАпп»

Потенциальные заказчики

- Финансовый сектор
- Корпоративный сектор (включая ИТ, промышленные компании, телеком-операторы)
- Государственные органы

Проблема

Корни доверия — фундаментальный элемент безопасности цифровой инфраструктуры. Они реализуются в микропроцессорах, SIM/e-SIM/i-SIM, HSM-модулях, модулях доверенной загрузки и обеспечивают хранение ключей, аутентификацию устройств, защиту прошивок и цепочек загрузки данных. Применяемые повсеместно (в банковском и платежном секторе, мобильных и телеком-сетях, государственных инфраструктурах, в потребительской электронике, IoT-системах и т. д.) корни доверия, построенные на классической криптографии, становятся особо уязвимыми к кибератакам с применением мощных квантовых вычислителей.

Решение

Интегрирование постквантовой криптографии обеспечит квантово-устойчивую защиту корней доверия.

- Внедрение постквантовых цифровых подписей и механизмов обмена ключами в HSM-модули и микропроцессоры создаст квантово-устойчивую безопасность загрузки низкоуровневого программного обеспечения, подписи транзакций и управление ключами
- Использование постквантовых алгоритмов в SIM/e-SIM/i-SIM для аутентификации и обновления профилей исключит клонирование и подделку SIM
- Использование квантово-устойчивых корней доверия в потребительской электронике защитит аутентификацию и цепочку доверенной загрузки от взлома с применением квантового компьютера

Эффекты

Повышение стойкости к криптографическим атакам с применением как классических, так и квантовых компьютеров

Защита инфраструктуры платежных мобильных терминалов

Технология

Постквантовая криптография

Бизнес-процесс

- Проведение платежей

Стоимость внедрения

4–8 млн руб.	**10–15** млн руб.
Лицензия	**НИОКР**

Срок внедрения

1 месяц	**6-12** месяцев
Лицензия	**НИОКР**

Тип инсталляции

Пилотная поставка программного квантово-устойчивого решения в ограниченный контур информационной системы бизнес-клиента

Экспорт решения

Нет

УГТ **5**

Наличие сертификации и аттестации:

ФСТЭК России

ФСБ России

Уровень доверия в соответствии со ФСТЭК России

–

Класс сертификации ФСБ России

–

Поставщик

QApp

УНИВЕРСИТЕТ ЛОБАЧЕВСКОГО

ООО «КуАпп», ННГУ

Потенциальные заказчики

- Финансовые организации
- Ритейл

Проблема

Решения на основе мобильных платежных терминалов (mPOS) используются в финансовой отрасли, ритейле и многих других. Применяемые на сегодняшний день классические криптографические алгоритмы, используемые mPOS, становятся особо уязвимыми к кибератакам с применением мощных квантовых вычислителей.

Решение

Пилотная интеграция постквантовой криптографии в процесс оплаты токенизированной картой на платежном мобильном терминале (mPOS) для обеспечения квантовой защиты платежных данных.

Сценарий, реализуемый в пилотном проекте:
- Онлайн-транзакция с дополнительной оффлайн аутентификацией
- Онлайн-аутентификация обеспечивается одноразовыми симметричными ключами, получаемыми из сети
- Офлайн-аутентификация обеспечивается статичными асимметричными постквантовыми ключами

Ключевые компоненты инфраструктуры в пилотном проекте:
- Мобильное устройство с постквантовым приложением
- Платежный терминал на основе ОС Android с терминальным приложением
- Хост-модель внешней инфраструктуры

Проект выполняется в рамках государственной программы поддержки университетов «Приоритет 2030».

Эффекты

Повышение стойкости к криптографическим атакам с применением как классических, так и квантовых компьютеров

Защита инфраструктуры блокчейн-сервисов

Технология

Постквантовая криптография

Бизнес-процесс

- Обеспечение ИБ
- ИТ-обеспечение и связь
- Подпись транзакций и генезиса в блокчейне

Стоимость внедрения

4–8 млн руб.	**10–15** млн руб.
Лицензия	**НИОКР**

Срок внедрения

1 месяц	**4-12** месяцев
Лицензия	**НИОКР**

Тип инсталляции

Пилотная поставка программного квантово-устойчивого решения в ограниченный контур информационной системы бизнес-клиента

Экспорт решения

Нет

УГТ **5**

Наличие сертификации и аттестации:

ФСТЭК России

ФСБ России

Уровень доверия в соответствии со ФСТЭК России

–

Класс сертификации ФСБ России

–

Поставщик

QApp

web³ tech

ООО «КуАпп»,
ООО «ВЕБ3 ТЕХНОЛОГИИ»

Потенциальные заказчики

- Государство
- Госкорпорации
- Финансово-промышленный холдинги
- Финтех

Проблема

Современные блокчейн-системы, как публичные, так и проприетарные, используют асимметричную криптографию (RSA, ГОСТ и др.), уязвимую перед атаками высокопроизводительных квантовых компьютеров. При их развитии возможны взлом цифровых подписей, подделка транзакций и компрометация корня доверия.
Уже сейчас существует риск атак типа «сохрани сейчас — расшифруй потом».

Решение

Интеграция ПО «PQC SDK» с отечественной блокчейн-платформой «Конфидент» позволит реализовать комплексную защиту распределенного реестра от угроз со стороны как классических, так и квантовых компьютеров. Постквантовые алгоритмы обеспечивают устойчивость ключевых операций — генерации ключей, электронной подписи, верификации и хэширования — без изменения архитектуры системы.

Эффекты

Повышение стойкости к криптографическим атакам с применением как классических, так и квантовых компьютеров

Программно-аппаратный комплекс мобильной квантово-защищенной связи

Технология

Квантовые коммуникации

Бизнес-процесс

- Обеспечение ИБ
- ИТ-обеспечение и связь

Стоимость внедрения

1-10 млн руб.

Лицензия

30 млн руб.

ПАК

Срок внедрения

до 1 дня

Тип инсталляции

On-premise

Экспорт решения

Да

УГТ **7**

Наличие сертификации и аттестации:

- ФСТЭК России
- ФСБ России

Уровень доверия в соответствии со ФСТЭК России

4

Класс сертификации ФСБ России

КС3

Поставщик

МФТИ

Потенциальные заказчики

- Государственные структуры
- Ведомства
- Госкорпорации
- Операторы связи
- Коммерческие компании

Проблема

Обеспечение доверия к ключам шифрования от момента выработки до вывода из эксплуатации. Нативная интеграция в экосистему информационной системы заказчика.

Решение

ПАК мобильной квантово-защищенной связи, функционирующий на отечественных симметричных криптографических алгоритмах и включающего устройство снабжения квантовыми/квантово-защищенными ключами мобильных устройств и ПО мобильного мессенджера, обеспечивает защиту информации на квантовых/квантово-защищенных ключах.

Решение использует технологию КРК как сервис. Обеспечивается подключение к квантовой сети для автоматического получения ключа, на базе которого организуется взаимодействие с территориально распределенными выделенными защищенными сегментами абонентов. Мобильный автономный модуль управления криптографическими ключами с интеграцией в квантовые сети обеспечивает полный контроль над жизненным циклом ключей. Модуль генерирует, безопасно хранит и автоматически распределяет ключи, исключая человеческий фактор и внешние уязвимости.

Эффекты

Повышение безопасности коммуникаций до уровня гарантии о невозможности компрометации	Автоматизация обслуживания систем ИБ за счет автоматизации выработки и распределения ключей	Исключение угрозы внутреннего нарушителя за счет исключения из процесса необходимости участия человека

Квантово-вдохновленный высокоскоростной алгоритм маршрутизации трафика в больших телекоммуникационных сетях

Технология

Квантовые коммуникации

Бизнес-процесс

- Обеспечение ИБ
- ИТ-обеспечение и связь

Стоимость внедрения

7-10
млн руб.

Срок внедрения

до 1
года

Тип инсталляции

On-premise, SaaS

Экспорт решения

Да

УГТ **6**

Наличие сертификации и аттестации:

ФСТЭК России	не требуется
ФСБ России	не требуется

Уровень доверия в соответствии со ФСТЭК России

не требуется

Класс сертификации ФСБ России

не требуется

Поставщик

МФТИ

Потенциальные заказчики

- Операторы телекоммуникационных и прочих транспортных сетей
- Вендоры сетевого оборудования

Проблема

Проблема масштабирования классических методов маршрутизации, балансировки нагрузки, построения логических карт транспортных, в частности, телекоммуникационных сетей, обладающих сильно возрастающей с размером системы вычислительной сложностью. Как следствие, медленная работа классических методов в сетях больших размеров, падение ключевых метрик Quality of Service работы сетей при увеличении размеров сети.

Решение

Разработан квантово-вдохновленный алгоритм интеллектуальной маршрутизации трафика для больших транспортных сетей (10 000+ узлов). Решение строит карту кратчайших путей из любого узла сетевого графа ко всем остальным при сохранении точности маршрутизации в среднем в 97 % за счет оригинального метода сокращения размера графа, построенного на основе выявленных свойств статистического самоподобия случайных графов. Обеспечивается ускорение расчета оптимальных маршрутов, как следствие, снижение задержек и уменьшение требований к вычислительным ресурсам при планировании и оперативном управлении сетью. Технология опирается на выявленные законы скейлинга — статистической самоподобности и масштабной инвариантности — в стохастических сетях связи, аналогичные тем, что наблюдаются в квантовых Изинг-моделях. Такое свойство позволяет надежно переносить результаты оптимизации с укрупненной модели на реальную сеть без потери качества, что критично для операторов, работающих с трафиком, который резко меняется во времени и пространстве. Драйвером эффективности выступает оригинальный метод редукции графа, который системно «сжимает» сетевые топологии, сохраняет значимые метрики и ускоряет вычисления без деградации конечных маршрутов. Для бизнеса это трансформируется в экономию OPEX/CAPEX на масштабирование инфраструктуры, повышение SLA и устойчивость сети при пиковых нагрузках и инцидентах.

Эффекты

Ускорение маршрутизации трафика в телекоммуникационных и прочих альтернативных сетях в 4,5–5 раз по сравнению с действующими протоколами при потере точности маршрутизации менее 4%.

Увеличение эффективной пропускной способности сети на пользователя.

Энергонезависимый программно-аппаратный комплекс управления ключевой информацией для квантово-защищенных коммуникаций

Технология

Квантовые коммуникации

Бизнес-процесс

- Обеспечение ИБ
- Управление жизненным циклом ключей
- Защита корпоративных коммуникаций

Стоимость внедрения

1–10 млн руб.

150 тыс. руб.

Лицензия **ПАК**

Срок внедрения

до 5–7 месяцев

Тип инсталляции

On-premise
Cloud (Key-aaS)

Экспорт решения

Нет

УГТ **7**

Наличие сертификации и аттестации:

ФСТЭК России	2026 г.
ФСБ России	2026 г.

Уровень доверия в соответствии со ФСТЭК России

4

Класс сертификации ФСБ России

КС3

Поставщик

МФТИ

Потенциальные заказчики

- Ведомства
- Госкорпорации
- Операторы

Проблема

Для обеспечения гарантии ИБ при использовании криптографических средств защиты в первую очередь необходимо гарантировать доверие к ключам шифрования на всех этапах их существования — от момента генерации до безопасного вывода из эксплуатации, включая защиту от действий внутреннего нарушителя.
Для возможности эксплуатации любой криптографической системы ИБ необходимо обеспечить выработку и защищенное распределение ключей между различными пользовательскими устройствами. Проблема заключается в необходимости автоматизации процессов генерации, распространения и применения ключей в коммуникациях и при организации защищенных сервисов, чтобы исключить человеческий фактор и обеспечить масштабируемость системы.

Решение

ПАК управления ключевой информацией для квантово-защищенных коммуникаций, функционирующий на отечественных симметричных криптографических алгоритмах и включающий устройство снабжения квантовыми/квантово-защищенными ключами мобильных устройств и ПО мобильного мессенджера, обеспечивает защиту информации на квантовых/квантово-защищенных ключах.

Решение использует технологию KPK как сервис. Обеспечивается подключение к инфраструктуре квантовой сети для автоматического получения ключей, на базе которых организуется взаимодействие с территориально распределенными сегментами сетей (защищаемые абоненты).

Мобильный автономный модуль управления криптографическими ключами с интеграцией в квантовые сети обеспечивает полный контроль над жизненным циклом ключей. Модуль генерирует, безопасно хранит и автоматически распределяет ключи, исключая человеческий фактор и внешние уязвимости.

Эффекты

Повышение доверия к безопасности коммуникаций до уровня гарантии о невозможности их компрометации	Автоматизация обслуживания систем ИБ за счет снижения человеческого фактора и автоматизации выработки и распределения ключей	Исключение угрозы внутреннего нарушителя за счет отсутствия доступа человека к криптографическим ключам и обеспечению собственного контроля за отсутствием компрометации

Система доверенной доставки ключевой информации для криптографических систем

Технология

Квантовые коммуникации

Бизнес-процесс

- Управление жизненным циклом криптографических ключей
- Доверенная доставка ключей до СКЗИ по запросу в режиме онлайн.

Стоимость внедрения

1–10 млн руб. **Лицензия**

70 млн руб. **ПАК**

Срок внедрения

15 месяцев

Тип инсталляции

On-premise
Cloud (Key-aaS)

Экспорт решения

Нет

УГТ **6**

Наличие сертификации и аттестации:

ФСТЭК России	2026 г.
ФСБ России	2026 г.

Уровень доверия в соответствии со ФСТЭК России

4

Класс сертификации ФСБ России

КС3

Поставщик

МФТИ

Потенциальные заказчики

- Ведомства
- Госкорпорации
- Операторы Интеграторы ИБ

Проблема

Доставка ключей для сети СКЗИ-потребителей и криптографических модулей в любой момент времени затруднена необходимостью обеспечить достаточный уровень доверия.

Необходимость регулярной смены ключей, в том числе внеплановой смены ключей по запросу осложнена при условии широкой территориально распределенной сети СКЗИ (межрегиональные сети охватывающие всю территорию страны).

Дороговизна и сложность организационно-технических мер доверенной курьерской доставки.

Решение

ПАК представляет собой автономную автоматизированную защищенную систему для организации доверенной доставки ключевой информации от центра выработки ключей (в том числе ККС ВРК) до СКЗИ-потребителей. ПАК выполнен с учетом требований к СКЗИ с использованием стандартизованных отечественных криптографических алгоритмов. ПАК обеспечивает управление защищенными каналами, которые используются для легитимной доставки ключевой информации до точки загрузки в СКЗИ или любой криптографический модуль, способный использовать симметричные криптографические ключи при своей непосредственной работе.

Решение использует квантовую сеть (ККС ВРК) в качестве сервиса для масштабирования собственной доверенной сети распространения секретной информации, а также имеет возможность выступать в роли доверенной системы «доведения» ключей, выработанных ККС ВРК для квантового СКЗИ-потребителя. Обеспечивается подключение к квантовой сети по стандартизованному интерфейсу ProtoQa. Система имеет независимый контур криптографической защиты, который не связан с ключевой системой обсуживаемой сети СКЗИ-потребителей.

Эффекты

Повышение доверия к безопасности коммуникаций до уровня гарантии о невозможности их компрометации	Ускорение процессов за счет автоматизации обеспечения управления и контроля за жизненным циклом ключей и повышение уровня безопасности за счет снижения человеческого фактора и автоматизации доставки и загрузки ключей	Снижение затрат на организацию процессов доставки и обновления ключей для СКЗИ

Программно-аппаратный комплекс атмосферного квантового распределения ключей

Технология

Атмосферные оптические квантовые коммуникации (КРК)

Бизнес-процесс

- Строительство квантовых сетей, где невозможен оптоволоконный квантовый канал

Стоимость внедрения

Рассчитывается под проект

Срок внедрения

Рассчитывается под проект

Тип инсталляции

On-premise

Экспорт решения

Нет

УГТ 4

Наличие сертификации и аттестации:

- ФСТЭК России
- ФСБ России

Уровень доверия в соответствии со ФСТЭК России

не требуется

Класс сертификации ФСБ России

КС3

Поставщик

ЦИР

АО «Центр Исследований и Разработок»

Потенциальные заказчики

- Интеграторы и операторы квантовых сетей
- Разработчики инфраструктурных решений мобильного и беспилотного транспорта

Проблема

При строительстве квантовых сетей на сегодняшний момент нет решения, способного работать там, где нет оптоволоконного кабеля.

Существуют участки на Земле, где прокладка кабеля слишком дорогая или вообще невозможна.

Распределение ключей между подвижными объектами требует технологии КРК, работающей по атмосферному каналу.

Решение

ПАК предназначен для защиты беспроводных каналов передачи данных на основе квантового распределения ключей (КРК), реализованного через атмосферные оптические каналы для использования на кораблях, беспилотных автомобилях, БПЛА, IIoT и мобильных устройствах.

ПАК обеспечивает выработку и распределение криптографических ключей между стационарным объектом и подвижным объектом по открытому каналу на расстоянии до 1500 метров с функциональностью удержания и коррекции оптического канала связи.

ПАК рассчитан, в том числе, на возможность работы в условиях северного морского климата.

Скорость выработки ключей составляет от 100 бит/с до 1 Кбит/с в зависимости от характеристик атмосферного канала.

Эффекты

Возможность «дотянуть» сеть КРК до труднодоступных территорий	Позволяет реализовать сценарии распределения ключей на подвижные объекты, которые невозможно соединить кабелями	Повышение скорости развертывания малых сегментов квантовой сети за счет отсутствия необходимости прокладывать кабель

Программно-аппаратный комплекс передачи данных и доставки предраспределенных квантовых ключей по технологии Li-Fi

Технология

Квантовые коммуникации

Бизнес-процесс

- Защищенная передача данных
- Доставка предраспреде-ленных квантовых ключей до конечного пользователя

Стоимость внедрения

Рассчитывается под проект

Срок внедрения

Рассчитывается под проект

Тип инсталляции

On-premise

Экспорт решения

Нет

УГТ **5**

Наличие сертификации и аттестации:

ФСТЭК России	не требуется
ФСБ России	не требуется

Уровень доверия в соответствии со ФСТЭК России

не требуется

Класс сертификации ФСБ России

КС3

Поставщик

ИТМО

Университет ИТМО

Потенциальные заказчики

- Заводы, где невозможно использовать радиочастотный спектр для IIoT
- Учреждения, где нужен защищенный беспроводной доступ
- Последняя миля для квантовых сим-карт

Проблема

Беспроводной доступ в интернет через радиочастотный спектр может быть перехвачен, так как Wi-Fi / LTE / Bluetooth проходят сквозь преграды, а с учетом приборов, которые усиливают радиочастотный сигнал, злоумышленник может быть далеко от сети, на которую идет атака.

При скоплении большого количества людей радиочастотные сети имеют ограниченную полосу приема, например, на стадионах, конференц-холлах необходимо ставить большое количество точек связи, что приводит к большему расходу энергии.

Решение

Использовать технологию Li-Fi (передача данных через светодиодное освещение) как дополнительный или альтернативный вариант для выхода в интернет вместо сетей радиочастотного спектра (Wi-Fi / LTE / Bluetooth).

Светильники Li-Fi одновременно освещают помещение и раздают широкополосный доступ в интернет, что ведет к экономии энергии.

Использование Li-Fi дает возможность иметь дополнительный защищенный канал связи в случае отключения радиочастотного спектра на критической инфраструктуре.

Эффекты

Беспроводной защищенный на физическом уровне доступ в Интернет за счет прямолинейного распространения света, что делает любой взлом заметным	Запасной канал передачи информации, когда радиочастотный спектр заглушен или отключен в результате атаки на критическую инфраструктуру, например, метро	Реализация «последней мили» при доставке предраспределенных криптографических ключей на смартфоны, планшеты, ноутбуки конечных пользователей

Модуль шифрования «МШ-ТР-СКР» из состава комплекса средств криптографической защиты конфиденциальной информации «Квазар»

Технология

Квантовые коммуникации

Бизнес-процесс

- Защита высокоскоростных каналов передачи данных

Стоимость внедрения

По запросу

Срок внедрения

7-10
месяцев

Тип инсталляции

On-premise

Экспорт решения

Нет

УГТ **7**

Наличие сертификации и аттестации:

ФСТЭК России	не требуется
ФСБ России	2026 г.

Уровень доверия в соответствии со ФСТЭК России

не требуется

Класс сертификации ФСБ России

КС3

Поставщик

СПБ СИСТЕМЫ ПРАКТИЧЕСКОЙ БЕЗОПАСНОСТИ

ООО «Системы практической безопасности»

Потенциальные заказчики

- Интеграторы и операторы квантовых сетей

Проблема

Защита высокоскоростных каналов требует частой смены ключей из-за большой нагрузки на ключ.

Необходимость частого ручного ввода ключей создает неудобство эксплуатации, в том числе связанные с перерывом в работе СКЗИ на время ввода ключей.

Защита высокоскоростных каналов требует обеспечения минимальных задержек на шифрование.

Решение

Модуль шифрования «МШ-ТР-СКР» из состава комплекса СКЗИ конфиденциальной информации «Квазар» — высокоскоростные транспондеры с встроенной функцией шифрования для оптических сетей и интерфейсом сопряжения с квантовой криптографической системой выработки и распределения ключей (ККС ВРК) позволяют организовать защиту высокоскоростного канала 10Гбит/с между территориально разнесенными центрами обработки данных или различными филиалами организации.

МШ-ТР-СКР обеспечивает криптографическую защиту конфиденциальной информации при передаче по OTN-сети, а также с применением спектрального уплотнения (DWDM).

Обеспечен увеличенный срок использования основных ключей за счет применения квантовых ключей, полученных от ККС ВРК.

Совместимость с коммуникационным оборудованием различных вендоров. Работа на уровне Ethernet-кадров не накладывает ограничений на протоколы более высокого уровня.

Поддержка протокола Fibre Channel и низкая задержка при передаче информации позволяет эффективно использовать СКЗИ комплекса «Квазар» для организации защищенных сетей хранения данных и связи ЦОД, без использования дополнительных преобразователей Fibre Channel — Ethernet.

Эффекты

Повышение автономности и безопасности за счет постоянной автоматической смены ключевой информации с помощью полученных от ККС ВРК квантовых ключей	Снижение затрат на организацию технических мер при процедуре смены ключей	Удобство эксплуатации, возможность использования на необслуживаемых объектах

Экспериментальная система криптографического квантового хэширования для верификации данных

Технология

Квантовые коммуникации

Бизнес-процесс

- Обеспечение ИБ

Стоимость внедрения

Эксперимен-тальный доступ — **120–150** млн руб.

Лицензия — **НИОКР**

Срок внедрения

2025–2027
Лабораторный прототип

2028–2030
Пилот в ГИС

Тип инсталляции

On-premise

Экспорт решения

Нет

УГТ **1,2**

Наличие сертификации и аттестации:

- ФСТЭК России
- ФСБ России

Уровень доверия в соответствии со ФСТЭК России

-

Класс сертификации ФСБ России

-

Поставщик

КФУ, КФТИ КазНЦ РАН

Потенциальные заказчики

-

Проблема

1. Уязвимость классических хэш-функций к атакам на квантовых компьютерах (алгоритм Шора)
2. Ограниченная стойкость к коллизиям при росте объемов данных
3. Невозможность верификации без раскрытия ключей

Решение

Модуль квантового хэширования, интегрируемый в существующие КРК-системы, преобразует данные в квантовые состояния (суперпозиции) с гарантированной стойкостью к восстановлению прообраза и появлению коллизий. Поддерживает модельные протоколы цифровой подписи (Готтесмана — Чанга) и верификации. Система преобразует цифровые данные (пароли, ключи, документы) в «квантовые слепки» — особые состояния света или атомов, которые невозможно скопировать или подделать. В отличие от обычных хэшей (где данные сжимаются в строку символов), здесь информация «растворяется» в квантовой системе, сохраняя связь с исходными данными, но делая их восстановление физически невозможным.

Ключевые компоненты:

1. Генератор квантовых хэшей
2. Модуль верификации
3. Интеграция с КРК

Эффекты

Абсолютная защита от квантовых атак	Экономия на инфраструктуре. Сокращение затрат на внедрение в 3–5 раз	Проверка подлинности данных без передачи секретов

Защита облачного хранилища и ЦОД

Технология

Квантовые коммуникации

Бизнес-процесс

- Обеспечение ИБ
- ИТ-обеспечение и связь
- Обслуживание и ведение банковских счетов
- Управление и оптимизация финансового портфеля

Стоимость внедрения

от 40
млн руб.

ПАК

Срок внедрения

от 6
месяцев

ПАК

Тип инсталляции

-

Экспорт решения

Нет

УГТ **8**

Наличие сертификации и аттестации:

ФСТЭК России ✓

ФСБ России ✓

Уровень доверия в соответствии со ФСТЭК России

-

Класс сертификации ФСБ России

КС3

Поставщик

QRATE

ООО «КуРэйт»

Потенциальные заказчики

- Банковские организации
- Организации, хранящие и обрабатывающие личные данные

Проблема

С развитием квантовых вычислений традиционные методы защиты данных в облачных хранилищах и ЦОД могут утратить устойчивость к атакам со стороны злоумышленников, что потенциально создаст угрозу компрометации конфиденциальной информации и приведет к финансовым и репутационным потерям организаций. Системы квантового распределения ключей, применяемые в решениях для защиты облачного хранения и ЦОД, обеспечивают устойчивость к атакам с применением квантовых вычислений и исключают человеческий фактор при выработке и распределении криптографических ключей, формируя физически защищенную основу ИБ.

Решение

Для обеспечения защиты данных при их передаче между центрами обработки данных или при загрузке в облако, в инфраструктуру интегрируется аппаратно-программный комплекс квантового распределения ключей. Он устанавливается на каждой стороне защищаемого канала и работает в тандеме с уже существующими средствами криптографической защиты (канальными шифраторами) класса КС3.

Система КРК в автоматическом режиме, без участия человека, генерирует и поставляет на шифраторы абсолютно секретные симметричные ключи.

Ключевое преимущество такого подхода — возможность частой смены ключей шифрования.

В то время как в классических системах один ключ может использоваться на протяжении года, КРК позволяет обновлять его с периодичностью вплоть до нескольких раз в секунду. Это кардинально снижает нагрузку на каждый отдельный ключ и практически до нуля сокращает временное окно для потенциальной атаки.

Эффекты

Повышение уровня доверия	Снижение успешности атак с применением квантовых вычислителей до 1%	Оптимизация защитных мер

Защита канала видеосвязи

Технология

Квантовые коммуникации

Бизнес-процесс

- ИБ
- Управление качеством услуг
- ИТ-обеспечение и связь
- Разработка продуктов и предложений
- Управление рисками

Стоимость внедрения

от 40
млн руб.

Лицензия

Срок внедрения

от 6
месяцев

Лицензия

Тип инсталляции

-

Экспорт решения

Нет

УГТ **8**

Наличие сертификации и аттестации:

ФСТЭК России ✓

ФСБ России ✓

Уровень доверия в соответствии со ФСТЭК России

-

Класс сертификации ФСБ России

КС3

Поставщик

QRATE

ООО «КуРэйт»

Потенциальные заказчики

- Операторы сотовой связи
- Интернет-провайдеры
- Разработчики телеком-оборудования

Проблема

По мере развития квантовых вычислений классические методы шифрования каналов видеосвязи потенциально могут перестать обеспечивать необходимый уровень защиты, что может привести к раскрытию корпоративных переговоров и утечке стратегически важной информации. Системы квантового распределения ключей, применяемые для защиты каналов видеосвязи, противостоят угрозам со стороны квантовых компьютеров и устраняют угрозу человеческого фактора при выработке и распределении криптографических ключей, используемых для защиты канала связи, обеспечивая тем самым защиту трафика.

Решение

Для защиты сеансов ВКС на узлах связи, обслуживающих трафик, устанавливается серверное решение — ККС ВРК в связке с канальным шифратором класса КС3.

Система является источником ключевой информации для систем шифрования видео- и аудиопотоков в реальном времени. Технология позволяет реализовать на физическом уровне принцип «совершенной прямой секретности» (perfect forward secrecy). Это означает, что для каждого короткого сегмента разговора система КРК сможет сгенерировать новый, абсолютно уникальный ключ шифрования.

Таким образом, даже гипотетическая компрометация одного ключа позволит злоумышленнику получить доступ лишь к ничтожному фрагменту данных длительностью в доли секунды. Вся остальная часть сеанса связи, как прошлая, так и будущая, останется в полной безопасности.

Эффективность данного подхода была неоднократно подтверждена в рамках пилотных проектов и демонстраций для крупнейших российских корпораций и государственных структур, что доказывает готовность систем ККС ВРК к защите критической информации.

Эффекты

Снижение количества утечек	Рост выручки от продажи услуг видеосвязи	Повышение уровня информационной безопасности

Защита канала корпоративных коммуникаций

Технология

Квантовые коммуникации

Бизнес-процесс

- ИБ
- Управление качеством услуг
- ИТ-обеспечение и связь
- Разработка продуктов и предложений
- Управление рисками

Стоимость внедрения

от 40
млн руб.

Лицензия

Срок внедрения

от 6
месяцев

Лицензия

Тип инсталляции

-

Экспорт решения

Нет

УГТ **8**

Наличие сертификации и аттестации:

ФСТЭК России ✓

ФСБ России ✓

Уровень доверия в соответствии со ФСТЭК России

-

Класс сертификации ФСБ России

КС3

Поставщик

QRATE

ООО «КуРэйт»

Потенциальные заказчики

- Операторы сотовой связи
- Интернет-провайдеры
- Разработчики телеком-оборудования

Проблема

Передача рабочих документов, файлов или сообщений по незащищенным каналам связи может привести к серьезным утечкам данных, включая как личную информацию сотрудников, так и корпоративные сведения. Одним из наиболее уязвимых мест в этом процессе является само устройство, например смартфон пользователя.

Решение

Для решения данной проблемы используется многоуровневая гибридная система.

На центральных узлах корпоративной сети устанавливается аппаратно-программный комплекс КРК, который непрерывно генерирует массив абсолютно случайных и секретных сессионных ключей.

Далее эти ключи по внутреннему защищенному каналу передаются на автоматизированное рабочее место (АРМ) администратора безопасности.

Администратор записывает полученные сессионные ключи на персональные аппаратные носители сотрудников.

Когда сотруднику необходимо установить защищенный сеанс связи, он прикладывает свою карту к считывателю, подключенному к его компьютеру, и сессионный ключ загружается непосредственно в коммуникационный сервис. Этот метод полностью изолирует процесс генерации и распределения ключей от потенциально уязвимой программной среды на конечном устройстве, создавая надежный «внешний» контур безопасности.

Эффекты

Повышение защищенности корпоративной сети	Вероятность утечки рабочей информации 0,7%	Повышение уровня информационной безопасности

Защита системы контроля управления доступом (СКУД)

Технология

Квантовые коммуникации, квантовая сенсорика

Бизнес-процесс

- ИБ
- Управление рисками
- ИТ-обеспечение и связь
- Разработка сервисов
- Соревнования профессиональ-ного мастерства

Стоимость внедрения

от 40
млн руб.

Лицензия

Срок внедрения

от 6
месяцев

Лицензия

Тип инсталляции

On-Premise

Экспорт решения

Нет

УГТ **6**

Наличие сертификации и аттестации:

ФСТЭК России ✓

ФСБ России ✓

Уровень доверия в соответствии со ФСТЭК России

-

Класс сертификации ФСБ России

КС3

Поставщик

QRATE

ООО «КуРэйт»

Потенциальные заказчики

- Банковские организации
- Организации, хранящие и обрабатывающие личные данные
- ФОИВ
- Промышленные и производственные компании (КИИ)
- Операторы платных дорог

Проблема

Современные системы контроля и управления доступом (СКУД) часто остаются примитивными с точки зрения защиты от подготовленного нарушителя. Многие решения ограничиваются базовыми механизмами (карты доступа, турникеты, простые биометрические сканеры), которые можно легко обойти. Также СКУД редко соответствуют строгим нормативно-правовым актам (НПА) в сфере информационной безопасности.

Решение

В центральный сервер СКУД интегрируется система ККС ВРК QKD312.

Она функционирует как источник уникальных криптографических ключей. Это позволяет полностью отказаться от статичных идентификаторов в системе.

При каждом запросе на доступ система генерирует и передает на токен доступа сотрудника уникальный одноразовый ключ. Этот ключ может использоваться как для одной сессии аутентификации, так и на более длительный срок после чего немедленно уничтожается из сервера СКУД, а также с токена.

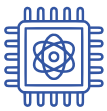
Проблема клонирования полностью решается: даже если злоумышленник сможет скопировать данные одной сессии, они будут бесполезны, так как для следующего прохода потребуется совершенно новый ключ. Система КРК гарантирует, что ключи генерируются и распределяются без малейшей возможности перехвата, превращая статичную СКУД в динамическую и защищенную от копирования систему.

Эффекты

Снижение количества утечек корпоративной информации	Оптимизация защитных мер	Повышение уровня информационной безопасности

Программная платформа для исследования уязвимостей методов шифрования к атакам на основе новых физических принципов

Технология



Квантовые вычисления

Бизнес-процесс

- Развитие инфраструктуры информационной безопасности
- Исследование новых вызовов отрасли ИБ

Стоимость внедрения

2–6	5–12
млн руб.	млн руб.
Лицензия	**НИОКР**

Срок внедрения

1	5-18
месяц	месяцев
Лицензия	**НИОКР**

Тип инсталляции

Программный пакет: сборка ПО под инфраструктуру заказчика, выполнение НИР/НИОКР на собственном оборудовании

Экспорт решения

Нет

УГТ 9

Наличие сертификации и аттестации:

ФСТЭК России	☑
ФСБ России	☑

Класс защищенности ИС по ФСТЭК России

–

Класс сертификации ФСБ России

–

Поставщик

S-Quantum

ООО «С-Квантум»

Потенциальные заказчики

- Разработчики СКЗИ
- Лаборатории сертификации

Проблема

Новые подходы к разработке квантовых алгоритмов меняют характер квантовой угрозы с порогового, ограниченного недостижимыми на горизонте 2–3 лет числом кубитов и глубиной алгоритма, на постепенно нарастающий. Вариационные алгоритмы и квантовое машинное обучение допускают реализацию атаки на ограниченный сегмент симметричного ключа и учет прочих сторонних данных для снижения требований к квантовому вычислителю.

Невозможность теоретического доказательства стойкости постквантовых алгоритмов шифрования.

Решение

Разработка реалистичного эмулятора, построенного с учетом глубоких принципов взаимодействия носителей квантовой информации с их окружением в аппаратном квантовом вычислителе.

Разработка и тестирование новых методов квантового и гибридного криптоанализа с использованием данного эмулятора.

Особенно актуально в данном контексте исследование вариационных квантовых алгоритмов для атаки на постквантовые методы защиты информации, стойкость которых в данный момент не может быть фундаментально доказана. Являясь методом решения задачи без заранее определенного алгоритма, вариационный квантовый криптоанализ потенциально способен указать на уязвимость разрабатываемых шифров к атаке квантовым вычислителем.

Эффекты

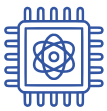
Разработан отечественный эмулятор квантовых вычислений, способный работать с регистрами до 37 кубитов в реалистичном режиме с учетом неунитарных шумов и моделированием смешанных квантовых состояний.

Обнаружен подход к реализации квантового криптоанализа, снижающий требования для атаки шифра S-AES с 32 до 23 кубитов в общем случае и до 11 кубитов при частичной утечке ключа.

Создан метод эмпирического тестирования для постквантовых методов шифрования, обеспечен технологический суверенитет разработок в данной области.

Квантовый эмулятор для реалистичного высокоточного моделирования квантовых алгоритмов

Технология



Квантовые вычисления

Бизнес-процесс

- RnD
- Цифровизация и развитие перспективной инфраструктуры

Стоимость внедрения

2–6 млн руб.	**4–6** млн руб.
Лицензия	**НИОКР**

Срок внедрения

1 месяц	**5-12** месяцев
Лицензия	**НИОКР**

Тип инсталляции

Программный пакет: сборка ПО под инфраструктуру заказчика, выполнение НИР/НИОКР на собственном оборудовании

Экспорт решения

Нет

УГТ **9**

Наличие сертификации и аттестации:

- ФСТЭК России ☑
- ФСБ России ☑

Класс защищенности ИС по ФСТЭК России

–

Класс сертификации ФСБ России

–

Поставщик

S-Quantum

ООО «С-Квантум»

Потенциальные заказчики

- Компании, планирующие внедрение квантовых технологий в ИБ
- Операторы облачных сервисов
- Крупные корпорации и инфраструктурные организации

Проблема

Отсутствие у компаний в сфере ИБ реальных сценариев применения квантовых технологий и квантового преимущества на доступном аппаратном обеспечении, особенно отечественном.

Отсутствие реалистичных инструментов моделирования увеличивает инвестиционные риски при вхождении в отрасль квантовых вычислений и квантовых коммуникаций.

Решение

Разработан специализированный квантовый эмулятор для высокоточного моделирования квантовых алгоритмов с учетом физических шумов.

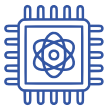
Позволяет на основе реальных экспериментальных данных о томографии квантовых гейтов прототипа квантового компьютера, получить декомпозицию матрицы процесса и использовать ее для моделирования реальных возможностей данной аппаратной конфигурации. Кроме того, данный подход применим для моделирования квантовых коммуникаций ввиду сложной природы шумов в реальных сетях квантового распределения ключей. Поддерживает масштабируемое параллельное моделирование (CPU/GPU, распределенные кластеры). Продемонстрировано моделирование регистра на 37 кубитов с реалистичными шумами — рекорд среди российских разработок.

Эффекты

Минимизация инвестиционных рисков при планировании внедрения квантовых технологий	Возможность реалистичной оценки готовности отечественного оборудования к решению задач ИБ	Подготовка инфраструктуры к будущему переходу на реальный квантовый компьютер без переделки ИТ-систем

Гибридный программный пакет для решения обобщенных задач комбинаторной оптимизации и машинного обучения

Технология



Квантовые вычисления

Бизнес-процесс

- RnD
- Цифровизация и развитие перспективной инфраструктуры

Стоимость внедрения

2–6 млн руб.	5–12 млн руб.
Лицензия	**НИОКР**

Срок внедрения

1 месяц	5-18 месяцев
Лицензия	**НИОКР**

Тип инсталляции

Программный пакет: сборка ПО под инфраструктуру заказчика, выполнение НИР/НИОКР на собственном оборудовании

Экспорт решения

Нет

УГТ 3

Наличие сертификации и аттестации:

- ФСТЭК России
- ФСБ России

Класс защищенности ИС по ФСТЭК России

-

Класс сертификации ФСБ России

-

Поставщик

S-Quantum

ООО «С-Квантум»

Потенциальные заказчики

- Компании, обрабатывающие большие массивы данных в ИБ
- Финансовые организации
- Операторы облачных сервисов

Проблема

Отсутствие инструментов поиска путей эффективного применения перспективных квантовых вычислителей для машинного обучения в сфере ИБ, допускающих подключение к реальным квантовым компьютерам для коммерциализации их вычислительного преимущества.

Решение

Разработка гибридного программного пакета, сочетающего:

- Классические методы оптимизации (работают на существующей ИТ-инфраструктуре).
- Гибридные квантово-классические методы машинного обучения (с использованием реалистичного квантового эмулятора).

Система обеспечивает импортозамещение зарубежных оптимизационных пакетов и автоматизированный поиск сценариев квантового преимущества внутри цифрового периметра клиента. При появлении аппаратных квантовых вычислителей, достаточных для реализации обнаруженных сценариев, вычислительное ядро системы может быть заменено с эмулятора на реальный вычислитель без изменений в инфраструктуре клиента. Реализуется сервис «подписки на квантовое преимущество» и полная квантовая готовность инфраструктуры заказчика, то есть готовность к мгновенному, бесшовному и безрисковому переходу к коммерческой реализации квантового преимущества.

Эффекты

Готовность инфраструктуры к мгновенному переходу на квантовые вычисления.	Импортозамещение зарубежных оптимизационных пакетов.	Снижение временных и финансовых затрат на интеграцию квантовых решений в ИБ-системы до 50%.

Программно-аппаратный комплекс адаптивной оптической системы для подавления негативных эффектов атмосферной турбулентности

Технология

Квантовые коммуникации

Бизнес-процесс

- ИБ
- ИТ-обеспечение и связь

Стоимость внедрения

От 35
млн руб.

Срок внедрения

12-18
месяцев

2025–2027

НИОКР

Лабораторный прототип

Тип инсталляции

On-premises

Экспорт решения

Нет

УГТ **4**

Наличие сертификации и аттестации:

- ФСТЭК России
- ФСБ России

Уровень доверия в соответствии со ФСТЭК России

6

Класс сертификации ФСБ России

КС1

Поставщик

МТУСИ

Потенциальные заказчики

- ОАО «РЖД»
- ПАО «Ростелеком»
- АО «ИнфоТеКС»
- ООО «КуРэйт»
- ООО «КуСпэйс Технологии»

Проблема

Потребность в стабильной и высокоскоростной оптической связи на горизонтальных, вертикальных и наклонных трассах, где качество передачи лазерного сигнала существенно зависит от возмущений волнового фронта, вызванных атмосферной турбулентностью.

Решение

Многофункциональный аппаратно-программный комплекс с функциями одновременного измерения параметров атмосферной турбулентности, компенсации искажений фазы излучения и отслеживания изменений количества передаваемых квантовых единиц позволит увеличить качество передачи информации в беспроводном оптическом канале связи. Эффекты атмосферной турбулентности приводят к повышению величины квантовых битовых ошибок в каналах связи, использующих протокол BB84.

В качестве измерителя волнового фронта будет использоваться датчик Шака — Гартмана, в качестве устройства стабилизации пучка и исправления искажений волнового фронта будет выступать деформируемое зеркало.

Эффекты

Увеличение дальности передачи излучения на дистанцию с 500 м до 1 км без потери качества связи в условиях средней турбулентности для приземных горизонтальных оптических трасс	Увеличение скорости передачи информации и увеличение уровня сигнала до 4 дБ	Снижение уровня битовых ошибок с 20% до порогового значения менее чем 11%

Система повышения коэффициента сопряжения с волокном для снижения уровня битовых ошибок

Технология

Квантовые коммуникации

Бизнес-процесс

- ИБ
- ИТ-обеспечение и связь

Стоимость внедрения

От 35
млн руб.

Срок внедрения

12-18
месяцев

НИОКР

Тип инсталляции

On-premises

Экспорт решения

Нет

УГТ **4**

Наличие сертификации и аттестации:

ФСТЭК России ✓

ФСБ России ✓

Уровень доверия в соответствии со ФСТЭК России

6

Класс сертификации ФСБ России

КС1

Поставщик

МТУСИ

МТУСИ

Потенциальные заказчики

- ОАО «РЖД»
- ПАО «Ростелеком»
- АО «ИнфоТеКС»
- ООО «КуРэйт»
- ООО «КуСпэйс Технологии»

Проблема

Квантовые системы передачи информации требуют как повышения эффективности доставки данных от источника к приемнику, так и увеличения дальности доставки. Для успешного решения проблемы необходимо учитывать и исправлять негативное влияние атмосферной турбулентности и аэрозольного рассеяния на оптический канал связи, а также разрабатывать новые алгоритмы управления адаптивными системами.

Решение

Адаптивная оптическая система коррекции искажений оптического излучения с помощью деформируемых зеркал. Ключевая идея состоит в том, что, компенсируя с помощью адаптивного зеркала волновой фронт излучения, прошедшего сквозь турбулентную и рассеивающую среду, можно существенно повысить коэффициент связи и снизить коэффициент битовых ошибок.

Система может адаптироваться под разные условия, и при этом лишена недостатков аналогичных методов формирования профилей, таких как амплитудные маски, голографические, дифракционные элементы.

Эффекты

Повышение эффективности квантового канала связи	Увеличение эффективности связи (Coupling Efficiency) на 30–40%	Снижение коэффициента битовых ошибок (Bit Error Rate) на 2 порядка, с 10^{-5} до 10^{-7}

Все кейсы размещены на портале Техлид.рф

КРК — сервис усиленной защиты каналов связи

Сервис КРК — это максимально высокий уровень защиты каналов связи с помощью СКЗИ с использованием технологии квантового распределения ключей. Не нужно покупать, внедрять и сертифицировать дорогостоящее квантовое оборудование. Достаточно просто подключить сервис КРК.

Ростелеком

Для кого

- Государственные органы и компании с государственным участием
- Финансовый сектор
- Медицинский сектор
- Центры обработки данных

Возможности

Автоматизация

Секретные ключи генерируются и передаются автоматически без участия человека.

Информирование клиентов

Оповещение клиента о воздействии на канал связи без компрометации защищаемой информации.

Гибкие политики

Если квантовый канал неисправен, можно как разрешить, так и запретить обмен информацией с использованием классических ключей шифрования.

Усиленная защита

Любое воздействие на канал связи детектируется, перехватить секретный ключ невозможно.

Варианты предоставления сервиса

В ЦОД «Ростелекома»

I. Вы размещаете ресурсы в ЦОД «Ростелекома», передача данных между которыми защищена с применением технологии КРК.

На площадках клиента

II. «Ростелеком» строит защищенный канал между вашими площадками с использованием алгоритма шифрования ГОСТ и технологии КРК.

ЦОДы «Ростелекома»

Преимущества

- **01.** Надежная защита передаваемой информации
- **02.** Устранение угрозы ИБ в долгосрочной перспективе
- **03.** Минимизация влияния человеческого фактора при работе с ключами шифрования
- **04.** В основе сервиса передовые отечественные технологии и оборудование
- **05.** Эксплуатация силами компании «Ростелеком-Солар»
- **06.** Не нужно покупать дорогостоящее квантовое оборудование

Инфраструктурное обеспечение развития квантовых технологий: оборудование, проекты, перспективы

Квантовая сеть в России: инфраструктура, достижения и цели

Ключевые вызовы:

- Создание индустрии и рынка квантовых коммуникаций
- Реализация сформированного технологического потенциала в виде передовых продуктов
- Достижение технологического суверенитета в области магистральных, абонентских и атмосферных квантовых сетей
- Развитие экосистемы: стандарты, кадры, регулирование

Протяженность наземной квантовой магистральной сети:

2025 год › 7 000 км
2030 год › 15 000 км

— Построено к 2025 году - - - Будет построено к 2030 году

Центр управления и мониторинга магистральной квантовой сети 24/7

186	545	465	2 319	>300 000
узлов сети под мониторингом	единиц квантового оборудования	единиц сетевого оборудования	датчиков инженерных систем	параметров под мониторингом

Инфраструктурное обеспечение развития квантовых технологий: оборудование, проекты, перспективы

Проекты в стадии разработки или пилотирования

- На ПМЭФ-2025 **Банк ВТБ, ОАО «РЖД» и холдинг Т1** объявили о расширении трехстороннего соглашения в сфере ИТ с акцентом на квантовые коммуникации. В рамках партнерства стартует пилотный проект на базе ВТБ и создается прототип программно-аппаратного комплекса (ПАК) **«Квантовый криптоанклав»**, не имеющего аналогов в России и впервые представленного рынку в 2023 году. Это высокозащищенная платформа нового поколения для конфиденциальной обработки данных и создания моделей машинного обучения в режиме полной анонимности. В основе — технология квантового распределения ключей, обеспечивающая невзламываемый обмен данными. Архитектура построена полностью на **российских технологиях**. Поддерживает автоматическую фильтрацию, шифрование, передачу и анализ информации
- **ОАО «РЖД» и ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации»** реализуют пилотное внедрение квантовых коммуникаций между информационными системами госорганов и банков с использованием магистральной квантовой сети ОАО «РЖД». **По итогам проекта будут разработаны типовые требования и рекомендации для финансового сектора**.

Текущее научно-техническое развитие

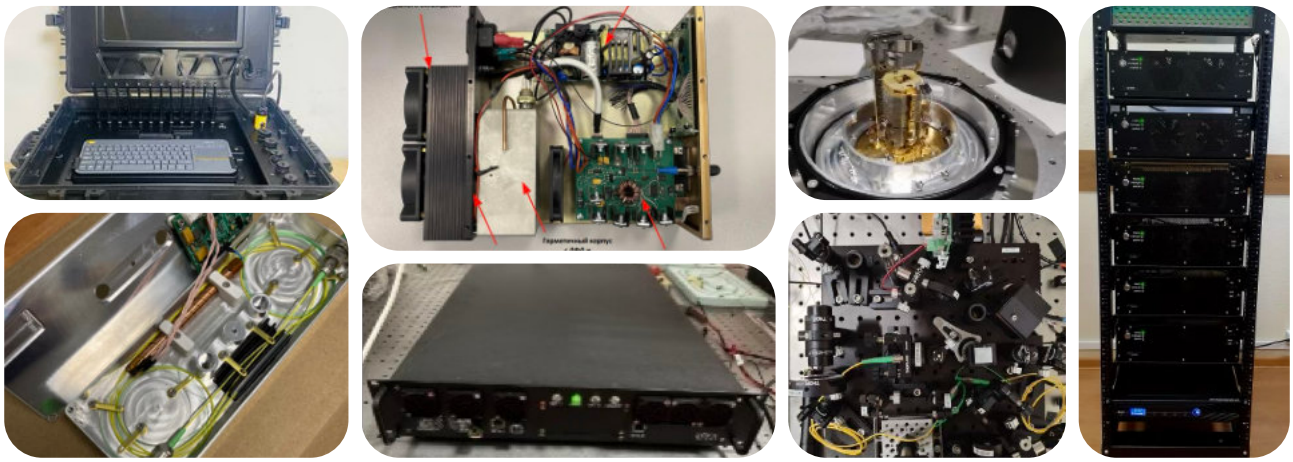
Количество научно-технических работ, шт.

Создано 18 образцов компонентов, устройств и систем квантовых коммуникаций, включая:

- **13** экспериментальных образцов.
- **5** опытных образцов.
- Получено **78** заявок на государственную регистрацию результатов интеллектуальной деятельности.
- Приняты в печать **46** статей для публикации в научно-технических журналах.

Импортозамещение:

- Приемник одиночных фотонов
- Электрооптический модулятор
- Низкошумящий детектор одиночных фотонов
- Волоконно-оптические фильтры
- Источники одиночных фотонов



Инфраструктурное обеспечение развития квантовых технологий: оборудование, проекты, перспективы

Итоги 2024 года и перспективы 2030 года в области развития кадрового потенциала по квантовым технологиям:

По итогам 2024 года:

- Профстандарт «Специалист по монтажу и технической эксплуатации квантовых сетей»
- Профстандарт «Специалист по исследованиям и разработкам в области квантовых коммуникаций»
- ФГОС СПО по специальности 11.02.19 «Квантовые коммуникации»

> 30
вузов реализуют образовательные программы

> 700
специалистов в области квантовых коммуникаций

К 2030 году

> 1600
специалистов, закончивших бакалавриат

> 1700
специалистов, закончивших магистратуру

> 90
специалистов, закончивших аспирантуру

28
образовательных программ, реализуемых вузами по всем уровням подготовки

Ожидаемые результаты к 2030 году

- Создан **сервис оператора связи,** включающий в себя автоматизированные информационные системы предоставления сервисов с гарантированным SLA, систему учета и расчетов (биллинг) для сервисов квантовых коммуникаций, зонтичную систему управления инцидентами **24/7**.
- Создана **инфраструктура для развития абонентский сетей** в крупнейших агломерациях России, обеспечен **географический охват магистральной инфраструктуры** (15 000 км магистральной квантовой сети), **созданы клиентские мультивендорные сети**.
- Разработано **более 10** перспективных технологий.
- **x3** созданных результатов интеллектуальной деятельности (более 150 патентов).
- **Рост уровня готовности** приоритетных технологий по основным направлениям.
- **Более 4 млн пользователей** информационных систем и сервисов с применением технологии квантовых коммуникаций.
- Обеспечена **локализация 80 %** номенклатуры критически важных оптических компонентов.
- **x2** рост экосистемы квантовых коммуникаций; система образования обеспечивает **100 % кадровой потребности** отрасли.
- Сформирована система нормативного регулирования отрасли и технической стандартизации **(принято более 35 НПА и стандартов)**.

ОАО «РЖД» утвержден План мероприятий по продвижению российских интересов по международной стандартизации в высокотехнологичной области «Квантовые коммуникации» на период до 2030 года.

Инфраструктурное обеспечение развития квантовых технологий: оборудование, проекты, перспективы

Квантовые итоги 2025 года:

- Готовность к аттестации Магистральной квантовой сети ОАО «РЖД» с сертифицированными ViPNet QTS РУКС, ViPNet L2Q-10G
- Сформированы планы по научно-исследовательским работам на МУКС для ВУЗов подключенных к МУКС оборудованием ViPNet QTS

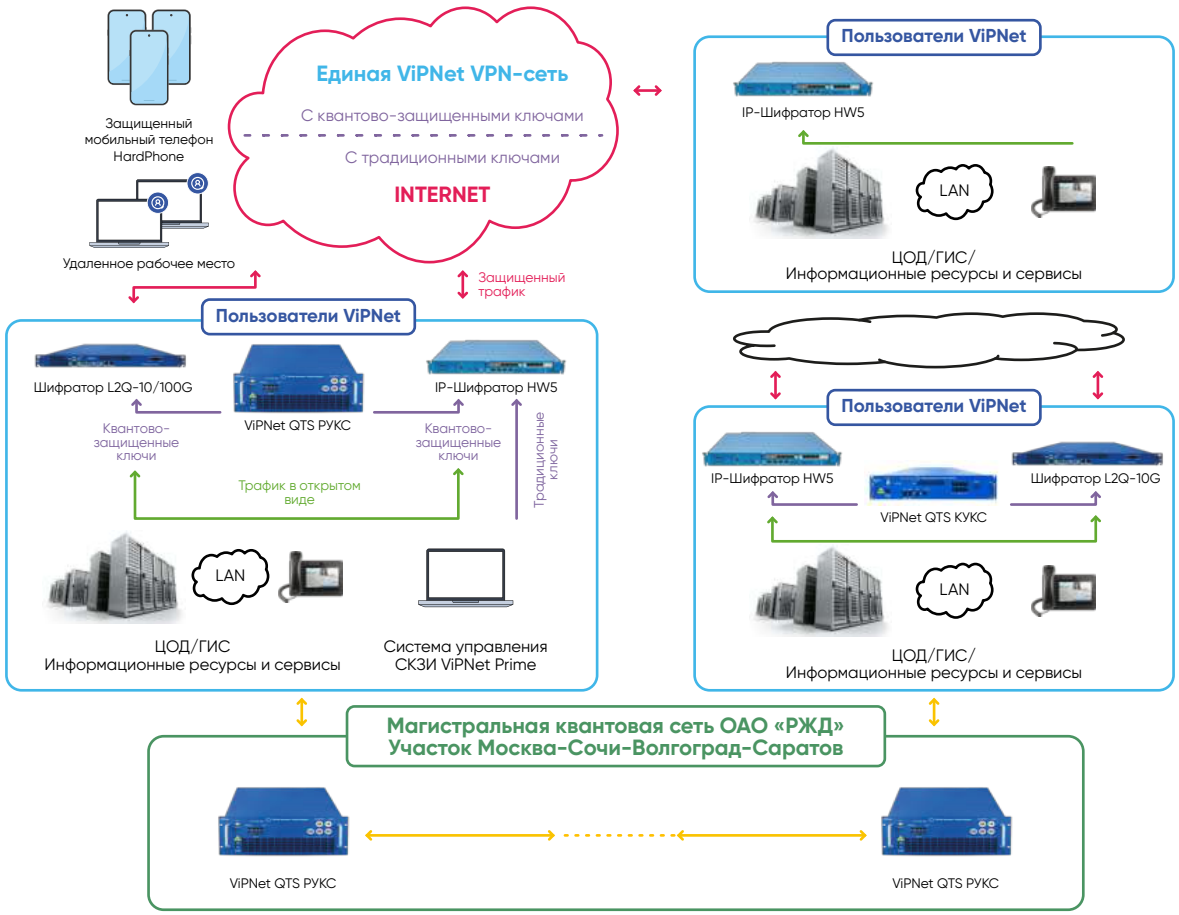
Разработаны/модернизированы и подготовлены к сертификации:

- ViPNet QTS КУКС - клиентский узел квантовой сети ViPNet
- ViPNet L2Q-100G - высокоскоростной L2-шифратор для работы с квантово-защищенными ключами
- ViPNet Coordinator HW 5 – криптошлюзы, умеющие работать в гибридных сетях (одновременно с традиционными и квантово-защищенными ключами)
- ViPNet Client – клиентское программное обеспечение, умеющее работать с квантово-защищенными ключами

Разработан и протестирован образец ViPNet QTS DWDM – система квантового распределения ключей, работающая в DWDM канале (не требует выделенной ВОЛС)

Разработан ViPNet QCL – Учебно-методический комплекс Квантовая криптографическая лаборатория

Гибридная VPN-сеть ViPNet



Инфраструктурное обеспечение развития квантовых технологий: оборудование, проекты, перспективы

QLab

QRATE

Научно-образовательный комплекс (НОК) по квантовым коммуникациям и фотонике

НОК предназначен для обучения квантовой оптике, информационной безопасности, программированию, а также реализации научных проектов в учебных заведениях.

Он является ключевой частью обучения по квантовым коммуникациям крупнейших российских образовательных учреждений.

Преимущества решения:

- Единственное в мире образовательное решение в области квантовых коммуникаций, выполненное на оптическом волокне устройство максимально приближено к промышленному оборудованию.
- Единственная система КРК, которая включена в инфраструктурные листы чемпионатов профессионального мастерства в компетенции «квантовые технологии» («Профессионалы» и AtomSkills).
- Модульный рабочий стол позволяет собирать и исследовать различные оптические схемы.
- QLab позволяет моделировать критерии отказа квантовых сетей и традиционных СКЗИ.

Оборудование используется в:

Томский государственный университет · МТУСИ · МФТИ · МИСИС · К54 · ГУАП

Соответствие профстандарту 06.050

Обобщенные трудовые функции	EDU – QCRY1 (Thorlabs)	QLab (QRate)
Монтаж, контроль технических характеристик и техническое обслуживание оптической части сети квантовых коммуникаций	○	●
Монтаж оборудования станционной части сети квантовых коммуникаций	○	●
Организация монтажных работ и комплексная проверка монтажа участка сети квантовых коммуникаций	○	●
Организация технического обслуживания и материально-технического обеспечения технической эксплуатации сети квантовых коммуникаций	○	●
Устранение технических проблем и технологическое обеспечение технической эксплуатации участка сети квантовых коммуникаций	●	●

Технические характеристики:

Рабочая длина волны	1550 нм
Оптика	Волоконная схемотехника
Протокол	BB84
Габариты блока «Алиса»	496x285x496 мм
Габариты блока «Боб»	496x285x496 мм
Потребляющая мощность	до 2 кВт
Электропитание	50 Гц, 220 В

QKDmini

Миниатюрный передатчик для системы квантового распределения ключей

QKDmini — это уменьшенная версия передающего блока системы квантового распределения ключей QKD312, предназначенная для построения квантово-защищенных сетей топологии «звезда». Позволяет создавать гибкую систему, которая устанавливается поверх существующей инфраструктуры и работает совместно с предустановленными средствами криптографической защиты информации (СКЗИ).

Миниатюрная клиентская часть позволяет реализовывать квантовое распределение ключей с использованием топологии «один ко многим» и снижает стоимость решения.

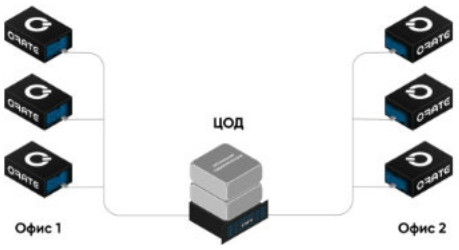
Продукт является актуальным решением для обеспечения безопасности в корпоративных сетях, объектах критической инфраструктуры и беспилотного транспорта.

Уровень готовности технологии: 6

Технические характеристики:

Протокол функционирования QKDmini	BB84 Decoy-State
Функциональный диапазон длины волны, нм	1 550 ± 10
Частота приготовления квантовых состояний, МГц	312,5
Скорость генерации ключа на расстоянии до 30 км, Кбит/с	10
Максимальное расстояние между доверенными узлами, км	100
Пиковая потребляемая мощность, Вт	200
Интерфейс интеграции в аппаратуру потребителя	PCI Express x16 (v3.0)
Максимальное число передатчиков на приемник	128
Габариты, Ш*Д*В, мм	150*317*88

Схема применения QKDmini:



Варианты применения технологии:

- Локальные сети
- Квантовый блокчейн
- Квантово-защищенное распределенное хранение данных
- Гибридный блокчейн квантовой сети с внешними классическими узлами

QButterfly

Детектор одиночных фотонов

Технология детектирования фотонов находит применение в различных научных и промышленных областях: в квантовой криптографии, телекоммуникациях, спектроскопии, разработке лекарственных препаратов, анализе ДНК, в системах газового мониторинга, флуоресцентной микроскопии, а также в производстве лидаров — ключевой системе беспилотных автомобилей.

Детектор одиночных фотонов (ДОФ) QButterfly — полностью отечественная разработка, сигнальные и шумовые характеристики которого соответствуют уровню ведущих мировых аналогов. Помимо этого, он обладает компактными размерами и удобным интерфейсом управления с возможностью гибкой подстройки параметров детектора под конкретную задачу.

Преимущества разработки ООО «КуРэйт» заключаются в низком уровне темновых отсчетов и настраиваемых параметрах задержек и мертвого времени. Возможно изменение характеристик продукта под нужды заказчика.

Уровень готовности технологии: 9

Технические характеристики:

Темновой счет, кГц	≤ 2
«Мертвое время», мкс	≤ 100
Тип оптоволокна	SMF
Потребляемый ток, А	≤ 2,5
Входное напряжение, В	12
Квантовая эффективность, %	5–20
Вероятность «послеимпульса», %	< 1
Время выхода в рабочий режим, с	≤ 60
Напряжение выходного импульса	LVTTL
Длительность выходного импульса, нс	80
Временное разрешение детектора, пс	≤ 1200
Взаимодействие с ПК	USB
Масса, кг	0,35 ± 0,1

Ключевые особенности:

- Низкий уровень темновых отсчетов
- Настраиваемые параметры задержек и мертвого времени
- Возможно изменение характеристик продукта по требованию заказчика
- Тип детектора: полупроводниковый, InGaAs/InP
- Длина волны: 900–1600 нм

QChaos

QRATE

Квантовый генератор случайных чисел

Принцип работы квантового генератора случайных чисел (КГСЧ) основан на интерференции лазерных импульсов со случайной фазой

При работе устройства преобразовываются флуктуации фазы лазера в амплитудные флуктуации

Уровень готовности технологии: 9

Технические характеристики:

Параметр	Параметр
Основные ТТХ	
Скорость генерации, Мбит/сек	до 300
Скорость выдачи энтропии, Гбит/сек	до 1
Тесты на случайность энтропии	
NIST SP 800-22	+
Интерфейсы	
Сетевой интерфейс	Gigabit Ethernet
Разъем подключения к устройству	RJ-45
Программная часть	
Операционная система	Linux
Command Line Interface (SSH)	+
Возможность кастомизации API по запросу	+

Варианты применения КГСЧ:

Генерация уникальных идентификаторо

Случайные числа используются для генерации уникальных идентификаторов (например, IMSI в мобильных сетях, session ID в веб-приложениях).

Тестирование и калибровка оборудования

Случайные числа используются для калибровки и тестирования оборудования (например, генерации тестовых сигналов).

Моделирование и тестирование сетей

Случайные числа используются для моделирования сетевого трафика, генерации тестовых данных и симуляции различных сценариев (например, атак, перегрузок сети).При тестировании QoS (Quality of Service) случайные числа помогают имитировать случайные задержки и потери пакетов.

Оптимизация использования ресурсов сети

Случайные числа используются в алгоритмах распределения каналов связи, частот или временных слотов в беспроводных сетях (Wi-Fi, LTE, 5G). Пример: В протоколах случайного доступа (Random Access Channel, RACH) в LTE/5G случайные числа помогают избежать коллизий при подключении устройств к базовой станции.

Генерация одноразовых паролей (OTP), токенов и nonce-значений (число, используемое один раз) в протоколах аутентификации (5G Authentication and Key Agreement).

PQC SDK

QApp

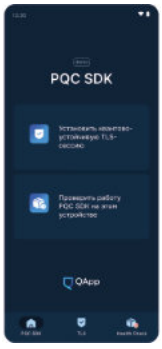
Инструмент разработки постквантовых решений

Программный инструментарий разработчика квантово-устойчивых решений на основе постквантовых алгоритмов.

Состоит из нескольких модулей:

- библиотека постквантовых алгоритмов отечественной реализации;
- средства, упрощающие интеграцию постквантовых алгоритмов в конечные решения заказчика.

https://qapp.tech/products/pqc_sdk



Решение пилотируется:

ГАЗПРОМБАНК

cTerra

МЦСТ ЭЛЬБРУС

НСПК

web3 tech

Сфера применения:

- Пользовательские данные
- Внутренние и внешние коммуникации
- Аутентификация
- Электронный документооборот
- Разработка новых квантово-устойчивых решений

Характеристики:

Количество постквантовых алгоритмов: **7**

- из них отечественных алгоритмов-кандидатов на включение в новые госстандарты: 1 (квантово-устойчивый алгоритм ЭЦП «Гиперикум»)

Отрасли применения и состав продукта:

- Информационные технологии
- Финансы, страхование
- Связь
- Здравоохранение
- Промышленность
- Транспорт
- Прочие отрасли, где применяются информационно-вычислительная техника, технологии IoT, блокчейн

УГТ: 7

Статус: пилотируется в ограниченных периметрах информационных систем

Стек технологий:

C, C++, Java, Kotlin, ES6, WASM, Python, Bash, Perl

Поддержка протоколов:

- OpenVPN
- TLS v1.2
- TLS v1.3

Поддержка платформ:

- Windows
- Linux
- Android v14

Поддержка архитектур:

- x86-64
- ARMv8
- E2k

Доказана совместимость с отечественными процессорами:
Эльбрус-8С и Байкал-М

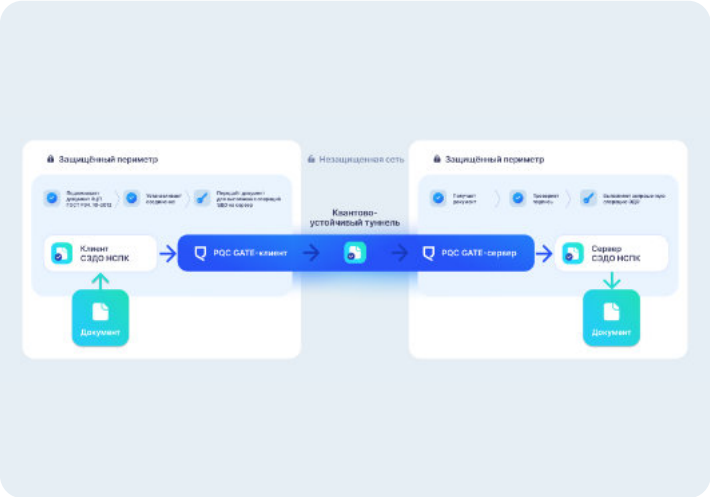
PQC GATE

QApp

Программное обеспечение для реализации квантово-устойчивых соединений в сетях различных топологий

Клиент-серверное решение, обеспечивающее квантово-устойчивый канал передачи данных во внутреннем и внешнем контуре в рамках инфраструктуры бизнеса.

https://qapp.tech/products/pqc_gate



Пример пилотной интеграции решения в ограниченном периметре информационной системы НСПК

Решение пилотируется:

ГАЗПРОМБАНК НСПК

c•терра MOEX GROUP

Сфера применения:

- Пользовательские данные
- Финансовые транзакции
- Внутренние и внешние коммуникации
- Электронный документооборот

Отрасли применения и состав продукта:

- Финансы, страхование
- Здравоохранение
- Промышленность
- Связь
- Информационные технологии
- Прочие отрасли, где применяются информационно-вычислительная техника, технологии IoT, ИИ, блокчейн

Состав продукта:

- Компонент PQC gate server
- Компонент PQC gate client
- Браузерное расширение PQC gate extension

Стек технологий:

C, C++, GO, ES6, WebExtensions API, Javascript

Поддержка протоколов и сертификатов:

- TLS v1.2
- TLS v1.3
- x.509

Поддержка платформ:

- Windows
- Linux

Поддержка архитектур:

- x86-64
- ARMv8

УГТ: 6

Статус: пилотируется в ограниченных периметрах информационных систем

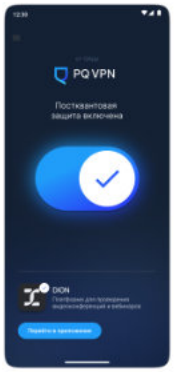
PQ VPN

QApp

Программное обеспечение для реализации квантово-устойчивых виртуальных частных сетей

Комплексная квантово-устойчивая защита трафика приложений — позволяет защищать различные виды трафика сетевого уровня и выше, путем его туннелирования с применением постквантовых алгоритмов.

https://qapp.tech/products/pq_vpn



Решение пилотируется:

T1

DION

Пример пилотной интеграции решения в ограниченном периметре информационной системы DION ИТ-холдинга T1

Сфера применения:

- Шифрование трафика на сетевом уровне с помощью ключа, получаемого на основе постквантовых алгоритмов распределения ключей
- Защита канала с применением как классических, так и постквантовых ЭЦП от атаки «человек посередине»
- Аутентификация доступа к виртуальной частной сети с применением классических и постквантовых ЭЦП

Отрасли применения и состав продукта:

- Финансы, страхование
- Здравоохранение
- Промышленность
- Связь
- Информационные технологии

Состав продукта:

- Серверная часть
- Клиентская часть

Стек технологий:

C, C++, Kotlin, Java

Поддержка протоколов:
OpenVPN, TLS v1.2, TLS v1.3

Поддержка платформ:

- Windows
- Linux (включая Astra Linux)
- Android v14

Поддержка архитектур:

- x86-64
- ARMv8

УГТ: 6

Статус: пилотируется в ограниченных периметрах информационных систем.

PQC PKI

QApp

Программное обеспечение для автоматизации целевых функций квантово-устойчивого Удостоверяющего Центра

Программное обеспечение, позволяющее автоматизировать основные операции, необходимые для функционирования удостоверяющего центра (УЦ) на основе постквантовых электронно-цифровых подписей (ЭЦП).

https://qapp.tech/products/pqc_pki

Решение пилотируется:

ГАЗПРОМБАНК

Сфера применения:

Автоматизация следующих процессов УЦ:

- Изготовление сертификатов открытых ключей для ЭЦП на основе постквантовых алгоритмов
- Управление сертификатами открытых ключей, в частности: аннулирование, приостановление, возобновление

Может использоваться для УЦ различного вида и назначения:

- Внутренний (корпоративный) и внешний (клиентский)
- Головной
- Облачный сервисный

Отрасли применения и состав продукта:

- Финансы, страхование
- Промышленность
- Связь
- Информационные технологии

Состав продукта:

- Серверная часть
- Клиентская часть

Стек технологий:

C, Bash

Поддержка протоколов и сертификатов:

- TLS v1.2
- TLS v1.3
- x.509

Поддержка платформ:
Linux

Поддержка архитектур:
x86-64

УГТ: 3

Статус: разработан прототип

Статус: пилотируется в ограниченных периметрах информационных систем.

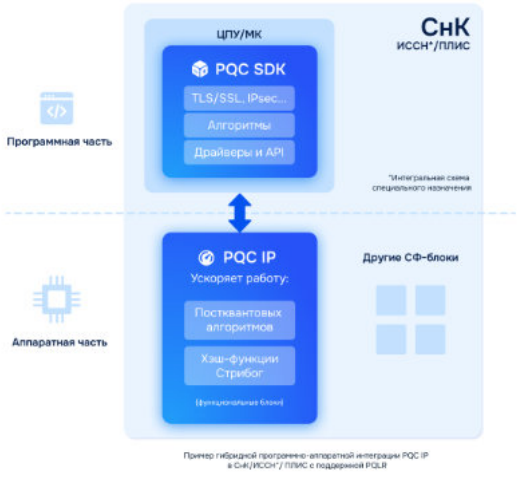
PQC IP

QApp

Библиотека сложно-функциональных блоков для аппаратного ускорения квантово-устойчивых и классических алгоритмов

Программно-аппаратная реализация библиотеки СФ-блоков (IP-ядер) для ускорения криптографических примитивов на малоресурсных системах. Совместима с ПО PQC SDK.

https://qapp.tech/products/pqc_ip



Сфера применения:

- Процессинг и клиринг финансовых транзакций (HSM модули)
- Встраиваемые устройства
- Смарт-карты
- Корни доверия систем доверенной загрузки
- Wi-Fi контроллеры
- Микроконтроллеры (для IoT, БПЛА)
- Микропроцессоры

Отрасли применения и состав продукта:

- Финансы
- Связь
- Промышленность (связанная с использованием и производством микроэлектроники)
- Прочие отрасли, где применяется информационно-вычислительная техника, технологии IoT

Состав продукта:

- Программная часть
- Аппаратная часть

Стек технологий:

Verilog, C, IP Core

Поддержка платформ:

- интегрируется в ОС на основе ядра Linux

Программная поддержка PQC IP реализована в ПО PQC SDK разработки ООО «КуАпп»

Варианты поставки в пилотные проекты: в составе ПО PQC SDK разработки ООО «КуАпп» и отдельно

УГТ: 3

Статус: разработан прототип

- реализован СФ-блок — хэш-функция, согласно ГОСТ Р 34.11-2012
- разработана программно-аппаратная модель для ускорения квантово-устойчивого алгоритма ЭЦП «Гиперикум» (алгоритм-кандидат на включение в новые госстандарты)

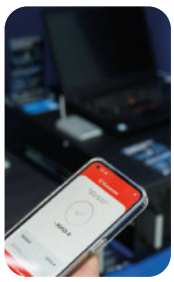
PQC PAY

QApp

Квантово-устойчивый программный продукт для платежной инфраструктуры

Сервис, позволяющий проводить бесконтактные платежи с поддержкой квантово-устойчивых алгоритмов шифрования с использованием технологии Bluetooth Low Energy (BLE). Полностью программное решение, работающее на стандартном смартфоне на стороне продавца и покупателя. Может быть интегрировано в уже существующие платежные сервисы, обеспечивая **квантово-устойчивые мобильные BLE-платежи.**

https://qapp.tech/products/pqc_pay



Решение пилотируется:

ГАЗПРОМБАНК

НСПК

Сфера применения:

Финансы

УГТ

УГТ: 5

Статус: пилотируется в ограниченных периметрах информационных систем.

Стек технологий:

Kotlin, Java

Поддержка протоколов:
OpenVPN

Поддержка платформ:
Android

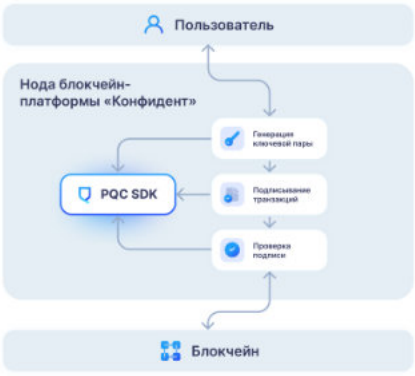
PQC CHAIN

QApp

Квантово-устойчивый блокчейн

Квантово-устойчивая версия блокчейн-платформы для построения государственных и корпоративных информационных систем, требующих распределенную и доверенную инфраструктуру.

https://qapp.tech/cases/web3_tech



Пример пилотной интеграции решения в ограниченном периметре квантово-устойчивой версии блокчейн-платформы «Конфидент»

Технологический партнер:

web3 tech

Сфера применения:

Постквантовая криптография используется в составе партнерской блокчейн-платформы для:

- Генерации ключевых пар
- Хэширования
- Генерации электронной подписи
- Проверки электронной подписи

Отрасли применения и состав продукта:

- Финансы, страхование
- Информационные технологии
- Логистика
- Государственное управление
- Прочие отрасли, где применяется технология блокчейн

Стек технологий:

Поддержка платформ:
- Windows
- Linux

Поддержка архитектур:
x86-64

Решение основано на:
- ПО PQC SDK разработки ООО «КуАпп»
- Блокчейн-платформа «Конфидент» разработки ООО «Веб3 Технологии»

УГТ: 5

Статус:
- разработан прототип
- решение готово к пилотированию в ограниченных периметрах информационных систем

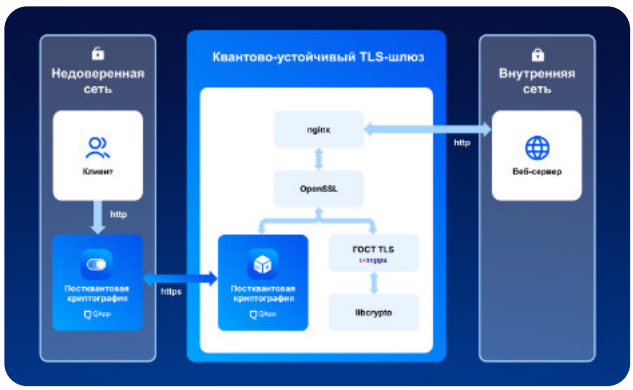
PQ TLS

QApp

Квантово-устойчивый TLS-шлюз

Программно-аппаратный комплекс, защищающий проходящий по открытой сети трафик путем его шифрования, в основу которого входят как классические алгоритмы, так и постквантовые. Обеспечивает многоступенчатую защиту сети любого масштаба и вида с различным количеством туннелей.

https://qapp.tech/cases/s-terra-tls



Технологический партнер:

с•терра®

Сфера применения:

Продукт обеспечивает квантово-устойчивую защиту (шифрование и имитозащита, аутентификация) данных, передаваемых по открытым каналам Интернета между клиентами и корпоративными сетями:

- Веб-порталы
- Корпоративные приложения
- Сервера

Прочие функции:

- Гранулированный доступ
- Управление параметрами доступа к защищаемым ресурсам
- Управление уровнями протоколирования событий

Отрасли применения и состав продукта:

Актуально для секторов экономики, где происходит одно- или двусторонняя передача конфиденциальной информации по открытым каналам связи.

Состав продукта:

- серверная часть
- клиентская часть

УГТ: 6

Статус:

- Разработан прототип продукта.
- Подтверждены рабочие характеристики в условиях, приближенных к реальным.
- Решение готово к пилотированию в ограниченных периметрах информационных систем.

Стек технологий:

C, C++

Поддержка протоколов и сертификатов:

- TLS v1.2
- VRRP
- x.509

Поддержка платформ:

- Windows
- Linux

Поддержка архитектур:

x86-64

Решение основано на:

ПО PQC SDK и ПО PQC GATE разработки ООО «КуАпп»
ПАК TLS-шлюз разработки ООО «С-Терра СиЭсПи».

PQCompute

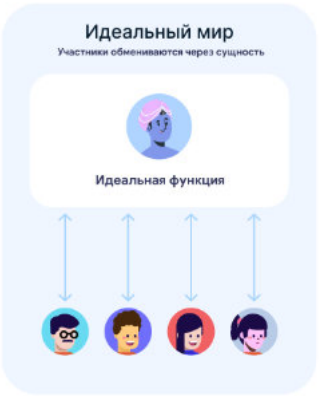
QApp

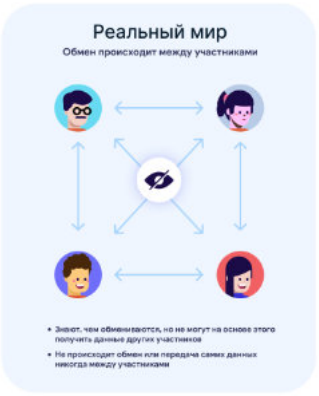
Программное ядро вычислительной системы для выполнения многосторонних конфиденциальных вычислений

Прототип ядра системы конфиденциальных вычислений, основанный на технологии Secure Multi-Party Computation (SMPC), для решения широкого спектра бизнес-задач. Протокол конфиденциального вычисления SMPC — это криптографический протокол, который распределяет вычисления между несколькими сторонами, при этом ни одна из сторон не может видеть данные других сторон.

Свидетельство о государственной регистрации программы для ЭВМ № 2024611073

https://qapp.tech/products/multi_party_computation





Решение пилотируется:

ГАЗПРОМБАНК

Сфера применения:

Технология «конфиденциальные вычисления» подходит для разных задач, где есть 2 и более сторон, и необходимо произвести безопасные вычисления над данными.

Примеры:

- Статистика с сохранением конфиденциальности
- Распределенные вычисления
- Электронное голосование

Отрасли применения и состав продукта:

- Финансы, страхование
- Информационные технологии
- Здравоохранение
- Торговля
- Логистика

Стек технологий:

C++, Python, ML

Поддержка платформ:
Linux

Поддержка архитектур:
x86-64

УГТ: 6

Статус: пилотируется в ограниченных периметрах информационных систем.

PQ EDU

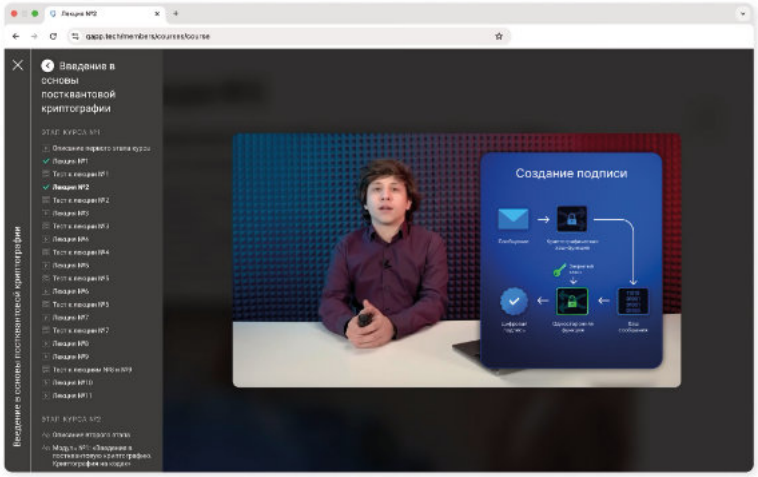
QApp

Теория и практика по квантово-устойчивой криптографии

Видеокурс с практическими задачами и материалами для самостоятельного обучения.

Задача курса — сформировать общее понимание о криптографии, квантовой угрозе, постквантовых алгоритмах, их актуальности и месте в современной индустрии информационной безопасности.

https://qapp.tech/products/pq_edu



Параметры курса

Формат обучения: онлайн

Курс состоит из двух этапов:

Первый этап:

Общая продолжительность лекций — 1 час 75 минут

Продолжительность одной лекции — от 3 до 7 минут

Тестовые задания: 60 минут

Второй этап:

Общая продолжительность лекций — 15 часов

Продолжительность одной лекций — от 15 до 45 минут

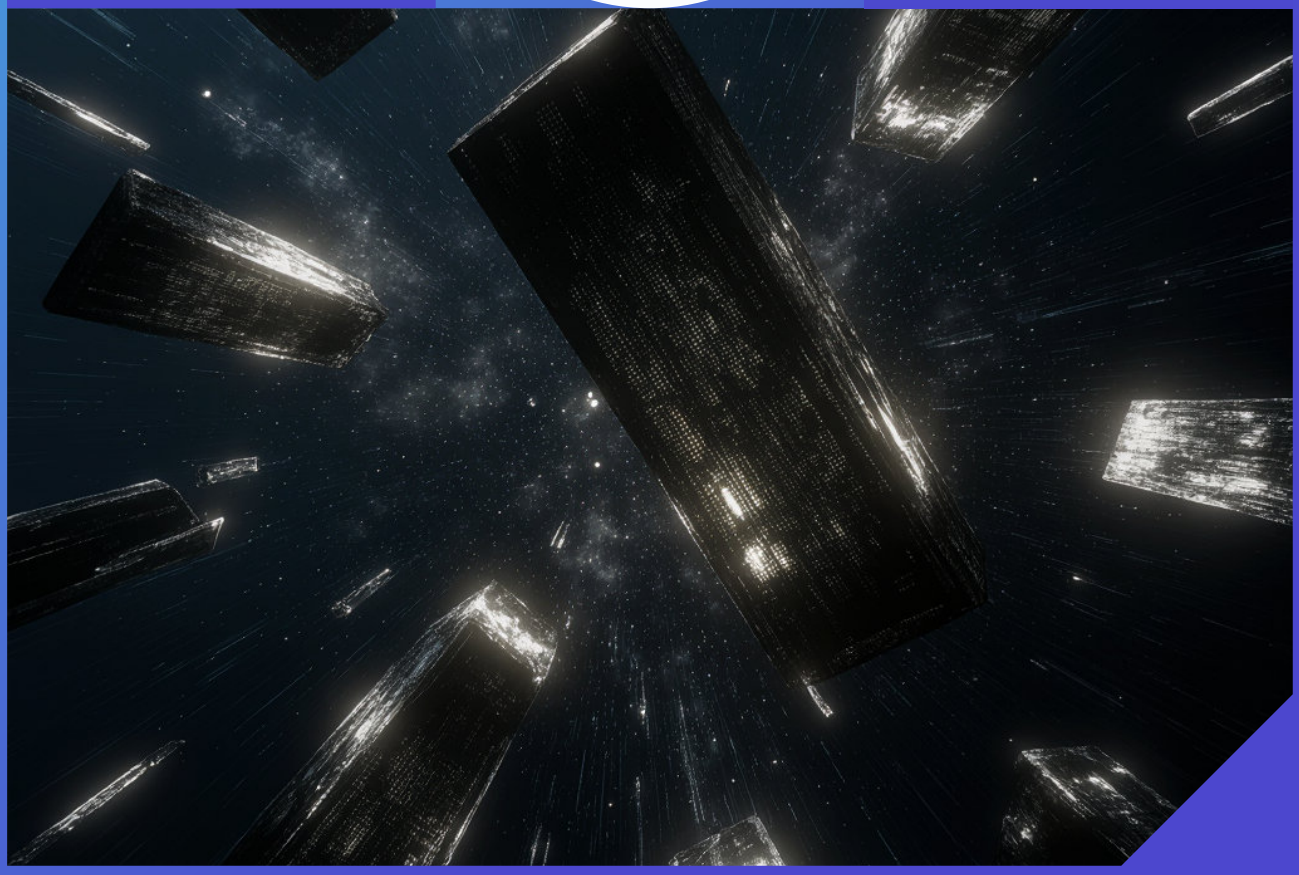
Лабораторные работы: 30 часов

Самостоятельное изучение: 205 часов

Программа первого этапа: 11 лекций

- Что такое криптография и зачем она нужна?
- Конфиденциальность сообщений. Блочные и поточные шифры
- Целостность и аутентификация сообщений. Криптографическая хэш-функция и MAC
- Выработка общего ключа для симметричной криптографии. Введение в асимметричную криптографию
- Электронно-цифровая подпись: еще один способ аутентификации сообщений
- Сертификаты открытых ключей. Протокол TLS
- Стойкость криптографического алгоритма. Основы криптоанализа
- Квантовый компьютер
- Квантовая угроза
- Постквантовая криптография
- Ознакомление с работой программного обеспечения, основанного на постквантовой криптографии, на примере продуктовой матрицы ООО «КуАпп»

Качественные эффекты внедрения квантовых и смежных технологий в сфере ИБ



Описание влияния квантовых и смежных технологий на трансформацию систем ИБ в компаниях и госструктурах

Внедрение квантовых и смежных технологий оказывает комплексное влияние на системы ИБ в компаниях и государственных структурах. Эти технологии не только создают принципиально новые подходы к обеспечению конфиденциальности и целостности данных, но и трансформируют архитектуру защиты, процессы управления ключами и эксплуатации инфраструктуры. Появляются специализированные элементы квантовых сетей, меняется состав и номенклатура средств защиты, возрастает роль автоматизации и снижается зависимость от традиционных криптографических механизмов. Одновременно усиливается потребность в высококвалифицированных кадрах на стыке физики, инженерии и ИБ, а также формируется новая модель взаимодействия бизнеса, государства и образовательных учреждений для масштабирования практических компетенций[1].

1. Архитектурные изменения

- Использование квантовых технологий приводит к созданию инфраструктуры квантовых сетей, которые делятся на различные сегменты: региональный сегмент, магистральный сегмент и корпоративный.
- Эти сегменты объединяются с существующей инфраструктурой, формируя новую криптографическую и транспортную основу ИБ.
- Для конечных пользователей изменения минимальны в интерфейсах, но значимы в архитектуре и процессах эксплуатации.

2. Оптимизация инфраструктуры и систем

- При гарантированной стойкости каналов (квантовое распределение ключей) возникает снижение номенклатуры и количества средств защиты:
  - Отпадает необходимость ставить ряд традиционных систем (например, фильтрующие компоненты, СМ-средства).
- Происходит оптимизация штатной численности обслуживающего ИБ-персонала.
- Системы становятся более однородными по архитектуре.

3. Изменения в кадрах и компетенциях

- Возникает нехватка специалистов с новыми компетенциями:
  - Квантовые инженеры
  - Специалисты по оптоэлектронике, фотонике
  - Инженеры, способные работать с аппаратными квантовыми системами
- Потребность в кадрах вызывает масштабирование обучения:
  - Курсы повышения квалификации, программы профпереподготовки
  - Стажировки в компаниях
  - Создание УМО[2] по квантовой инженерии
- Вовлечение специалистов происходит преимущественно через реальные проекты, пилоты, практическую эксплуатацию, обучение на реальных кейсах.

4. Процессные изменения

- Меняется жизненный цикл управления ключами:
  - Внедряются квантовые генераторы случайных чисел и квантовое распределение ключей с автоматической ротацией по квантовым сетям.
- Появляются новые роли или специалисты ИБ с расширенными компетенциями:
  - Эксплуатанты квантовых систем
  - Специалисты по мониторингу квантовых каналов
  - Операторы пуско-наладки квантового оборудования
- Увеличение уровня автоматизации и уменьшение влияния человеческого фактора.

[1] Консолидированная позиция экспертного сообщества Центра технологического лидерства при АНО «Цифровая экономика» в рамках проведенных экспертных сессий и глубинных интервью.
[2] Учебно-методическое объединение.

Ключевые эффекты стратегического уровня (для государства, бизнеса, граждан) и иные эффекты, которые могут быть достигнуты или уже достигнуты благодаря развитию квантовых технологий в ИБ

Ключевые стратегические эффекты:[1]

Для государства

- Защита критической инфраструктуры и обеспечение национальной безопасности
- Формирование сертифицированных решений, устойчивых к новым угрозам
- Генерация кумулятивных эффектов в экономике, технологическое лидерство и укрепление конкурентных позиций
- Внедрение квантовой спутниковой связи, иных перспективных каналов квантовых связи для повышения уровня доверия и безопасности передачи данных
- Развитие собственной компонентной базы
- Рост налоговой базы

Для бизнеса

- Усиление безопасности критичных систем, включая банковский сектор
- Обеспечение доступности квантовой защиты через модель сервиса
- Снижение совокупных издержек и стоимости сопровождения криптографии и страхования киберрисков
- Расширение возможностей новых рынков и развитие услуг
- Защита информации и устойчивость к квантовой угрозе
- Упрощение аттестации и повышение доверия к продукции

Для граждан

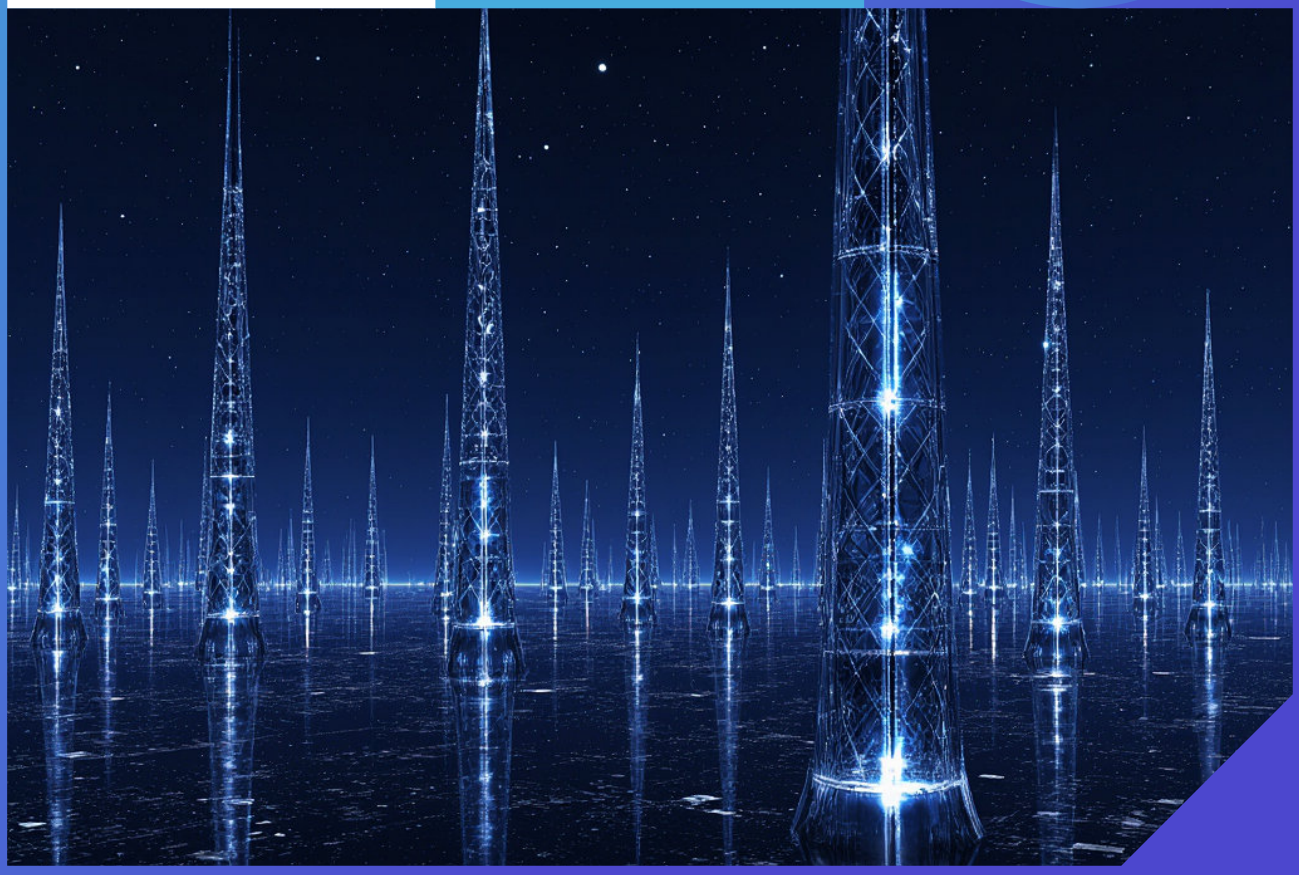
- Усиление защиты персональных данных
- Повышение доверия к цифровой инфраструктуре и сервисам
- Безопасность цифровых сервисов, электронных подписей, финансовых операций и защищенные транзакции
- Исключение человеческого фактора

Иные эффекты

- Повышение престижности вузов и конкурентоспособности специалистов
- Формирование новых рынков и развитие смежных отраслей
- Создание основы для технологического лидерства
- Рост доверия к инфраструктуре и укрепление имиджа государства и бизнеса как новаторов

[1] Консолидированная позиция экспертного сообщества Центра технологического лидерства при АНО «Цифровая экономика» в рамках проведенных экспертных сессий и глубинных интервью.

Рекомендации по развитию квантовых и смежных технологий в сфере ИБ



Описание барьеров при внедрении квантовых технологий в ИБ и рекомендации по преодолению барьеров

Наименование барьера	Описание барьера	Для кого актуален барьер	Критичность барьера[1]	Сложность преодоления барьера[2]	Приоритет работы с барьером[3]	Рекомендации по преодолению барьера[4]
Высокая стоимость оборудования	Высокая стоимость решений на базе квантовых технологий в ИБ	• Для потребителей	●	●	1	**(а)** Субсидирование со стороны государства приобретения решений на базе квантовых технологий в ИБ (в т. ч. с привлечением кредитных средств) **(б)** Принятие мер, направленных на увеличение спроса на решения на базе квантовых технологий в ИБ (увеличение спроса повлечет за собой увеличение объема выпуска и снижение стоимости продукции) **(в)** Применение решений на базе квантовых технологий в ИБ на критично значимых участках сети, на остальных же участках — применение постквантовой криптографии и классических ИБ-решений
Малый спрос	Малый спрос на решения на базе квантовых технологий в ИБ, который, в свою очередь, затрудняет увеличение объема выпуска и снижение стоимости продукции разработчиками	• Для разработчиков решений	●	●	2	**(а)** Закрепление в федеральных нормативных документах требований/рекомендаций о наличии в организациях решений на базе квантовых технологий в ИБ[5] **(б)** Субсидирование со стороны государства приобретения отечественных решений на базе квантовых технологий в ИБ **(в)** Обеспечение государственного заказа **(г)** Программы по ознакомлению потребителей с преимуществами внедрения квантовых технологий в ИБ (в т. ч. через пилотные проекты на испытательных полигонах, субсидирование со стороны государства аренды оборудования и др.), рекомендации по внедрению в той или иной отрасли/сфере в конкретные бизнес-процессы

[1] Чем больше заливка шара, тем выше критичность барьера.
[2] Чем больше заливка шара, тем выше сложность преодоления барьера.
[3] Чем выше критичность барьера и выше сложность преодоления барьера, тем выше приоритет работы с барьером (по его преодолению).
[4] Рекомендации перечислены в порядке убывания важности.
[5] В первую очередь установить обязательность для государственных организаций и компаний, что послужит положительным примером для других потребителей.

Описание барьеров при внедрении квантовых технологий в ИБ и рекомендации по преодолению барьеров

Наименование барьера	Описание барьера	Для кого актуален барьер	Критичность барьера[1]	Сложность преодоления барьера[2]	Приоритет работы с барьером[3]	Рекомендации по преодолению барьера[4]
Высокая стоимость инфраструктуры	Высокая стоимость строительства инфраструктуры, необходимой для функционирования решений на базе квантовых технологий в ИБ	• Для операторов • Для потребителей			3	**(а)** Меры поддержки со стороны государства (субсидирование, льготное налогообложение и др.) **(б)** Государственно-частное партнерство **(в)** Разработка решений, для функционирования которых может использоваться уже существующая инфраструктура
Неактуальность стандартов	Отсутствие достаточного количества актуальных национальных стандартов (ГОСТ Р, ПНСТ), а также предшествующих им документов (методических рекомендаций, рекомендаций по стандартизации) в сфере квантовых и смежных технологий в ИБ	• Для разработчиков решений • Для операторов • Для потребителей			4	**(а)** Определение потребностей в стандартах, разработка новых/модернизация текущих соответствующих стандартов и предшествующим им документов (с привлечением всех заинтересованных сторон, а также с учетом зарубежного опыта)

[1] Чем больше заливка шара, тем выше критичность барьера.
[2] Чем больше заливка шара, тем выше сложность преодоления барьера.
[3] Чем выше критичность барьера и выше сложность преодоления барьера, тем выше приоритет работы с барьером (по его преодолению).
[4] Рекомендации перечислены в порядке убывания важности.

Описание барьеров при внедрении квантовых технологий в ИБ и рекомендации по преодолению барьеров

Наименование барьера	Описание барьера	Для кого актуален барьер	Критичность барьера[1]	Сложность преодоления барьера[2]	Приоритет работы с барьером[3]	Рекомендации по преодолению барьера[4]
Несовместимость оборудования	Несовместимость оборудования различных разработчиков (вследствие применения разработчиками различных протоколов обмена данными)	• Для операторов • Для потребителей			5	**(а)** Стимулирование разработки и перехода на единые протоколы обмена данными **(б)** Субсидирование приобретения и внедрения технических решений, позволяющих преодолеть данный барьер
Отсутствие стратегического планирования	Отсутствие у компаний долгосрочного стратегического планирования для обеспечения собственного технологического развития	• Для потребителей			6	**(а)** Разработка и реализация стратегий технологического развития, трансформации (в т. ч. включающие внедрение квантовых технологий)
Сложность интеграции	Сложности при интеграции решений на базе квантовых технологий в текущие бизнес-процессы и системы ИБ	• Для потребителей • Для операторов			7	**(а)** Распространение успешного опыта интеграции среди всех заинтересованных участников (проведение образовательных мероприятий, подготовка и распространение рекомендаций и др.)

[1] Чем больше заливка шара, тем выше критичность барьера.
[2] Чем больше заливка шара, тем выше сложность преодоления барьера.
[3] Чем выше критичность барьера и выше сложность преодоления барьера, тем выше приоритет работы с барьером (по его преодолению).
[4] Рекомендации перечислены в порядке убывания важности.

Описание барьеров при внедрении квантовых технологий в ИБ и рекомендации по преодолению барьеров

Наименование барьера	Описание барьера	Для кого актуален барьер	Критичность барьера[1]	Сложность преодоления барьера[2]	Приоритет работы с барьером[3]	Рекомендации по преодолению барьера[4]
Дефицит специалистов	Нехватка специалистов с высшим и средним профессиональным образованием, в т. ч. с междисциплинарными компетенциями	• Для потребителей • Для разработчиков решений • Для операторов			8	**(а)** Запуск новых образовательных программ в высших и средне профессиональных учебных заведениях, как в государственных, так и в частных (при государственной поддержке) **(б)** Увеличение количества бюджетных мест по уже запущенным соответствующим образовательным программам **(в)** Переподготовка работающих специалистов смежных (с квантовыми технологиями, ИБ) специальностей **(г)** Изменение действующих образовательных программ для студентов (наполнение новыми соответствующими дисциплинами) **(д)** Увеличение количества интенсивных открытых образовательных мероприятий: хакатонов, семинаров
Отсутствие сертификации у части решений	Потребители не готовы приобретать и внедрять решения на базе квантовых технологий в ИБ, которые не прошли сертификацию регулирующих органов	• Для потребителей • Для разработчиков решений			9	**(а)** Принятие новых стандартов, которые согласованы регулятором (позволит ускорить прохождение сертификации решений разработчиков) **(б)** Содействие прохождению сертификации решений разработчиков на базе уже принятых нормативных документов

[1] Чем больше заливка шара, тем выше критичность барьера.
[2] Чем больше заливка шара, тем выше сложность преодоления барьера.
[3] Чем выше критичность барьера и выше сложность преодоления барьера, тем выше приоритет работы с барьером (по его преодолению).
[4] Рекомендации перечислены в порядке убывания важности.

Экосистема развития квантовых и смежных технологий

Экосистема развития квантовых технологий

Президиум Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (ГРИГОРЕНКО Д. Ю.)

Федеральные органы исполнительной власти

ФСБ России – регулирование и контроль

ФСТЭК России – нормативно методическое обеспечение и контроль

Минцифры – координация и верификация

Минэкономразвития – общая методология

Минобрнауки – государственная политика в сфере высшего образования

Минфин – ФЭО и финансирование

ГК «Росатом»
ответственная корпорация за развитие технологии квантовых вычислений

ООО «СП «КВАНТ»
Проектный офис, оператор ДК «Квантовые вычисления» и заказчик НИОКР

Научный совет РАН «Квантовые технологии»

Научная экспертиза

Проектный офис Правительства РФ (АНО «Цифровая экономика», Аналитический центр, ФГБУ ЦЭКИ)

- Комплексная оценка реализации
- Бизнес и экономическая экспертиза

ОАО «РЖД»
Ответственная государственная компания за развитие квантовых технологий и реализации ДК «Квантовые коммуникации»

Отраслевые научно-технические комитеты

Научная экспертиза

Государство

Институты развития

Научная и отраслевая экспертиза

Исследовательские центры

Вендоры/разработчики и интеграторы

Консорциумы

Участники экосистемы развития квантовых технологий: Федеральные органы исполнительной власти

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

минцифры_

Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, электросвязи и почтовой связи, массовых коммуникаций и средств массовой информации, в том числе электронных, печати, издательской и полиграфической деятельности, обработки персональных данных, управления государственным имуществом и оказания государственных услуг в области информационных технологий.

Министерство экономического развития Российской Федерации

Министерство экономического развития Российской Федерации

Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации экономической политики Правительства России по ряду направлений, в том числе осуществляющий координацию развития высокотехнологичных направлений в России.

Министерство науки и высшего образования Российской Федерации

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный орган исполнительной власти России, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере высшего образования и соответствующего дополнительного профессионального образования, а также научной, научно-технической и инновационной деятельности и по развитию федеральных центров науки и высоких технологий.

Министерство финансов Российской Федерации

Минфин России

Министерство финансов России занимается разработкой правовой базы в сфере финансов, анализирует и прогнозирует экономическое развитие, совершенствует бюджетную систему и готовит предложения по изменению денежно-кредитной политики. В части развития технологий Минфин России занимается разработкой и согласованием финансово-экономических обоснований и объемов бюджетных инвестиций, направляемых на развитие высокотехнологичных областей, в том числе квантовых технологий.

Участники экосистемы развития квантовых технологий: организации, осуществляющие реализацию государственных программ развития квантовых технологий

Госкорпорация «Росатом»

Многопрофильный холдинг, объединяющий активы в энергетике, машиностроении, цифровой сфере. ГК «Росатом» — ответственная организация в России за развитие высокотехнологичной области «Квантовые вычисления». Соответствующее соглашение было подписано между Правительством РФ и руководством корпорации в 2019 году. Основным механизмом реализации соглашения является дорожная карта, утвержденная в 2020 году. В целях обеспечения выполнения основных задач, целевых показателей, индикаторов и мероприятий дорожной карты создано ООО «СП «Квант» — оператор дорожной карты, единый центр компетенций и проектный офис по направлению «Квантовые вычисления» в структуре корпорации.

Открытое акционерное общество «Российские железные дороги»

ОАО «РЖД» — владелец инфраструктуры общего пользования и крупнейший перевозчик российской сети железных дорог. Компания курирует программу по развитию высокотехнологичной области квантовых коммуникаций в России. Соответствующее соглашение было подписано между Правительством РФ и руководством компании в 2019 году. Его цель — достижение Российской Федерацией лидерских позиций на глобальных технологических рынках в области квантовых коммуникаций. Дорожная карта «Квантовые коммуникации» была разработана и утверждена в 2020 году. Основной целью дорожной карты и результатом работы в ее рамках должен стать выход России на лидирующие позиции в мире по технологиям, продуктам и сервисам в области квантовых коммуникаций.

Российская академия наук

Государственная академия наук Российской Федерации, крупнейший в стране центр фундаментальных исследований. Основной целью деятельности является организация и проведение фундаментальных и прикладных научных исследований по проблемам естественных, технических, гуманитарных и общественных наук. Научно-технический совет РАН «Квантовые технологии» осуществляет координацию и комплексную экспертизу исследований в области квантовых технологий, выполняемых за счет средств федерального бюджета научными организациями и образовательными учреждениями ВПО.

Автономная некоммерческая организация «Цифровая экономика»

АНО «Цифровая экономика» — главная платформа взаимодействия бизнеса и государства по развитию цифровой экономики в России. Деятельность АНО «Цифровая экономика» сфокусирована на направлениях, отвечающих текущим задачам развития высокотехнологичных секторов экономики РФ. Сегодня АНО «Цифровая экономика» — это аналитика и исследования, экосистема поддержки бизнеса, кадровое обеспечение, продвижение технологий и решений, устранение проблем применимости цифровых технологий, национальная платформа поддержки цифровой трансформации.

Участники экосистемы развития квантовых технологий: вендоры/разработчики и интеграторы

ООО «ВЕБ3 ТЕХНОЛОГИИ»

Компания Web3 Tech (ООО «Веб3 Технологии») — ведущий разработчик в сфере блокчейн-технологий и продуктов в России и СНГ, создатель блокчейн-платформы «Конфидент», включенной в реестр российского ПО. На основе их технологий реализованы проекты для крупнейших частных и государственных компаний в различных отраслях — национальная система дистанционного электронного голосования, блокчейн-платформа ФНС, финтех-сервисы и другие решения, требующие распределенную и доверенную инфраструктуру.

ООО «КуАпп»

Российская компания — разработчик программных решений информационной безопасности на основе квантово-устойчивых (постквантовых) алгоритмов шифрования. Ключевая экспертиза компании: постквантовые технологии и технологии конфиденциальных вычислений. Компания «КуАпп» активно участвует в процессе разработки государственных стандартов по постквантовым алгоритмам шифрования. Также компания занимается прикладными научными исследованиями и пилотированием программных решений в сфере кибербезопасности. Компания «КуАпп» является участником Сколково, МИК и Нижегородского НОЦ. Результаты работы удостоены высших наград всероссийских конкурсов по направлению кибербезопасности.

ООО «КуРэйт»

Компания развивает и внедряет технологии квантового шифрования в инфраструктуры крупнейших российских организаций. Инновационность решений базируется на фундаментальных законах физики. ООО «КуРэйт» уже сегодня создает инструменты, способные противостоять новым типам атак на критическую инфраструктуру и данные. Компания — резидент «Сколково» и член консорциума НТИ «Квантовые коммуникации», а также стратегический партнер НИТУ МИСИС. Компания является разработчиком и правообладателем программ для электронных вычислительных машин.

АО «Центр Исследований и Разработок»

АО «Центр Исследований и Разработок» — инновационный интегратор, специализирующийся на высокотехнологичных разработках и внедрении новых средств защиты информации, систем коммуникаций, обработки данных и оптимизации вычислений, сенсорики и метрологии, а также на управлении исследовательскими проектами и разработке профильных технологических стандартов для государственных регуляторов.

Участники экосистемы развития квантовых технологий: вендоры/разработчики и интеграторы

«Газпромбанк» (Акционерное общество)

«Газпромбанк» (Акционерное общество) входит в тройку лидеров банковской отрасли России по основным объемным показателям и обслуживает ключевые отрасли российской экономики. Газпромбанк поддерживает развитие квантовых и смежных технологий с 2014 года. Банк первым среди финансовых организаций протестировал средства квантовой криптографии для защиты каналов связи между дата-центрами, а также системно пилотирует программные решения на основе постквантовой криптографии в ограниченном периметре своих информационных систем. Газпромбанк является соучредителем Российского квантового центра.

ПАО «Ростелеком»

ПАО «Ростелеком» — крупнейший в России интегрированный провайдер цифровых услуг и решений, который присутствует во всех сегментах рынка и охватывает миллионы домохозяйств, государственных и частных организаций. Компания занимает лидирующие позиции на рынке услуг высокоскоростного доступа в интернет, мобильной связи и онлайн-кинотеатров. Компания — признанный технологический лидер в инновационных решениях для цифровых государственных сервисов, кибербезопасности, цифровизации регионов, здравоохранения, квантовых коммуникаций, ЖКХ, а также в сфере облачных вычислений и услуг дата-центров.

ПАО Сбербанк

Крупнейший банк страны. В Центре квантовых технологий «Сбера» разрабатываются системы для повышения производительности машинного обучения и ИИ, инструменты защиты от квантового взлома, независимая от GPS навигация. Центр также участвует в создании квантовых эмуляторов и компьютеров.

АО «Компания ТрансТелеКом»

АО «Компания ТрансТелеКом» — российская телекоммуникационная компания, входит в число крупнейших магистральных операторов связи. Основной акционер — ОАО «РЖД», владеет 99,99% акций компании. Компания является одним из основных поставщиков магистральных услуг связи для операторов и крупнейших корпораций России, а также одним из лидеров среди провайдеров услуг широкополосного доступа в интернет, телевидения и телефонии для конечных пользователей в регионах. Компания является интегратором в сфере предоставления услуг и сервисов квантовых коммуникаций.

Участники экосистемы развития квантовых технологий: вендоры/разработчики и интеграторы

АО «ИнфоТеКС»

АО «ИнфоТеКС» — ведущий российский разработчик программно-аппаратных VPN-решений и средств криптографической защиты информации.
АО «ИнфоТеКС» входит в пятерку крупнейших компаний России в сфере защиты информации. Среди продуктов компании: защита каналов связи и конечных устройств, защита систем промышленной автоматизации, инфраструктура открытых ключей, квантовые криптографические системы.

ООО «СМАРТС-Квантттелеком»

ООО «СМАРТС-Квантттелеком» является российским производителем систем квантового распределения ключей и компонентной базы квантовых технологий: детекторов одиночных фотонов, фазовых и амплитудных модуляторов. Компания обеспечивает комплексное проектирование квантовых сетей, реализует фундаментальные и прикладные научные исследования в сфере квантовых коммуникаций. Резидент фонда «Сколково» и ИНТЦ «Интеллектуальная электроника Валдай».

ООО «Системы практической безопасности»

ООО «Системы практической безопасности» занимается разработкой СКЗИ высокого класса на базе программно-аппаратных решений собственной разработки, разработкой программного обеспечения для защищенных систем различного назначения, производством СКЗИ, созданием защищенных сетей обмена данными на базе СКЗИ собственной разработки, внедрением и сопровождением эксплуатации СКЗИ и защищенных систем. В настоящее время компания «СПБ» выполняет исключительно своими силами весь комплекс научно-исследовательских и опытно-конструкторских работ в области создания СКЗИ и защищенных систем.

Научно-технологический университет «Сириус»

НТУ «Сириус» — это институциональный центр, формирующий молодых ученых, инженеров и технологических предпринимателей, обладающих широким спектром научных и социальных компетенций, способных создавать технологические решения.
Его миссия включает подготовку всесторонне развитых специалистов и тиражирование уникальных образовательных программ в партнерские вузы, содействие формированию экономической модели, создание окружения, стимулирующего научно-технологическую, образовательную, предпринимательскую и общественную деятельность в интересах страны. Основные направления — квантовая информатика и информационная безопасность, информационные технологии и ИИ, генетика и науки о жизни, когнитивные исследования, экология и изменение климата и др.

Участники экосистемы развития квантовых технологий: вендоры/разработчики и интеграторы

ООО «РусБИТех-Астра»

ООО «РусБИТех-Астра» — один из лидеров российского рынка информационных технологий в области разработки программного обеспечения (ПО) и средств защиты информации. Программные продукты «Группы Астра» используются во всех отраслях экономики: в ведущих энергетических и нефтегазовых компаниях, в организациях финансового сектора, а также в госкомпаниях и госкорпорациях, в медицине и образовании.

ООО «С-Квантум»

ООО «С-Квантум» — один из ведущих российских разработчиков квантовых эмуляторов и смежных программных решений. Цель компании — дать отечественной IT-индустрии инфраструктуру полной квантовой готовности. Для этого создаются инструменты гибридного и квантового машинного обучения.
В сочетании с уникальными реалистичными эмуляторами они позволяют достоверно оценить потенциал квантовых технологий для конкретных бизнес-задач. Понимание стратегии коммерциализации квантовых вычислений и возможность бесшовного перехода к их использованию через унифицированный с классическими инструментами программный интерфейс обеспечивает пользователям максимальный контроль на пути технологического развития.

ООО «КуБорд»

Миссия компании — сделать квантовые вычисления доступными для бизнеса. Квантовые вычисления стремительно развиваются во всем мире и в Российской Федерации. Квантовые компьютеры за счет новой схемотехники требуют новых подходов в программировании и компетенций. ООО «КуБорд» разработал и уже коммерциализовал «цифровые двойники» квантовых компьютеров (программные эмуляторы квантовых вычислений), облачный интерфейс доступа к ним и библиотеки отраслевых квантовых алгоритмов. Компания является участником Сколково, МИК и Нижегородского НОЦ.

ООО «КуСпэйс Технологии»

Компания — разработчик спутниковых и атмосферных систем квантового распределения ключей, в которых ключ распределяется через открытое пространство, что эффективно дополняет оптоволоконные квантовые сети. Стартап появился в научной группе по квантовым коммуникациям Российского квантового центра, затем выделился в отдельное направление из компании ООО «КуРэйт».

ООО «КуСпэйс Технологии» — единственная в России компания, которая фокусируется на создании спутниковых систем на базе малых космических аппаратов. Участник «Сколково».

Участники экосистемы развития квантовых технологий: исследовательские центры

Российская академия наук

Российская академия наук (РАН) проводит обширные исследования в области квантовых технологий. Большинство исследований в этих областях носят фундаментальный характер, закладывая основу для технологических решений. РАН также активно участвует в разработке прикладных квантовых технологий, часто в сотрудничестве с промышленными партнерами. РАН координирует исследования по квантовым технологиям, взаимодействует с профильными министерствами и ведомствами Российской Федерации для решения прикладных научно-технических задач в различных отраслях промышленности.

НИЦ «Курчатовский институт»

Курчатовский институт принимал активное участие в проектах развития российского интернета и электронных научных коммуникаций. В 2024 году Курчатовским институтом совместно с Объединенным институтом ядерных исследований (Дубна) и Институтом системного программирования РАН создан консорциум РДИГ-М для работы со сверхбольшими массивами научных данных, в частности получаемых на исследовательских мегаустановках. Сегодня в России действует созданная в 2019 году Национальная исследовательская компьютерная сеть нового поколения (НИКС), которую развивает Курчатовский институт. В рамках этого проекта в 2024 году по поручению Президента РФ создается МУКС — межуниверситетская квантовая сеть.

ООО «МЦКТ»

Российский квантовый центр — научно-исследовательская организация, ведущая разработки полного стека квантовых технологий, включая вычисления, коммуникации, криптографию и сенсоры. РКЦ является головным исполнителем национальной дорожной карты по развитию высокотехнологичной области «Квантовые вычисления». Центр обладает широкой экспертизой в области реализации консультационных, научно-исследовательских и опытно-конструкторских проектов по квантовым и смежным технологиям различного уровня сложности.

Московский государственный университет им. М. В. Ломоносова

Центр квантовых технологий МГУ имени М. В. Ломоносова создан в рамках Национальной технологической инициативы. Деятельность центра направлена на развитие научных направлений в сфере квантовых технологий, разработку соответствующих образовательных программ и создание связей с индустриальными партнерами для последующей коммерциализации разработок в области квантовых технологий. В рамках центра ведутся исследования в области волоконной и атмосферной квантовой криптографии, физики холодных атомов, квантовой оптики, нанофотоники и нелинейной оптики и криоэлектроники.

Участники экосистемы развития квантовых технологий: исследовательские центры

Университет науки и технологий МИСИС

Институт физики и квантовой инженерии МИСИС является структурным подразделением университета и готовит специалистов по квантовым технологиям. Ученые института ведут исследования в области квантовых вычислений, квантовых коммуникаций и квантовых сенсоров. Также в составе университета есть дизайн-центр квантового проектирования, деятельность которого направлена на проектирование элементов и систем квантовых процессоров и квантовых симуляторов на основе сверхпроводниковых кубитов, а также на достижение стратегической цели по созданию многокубитных схем как платформ для квантовых вычислений и симуляций.

Физический институт им. П. Н. Лебедева РАН

Российский физический институт им. П. Н. Лебедева (ФИАН) — старейший научно-исследовательский центр России, ровесник Российской академии наук, после учреждения которой физика получила в России полноправный статус самостоятельной науки. Широкая тематика исследований, охватывающих практически все направления физики, обусловила нынешнюю структуру ФИАН, включающую шесть научных отделений, приравненных в основных направлениях к научно-исследовательским институтам РАН. В ФИАН проводятся активные исследования в области создания передовых технологий квантовых вычислений.

Московский физико-технический институт

Один из ведущих российских вузов по подготовке специалистов в области теоретической, экспериментальной и прикладной физики, математики, информатики, химии, биологии и смежных дисциплин. Согласно большинству национальных и международных рейтингов, МФТИ входит в тройку лучших вузов России, занимая высокие позиции в области физики, математики, компьютерных и технических наук, биологии и электроники. Институт квантовых технологий МФТИ выполняет исследования полного цикла от поисковых научно- исследовательских работ до опытно-конструкторских работ по разработке технологий и оборудования. Для этого в институте создана необходимая научная инфраструктура.

Сколковский институт науки и технологий

Сколтех занимается развитием квантовых технологий через магистерскую программу «Фотоника и квантовые материалы», которая охватывает ключевые аспекты квантовых технологий, включая сверхпроводящие технологии и квантовую спектроскопию. Студенты программы получают теоретические знания и практические навыки в области квантовых систем, участвуя в исследовательских проектах, результаты которых часто публикуются в международных журналах. Сколтех также сотрудничает с промышленностью, что позволяет студентам работать над реальными проектами и развивать инновационные решения на стыке науки и бизнеса.

Участники экосистемы развития квантовых технологий: исследовательские центры

Новосибирский государственный университет

Новосибирский государственный университет
*НАСТОЯЩАЯ НАУКА

НГУ занимается исследованиями в области квантовых технологий, предлагая магистерскую программу по квантовым информационным технологиям, где студенты изучают квантовое программирование, криптографию и метрологию. В университете функционирует Лаборатория квантовых оптических технологий, которая разрабатывает новые источники излучения для различных приложений, включая медицину и экологию. НГУ также участвует в разработке новых лазерных систем и систем квантовой связи, что способствует внедрению инновационных решений в практику и подготовке специалистов для высокотехнологичной отрасли.

Национальный исследовательский ядерный университет «МИФИ»

МИФИ

Национальный исследовательский ядерный университет

МИФИ развивает квантовые технологии через программу бакалавриата «Квантовый инжиниринг», которая является первой в России, полностью ориентированной на подготовку специалистов в этой области. Программа охватывает широкий спектр дисциплин, включая квантовые вычисления, квантовую криптографию и прецизионные измерения, обеспечивая студентов практическими навыками работы с современным оборудованием. МИФИ также проводит олимпиаду «Квантовый вызов», направленную на выявление талантливых студентов и развитие их компетенций в области квантовых технологий. В университете активно ведутся исследования по созданию высокоточных квантовых сенсоров и систем обработки данных, что способствует подготовке кадров для быстро развивающегося рынка квантовых технологий в России.

Самарский университет им. академика С. П. Королева

САМАРСКИЙ УНИВЕРСИТЕТ

Университет активно развивает квантовые технологии, участвуя в создании межуниверситетской квантовой сети (МУКС), которая объединяет несколько ведущих российских университетов и научных центров. В рамках этого проекта университет запускает новую образовательную программу «Квантовые коммуникации и оптоэлектроника», направленную на подготовку специалистов в области квантовых технологий. Исследования университета охватывают широкий спектр тем, включая применение квантовых технологий в медицине и других отраслях.

Университет ИТМО

ИТМО

Университет ИТМО развивает квантовые технологии через создание специализированных лабораторий и программ, включая Лабораторию квантовых коммуникаций и Научно-образовательный центр фотоники и оптоинформатики. В университете проводятся исследования в области квантового распределения ключей, квантовых сетей и квантового имаджинга, а также разрабатываются прототипы систем для беспроводной передачи информации и квантовых сенсоров. ИТМО является одним из лидеров в создании многоузловых квантовых сетей в России, что способствует интеграции квантовых технологий в реальную инфраструктуру. Университет также предлагает образовательные программы по квантовым и нанофотонным системам, готовя специалистов для высокотехнологичной отрасли и активно сотрудничая с международными научными центрами.

Участники экосистемы развития квантовых технологий: исследовательские центры

Нижегородский государственный университет им. Н. И. Лобачевского

Университет участвует в развитии квантовых технологий, присоединившись к «Национальной квантовой лаборатории» и запустив новые научно-исследовательские лаборатории, включая Лабораторию материалов для квантовых технологий и Лабораторию перспективных квантовых стандартов частоты. В университете также реализуются образовательные программы по квантовым технологиям, направленные на подготовку специалистов в этой области. Исследования охватывают создание полупроводниковых квантовых кубитов и разработку квантовых вычислений, что позволяет университету вносить значительный вклад в российскую квантовую отрасль. Кроме того, университет активно вовлекает молодежь в квантовую науку через мероприятия, такие как «Квантовая неделя», что способствует популяризации знаний в этой перспективной области.

Санкт-Петербургский государственный университет

Университет занимается развитием квантовых технологий через организацию образовательных мероприятий и исследовательские проекты. В рамках экосистемного проекта «Квантовая неделя» университет проводит лекции, мастер-классы и практические занятия, направленные на популяризацию квантовых технологий среди школьников и студентов, а также на подготовку научных кадров в этой области. СПбГУ входит в консорциум «Национальная квантовая лаборатория» и сотрудничает с ГК «Росатом», что позволяет ему участвовать в реализации совместных проектов по развитию квантовых вычислений и технологий. Исследования университета охватывают широкий спектр тем, включая квантовую криптографию и создание новых квантовых устройств, что способствует внедрению инновационных решений в различные сферы науки и техники.

НИУ «Высшая школа экономики»

Высшая школа экономики активно развивает образовательные программы и проводит исследования в области квантовых технологий. Создан Учебный центр квантовых технологий как часть Департамента электронной инженерии. ВШЭ сотрудничает с ведущими российскими научными институтами, в частности с Институтом общей физики им. А. М. Прохорова РАН. Университет является одним из лидеров в области исследования квантовой физики, сотрудничает с научными и образовательными учреждениями для развития квантовых технологий.

Московский энергетический институт

Московский энергетический институт активно занимается исследованиями и разработками в области квантовых технологий, охватывая несколько ключевых направлений. В частности, институт исследует создание и применение квантовых компьютеров, разрабатывает квантовые алгоритмы и программные эмуляторы для решения сложных задач. МЭИ разрабатывает высокочувствительные квантовые сенсоры для точных измерений в медицине и биотехнологиях, а также технологии квантовой связи для обеспечения защищенной передачи информации на основе принципов квантовой механики.

Участники экосистемы развития квантовых технологий: исследовательские центры

Санкт-Петербургский государственный университет аэрокосмического приборостроения

ГУАП

ГУАП занимается исследованиями в области квантовой электроники и фотоники, разрабатывает новые материалы и компоненты, создает инновационные технологии для применения в электронике и оптике. Специалисты работают над созданием квантовых компьютеров, лазеров, оптических систем передачи информации и других устройств, применяемых в науке, промышленности и медицине.

Уральский федеральный университет

Уральский федеральный университет имени первого Президента России Б.Н.Ельцина

УрФУ занимается исследованиями в области квантовых технологий через свою кафедру Теоретической физики и прикладной математики. В рамках образовательной программы по прикладной математике и физике акцент делается на квантовые вычисления и машинное обучение. Исследования охватывают такие области, как квантовая криптография, материаловедение и ИИ, с акцентом на применение квантовых алгоритмов для решения сложных задач.

Казанский федеральный университет

Казанский федеральный университет

КФУ активно занимается исследованиями в области квантовых технологий, включая квантовые вычисления, квантовую оптику и квантовые коммуникации.
В университете функционирует Центр квантовых технологий, который фокусируется на разработке волноводных нелинейно-оптических методов получения квантовых состояний света и создании оптоволоконных квантовых сенсоров. Исследования охватывают такие направления, как генерация однофотонных состояний и квантовая микроспектроскопия, что способствует развитию новых приложений в области квантовых систем.

Университет Иннополис

УНИВЕРСИТЕТ ИННОПОЛИС

Университет Иннополис активно занимается исследованиями и разработками в области квантовых технологий. Основные направления деятельности включают создание доверенных квантовых компьютеров, разработку квантовых алгоритмов и протоколов безопасности, создание стандартов постквантовой криптографии, создание QUBO-решателей на основе машины Игинга и др. Кроме того, университет сотрудничает с различными компаниями и организациями для коммерциализации своих разработок и внедрения квантовых технологий в различные сферы жизни.

Участники экосистемы развития квантовых технологий: исследовательские центры

Томский государственный университет

ТГУ с 2018 года активно участвует в развитии квантовых технологий. Университет стал частью консорциума «Национальная квантовая лаборатория», что позволяет ему сосредоточиться на создании кубитов на основе NV-центров в алмазе и разработке квантовых вычислений. В ТГУ функционируют кафедры и лаборатории, занимающиеся квантовыми информационными технологиями, а также проводятся мероприятия, такие как «Неделя квантовых технологий», совместно с госкорпорацией «Росатом». Исследования охватывают широкий спектр тем, включая лазерную генерацию на NV центрах и создание оптоволоконных квантовых сенсоров, что способствует подготовке специалистов и внедрению новых технологий в практику.

Московский технический университет связи и информатики

МТУСИ активно развивает квантовые технологии через создание специализированного Квантового центра и реализацию образовательных программ в области квантовых коммуникаций. В университете проводятся лекции и семинары по основам квантовой информатики и алгоритмов, а также исследования в сфере квантового распределения ключей и беспроводной квантовой связи. МТУСИ сотрудничает с компанией ООО «КуРэйт» для внедрения практических курсов, где студенты изучают электромагнитные волны и интерференцию многофотонных состояний. Также университет работает над созданием межвузовской квантовой сети, что способствует подготовке специалистов в области квантовых технологий и их применению в реальных задачах.

Томский государственный университет систем управления и радиоэлектроники

Университет активно развивает квантовые технологии через создание образовательных программ и научных исследований. В 2024 году университет запустил новую магистерскую программу «Квантовые и оптические системы связи», направленную на подготовку специалистов в области проектирования систем, использующих оптоволокно и квантовые технологии для защиты данных. ТУСУР также сотрудничает с компанией АО «ИнфоТеКС» для создания межуниверситетской квантовой сети в Томске, что позволит реализовать научные и образовательные проекты в области квантовых коммуникаций. В рамках этого сотрудничества разработан учебный стенд по квантовой криптографии, который станет основой для подготовки кадров в области информационной безопасности и квантовых технологий.

Казанский научный центр РАН

КНЦ РАН активно занимается исследованиями в области квантовых технологий, сосредоточив внимание на квантовой оптике и спиновых технологиях. В центре проводятся фундаментальные и прикладные исследования, направленные на развитие технологий квантовой обработки информации, включая разработку квантовых цифровых подписей и систем опознавания на новых физических принципах. Также осуществляется интеграция с другими научными учреждениями для создания федеральных и международных квантовых сетей. Важным аспектом работы центра является подготовка кадров, включая студентов и молодых ученых, что способствует развитию научного потенциала в области квантовых технологий в регионе.

Участники экосистемы развития квантовых технологий: исследовательские центры

Математический институт им. В. А. Стеклова РАН

МИАН активно занимается исследованиями в области квантовых технологий через свой Отдел математических методов квантовых технологий, созданный в 2018 году. Основная цель отдела заключается в решении математических задач, связанных с квантовыми системами, включая квантовые вычисления, квантовую криптографию и квантовую метрологию. Исследования охватывают управление квантовыми системами и разработку новых методов для их применения, что соответствует современным требованиям и вызовам в области квантовых технологий. МИАН также проводит семинары и конференции, способствующие обмену знаниями и развитию научных кадров в этой перспективной области.

Институт радиотехники и электроники им. В. А. Котельникова РАН

ИРЭ занимается исследованиями в области квантовых технологий, включая квантовую электронику и спинтронные устройства. В институте проводятся фундаментальные исследования, направленные на разработку новых методов и технологий для квантовых систем, таких как квантовые вычисления и квантовая криптография. ИРЭ также разрабатывает современные микросхемы и устройства на основе фотоники, что позволяет создавать инновационные решения для передачи и обработки квантовой информации. Важным аспектом работы института является сотрудничество с промышленностью для внедрения научных разработок в практику, что способствует развитию высоких технологий в России.

Казанский национальный исследовательский технический университет им. А. Н. Туполева — КАИ

Университет активно развивает квантовые технологии через Казанский квантовый центр, где проводятся исследования в области квантовой памяти и квантовых коммуникаций. Ученые университета работают над созданием квантовой памяти для микроволновых фотонов, что является ключевым элементом для разработки универсальных квантовых компьютеров. Кроме того, в центре разрабатываются методы защиты информации на основе квантовых технологий и проводятся эксперименты по передаче квантовой информации между различными системами. КНИТУ-КАИ также предлагает образовательные программы, включая магистерские курсы по квантовым технологиям, что способствует подготовке специалистов в этой перспективной области.

Казанский физико-технический институт им. Е. К. Завойского КазНЦ РАН (КФТИ КазНЦ РАН)

Казанский физико-технический институт им. Е. К. Завойского является одним из ведущих мировых научных центров в области магнитной радиоспектроскопии. Основными направлениями исследований института являются:

- Электронный парамагнитный резонанс в спиновой физике и спиновой химии
- Квантовая обработка информации
- Нанофизика перспективных материалов и гибридных мезоскопических структур и др.

За последние годы получены важные результаты в области квантовой памяти, развития методологии и применения ЭПР, нанотехнологий, когерентной оптической твердотельной спектроскопии, быстропротекающих процессов, о нестандартных физических свойствах новых материалов.

Участники экосистемы развития квантовых технологий: исследовательские центры

Поволжский государственный университет телекоммуникаций и информатики (ПГУТИ)

ПГУТИ

ПГУТИ — один из крупнейших технических вузов России, который ведет подготовку будущих работников в области связи, телевидения и радиовещания, информатики и массовых коммуникаций. Также университет ведет работу в направлениях: квантовые коммуникации и информационная безопасность. В сфере квантовых технологий в ПГУТИ есть программа обучения, которая дает знания о принципах и применении квантовых явлений, таких как суперпозиция и запутанность, в области коммуникаций. Также есть программа подготовки в области информационной безопасности,, которая охватывает защиту информации и информационных систем от различных угроз, включая кибератаки, несанкционированный доступ и утечку данных.

Участники экосистемы развития квантовых технологий: консорциумы

Национальная квантовая лаборатория

НКЛ Национальная Квантовая Лаборатория

В рамках выполнения мероприятий, предусмотренных дорожной картой, основан консорциум «Национальная квантовая лаборатория» (НКЛ) — международный научно-технологический консорциум, в который вошли ключевые участники российского квантового сообщества. 25 ноября 2020 года подписано соглашение о создании консорциума, который консолидирует усилия университетов, научных центров, команд-разработчиков, стартапов, технологических компаний и финансовых организаций и является основой отечественной квантовой экосистемы. НКЛ является прямым аналогом научно-индустриальных объединений, созданных в США, ЕС, Канаде, Японии и других странах, и основой отечественной квантовой экосистемы. НКЛ предполагает создание инфраструктуры для исследований и разработок, кадровую поддержку (включая привлечение иностранных специалистов), образовательные мероприятия, организацию международного консультирования, взаимодействие с ФОИВ и институтами развития, организацию различных мероприятий, включая международные конференции, научные школы, хакатоны, постоянное информационное взаимодействие между участниками экосистемы, работу с индустрией и формирование рынка квантовых вычислений. На будущих индустриальных партнеров НКЛ возложена обязанность коммерциализации полученных результатов проектов, в том числе в рамках мероприятий по импортозамещению. Кроме того, в части стимулирования спроса планируются мероприятия по оказанию консалтинговых услуг клиентам для повышения эффективности деятельности и образования стоимости как путем предоставления информации и рекомендаций, так и путем предоставления услуг по доступу к облачной платформе. На первичных этапах это будет выражено в подготовке рынка к квантовым вычислениям, формировании у персонала потенциального заказчика понимания, где в его деятельности возможно применение технологии, обобщении отраслевого опыта применения квантовых вычислений для компании, проведении исследований потенциально интересных применений для бизнес-процессов конкретной индустриальной компании, оценке потенциала влияния квантовых вычислений на бизнес и пр.

Межуниверситетская квантовая сеть

МУКС

На IV Конгрессе молодых ученых было подписано соглашение о создании научно-образовательного консорциума для развития межуниверситетской квантовой сети (МУКС). В консорциум вошли ведущие научные и образовательные учреждения России, включая Курчатовский институт, МГУ им. Ломоносова, Университет ИТМО и Казанский научный центр РАН, а также другие организации. Инициаторами создания сети стали МГУ и «Иннопрактика», а научное руководство и администрирование осуществляет Курчатовский институт. Разработка велась при поддержке ОАО «РЖД», которое предоставило магистральную квантовую инфраструктуру, позволившую, объединить университеты и научные центры в единое цифровое пространство. Консорциум займется развитием сети, созданием новых приложений для квантовых коммуникаций и подготовкой специалистов. МУКС уже стала важным шагом к реализации дорожной карты «Квантовые коммуникации», утвержденной Правительством России в 2020 году. Эта технология откроет новые возможности для научных исследований и повышения уровня информационной безопасности.

Ассоциация развития финансовых технологий (Ассоциация ФинТех)

АССОЦИАЦИЯ ФИНТЕХ

Ассоциация ФинТех — объединение представителей российского финансового и ИТ-сектора, развивающее инновационные финансовые технологии и цифровую инфраструктуру в России. Направления работы ассоциации: исследования и аналитика, развитие цифровых продуктов и сервисов, развитие финансовых и информационных технологий, пилотирование инициатив, информационная безопасность финансового рынка.

Участники экосистемы развития квантовых технологий: институты развития

Иннопрактика

Иннопрактика

Негосударственный институт развития, миссией которого является содействие росту национального человеческого капитала России путем формирования благоприятных условий для создания новых технологий и продуктов. Компания выступает медиатором между представителями науки, бизнеса и власти: выстраивая коммуникации, компания выявляет и анализирует потребности бизнеса в инновациях, предлагая эффективные решения.

Российский научный фонд

РНФ Российский научный фонд

РНФ финансирует научные и научно-технические программы и проекты в сфере фундаментальных исследований — исследований, направленных на получение новых знаний об основных закономерностях строения, функционирования и развития человека, общества, окружающей среды. Фонд был учрежден по инициативе Президента России в конце 2013 года, за это время Фондом было поддержано более 60 тысяч российских ученых. С 2022 года расширены полномочия Фонда по поддержке опытно-конструкторских и технологических работ.

Фонд «Сколково»

Sk Сколково

Современный научно-технологический инновационный комплекс по разработке и коммерциализации новых технологий, который был создан в 2010 году. Фонд «Сколково» выступает в качестве института развития в рамках различных высокотехнологичных направлений. Ежегодно Фонд «Сколково» объявляет о новом конкурсном отборе проектов российских компаний, внедряющих инновационные отечественные решения.

Российский фонд прямых инвестиций

РОССИЙСКИЙ ФОНД ПРЯМЫХ ИНВЕСТИЦИЙ

РФПИ осуществляет прямые инвестиции в лидирующие и перспективные российские компании совместно с ведущими инвесторами. Фонд создан в соответствии с Распоряжением Правительства Российской Федерации от 7 июня 2006 года № 838-р с целью стимулирования создания в России собственной индустрии венчурного инвестирования, развития инновационных отраслей экономики и продвижения на международный рынок российских наукоемких технологических продуктов.

Участники экосистемы развития квантовых технологий: институты развития

Фонд Национальной технологической инициативы

ФОНД НТИ

Фонд НТИ — проектный офис Национальной технологической инициативы, оказывает финансовую и экспертную поддержку компаниям для реализации проектов НТИ из средств федерального бюджета. НТИ — это объединение представителей бизнеса и экспертных сообществ для развития в России перспективных технологических рынков и отраслей, которые могут стать основой мировой экономики. В рамках НТИ реализуется несколько дорожных карт различных направлений науки и техники.

Фонд содействия развитию малых форм предприятий в научно-технической сфере (Фонд содействия инновациям)

ФОНД СОДЕЙСТВИЯ ИННОВАЦИЯМ

Фонд содействия инновациям является государственной некоммерческой организацией, созданной для поддержки молодых ученых и малых предприятий, занимающихся высокотехнологичными разработками с потенциалом коммерциализации. Основные направления деятельности фонда включают вовлечение молодежи в инновационную деятельность, поддержку стартапов, содействие коммерциализации научных разработок и развитие высокотехнологичных секторов экономики.

Авторы

Авторы

АНО «Цифровая экономика»

Ярослав Авдиев
Куратор проекта
Директор направления
«Технологическое лидерство»

Шушанна Петросян
Руководитель проекта

Карен Казарян
Директор по аналитике

Николай Ляпичев
Директор направления
«Безопасность цифровых
технологий»

Михаил Вайнштейн
Аналитик

O2Consulting

Анна Никитченко
Управляющий партнер

Елена Казбанова
Руководитель проектов

Сергей Дранев
Руководитель проектов

Александр Чоланюк
Ведущий аналитик

Полина Скалабан
Старший аналитик

Людмила Белехова
Аналитик

Эксперты

Алексей Сантьев
ООО «СМАРТС-Кванттелеком»

Антон Гугля
ООО «КуАпп»

Алексей Уривский
АО «ИнфоТеКС»

Александр Поздняков
АО «Центр исследований и разработок»

Александр Приютов
ООО «КуРэйт»

Александр Шаманаев
АО «ИнфоТеКС»

Сергей Петренко
АНО ВО «Университет Иннополис», НТУ «Сириус»

Нияз Исмагилов
ПАО «Газпром нефть»

Даниил Лобов
Kept

Евгений Семёнов
АО «Компания ТрансТелеКом»

Михаил Котков
ОАО «РЖД»

Михаил Корягин
АНО «Цифровая экономика»

Сергей Ханенков
ПАО «Ростелеком»

Александр Клемин
АО НИП «ИНФОРМЗАЩИТА»

Николай Спирихин
ПАО «Софтлайн»

Дмитрий Хан
ООО «НЕОТЕХ»,
ООО «Квантовые коммуникации»,
ООО «СМАРТС-Квантелеком»,
ООО «АПИК»

Кирилл Антонов
ООО «ВЕБ3 ТЕХНОЛОГИИ»

Даниил Яшин
ООО «СМАРТС-Квантелеком»

Виктор Белохин
Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26)

Алексей Моисеевский
ООО «С-Квантум»

Ярослав Кожемяко
ООО «КуРэйт»

Сергей Кулик
Инновационный научно-технический центр МГУ «Воробьевы горы», кластер «Ломоносов»

Андрей Крючков
РТУ МИРЭА

Владимир Егоров
Университет ИТМО,
ООО «СМАРТС-Квантелеком»

Основные определения

Основные определения

АЛГОРИТМ ШОРА (КВАНТОВЫЙ АЛГОРИТМ ФАКТОРИЗАЦИИ) — квантовый алгоритм разложения числа на простые множители, работающий экспоненциально быстрее, чем классические методы, благодаря чему создает критическую угрозу для систем защиты данных, основанных на сложности этой задачи.

АЛГОРИТМ ГРОВЕРА — квантовый алгоритм ускоренного поиска по неструктурированной базе данных, способный давать не экспоненциальное, но квадратичное ускорение.

ГИБРИДНЫЕ КВАНТОВЫЕ СЕТИ — системы связи, которые объединяют квантовые технологии для передачи информации с классическими сетями для управления и обработки данных.

ДОВЕРЕННЫЙ ПРОМЕЖУТОЧНЫЙ УЗЕЛ (ДПУ) — доверенный узел сети квантового распределения ключей, вырабатывающий в паре с другими доверенными промежуточными узлами квантовые и/или целевые ключи.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ИБ) — состояние защищенности национальных интересов, при котором обеспечивается нейтрализация угроз информационной безопасности РФ.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ (ИИ) — комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение, поиск решений без заранее заданного алгоритма и достижение инсайта) и получать при выполнении конкретных практически значимых задач обработки данных результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека.

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ — тип вычислений, в которых информация представляется как различимые состояния квантовых систем, над которыми реализуется возможность осуществления универсального набора преобразований (можно построить любой алгоритм).

КВАНТОВО-ГОМОМОРФНОЕ ШИФРОВАНИЕ — форма шифрования, позволяющая производить определенные математические действия с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполненных с открытым текстом.

КВАНТОВЫЙ ИНТЕРНЕТ — глобальная информационная квантовая сеть, в узлах которой формируется, обрабатывается и хранится квантовая информация, и узлы которой соединены квантовыми каналами.

КВАНТОВЫЕ КОММУНИКАЦИИ (КВАНТОВАЯ КРИПТОГРАФИЯ) — передача информации посредством прямой передачи квантовых состояний или посредством квантовой запутанности.

КВАНТОВЫЙ КОМПЬЮТЕР (ВЫЧИСЛИТЕЛЬ) — квантовое вычислительное устройство, основанное на кодировании информации в квантовом состоянии двухуровневой системы — кубита (или многоуровневой системы — кудита). В отличие от классического компьютера, основанного на бинарном коде (т. е. анализирующем информацию, представленную в виде «0» и «1»), такие машины основаны на кодировании информации в квантовом состоянии двухуровневой системы, что позволяет работать не только с состояниями «0» и «1», но и любой их суперпозицией.

Основные определения

КВАНТОВАЯ ПЛАТФОРМА — способ физической реализации кубитов (например, энергетические уровни атомов или ионов, поляризация фотонов, направление спина и пр.).

КВАНТОВОЕ ПРЕИМУЩЕСТВО — способность квантовых вычислителей решать ряд задач принципиально более эффективно, чем любые классические компьютеры.

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ (КРК) — процедура выработки и распределения секретных ключей, реализуемая с помощью квантовых криптографических протоколов и квантовых каналов связи.

КВАНТОВЫЕ ОСЦИЛЛЯТОРЫ — квантовый аналог классического гармонического осциллятора, представляющий собой квантовую систему, совершающую периодические колебания, где энергия может принимать лишь дискретные (квантованные) значения.

КВАНТОВЫЕ СЕНСОРЫ — высокочувствительные измерительные приборы, основанные на регистрации индивидуальных квантовых эффектов, то есть квантовых эффектов, касающихся отдельных квантовых систем.

КВАНТОВЫЙ ЭМУЛЯТОР (ЭМУЛЯТОР КВАНТОВОГО ПРОЦЕССОРА) — программно-аппаратный комплекс или программное обеспечение, позволяющий моделировать поведение квантового процессора посредством классических вычислительных средств.

КВАНТОВЫЙ ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ (КГСЧ) — устройство, использующее квантово-механические эффекты для выработки случайных чисел.

КВАНТОВО-ЗАЩИЩЕННЫЙ КЛЮЧ (КЗК) — секретный ключ, защита которого при передаче или хранении осуществляется с использованием квантового ключа/ключей.

КВАНТОВО-ЗАЩИЩЕННАЯ СЕТЬ СВЯЗИ (КЗСС) — сеть связи, предназначенная для защищенной передачи данных с использованием квантовых ключей и/или квантово-защищенных ключей.

КУБИТ — единица представления квантовой информации, реализуемая двумя состояниями квантовой системы, находящейся в одном из состояний или в суперпозиции обоих состояний.

ЛОКАЛЬНЫЕ НОРМАТИВНЫЕ АКТЫ (ЛНА) — документ, содержащий нормы трудового права, который принимается работодателем в пределах его компетенции в соответствии с законами и иными нормативными правовыми актами, коллективным договором, соглашениями.

МАШИННОЕ ОБУЧЕНИЕ — процесс, реализующий вычислительные методы, которые предоставляют системам возможность обучаться на данных или на основе опыта, что позволяет автоматизировать решение задачи без заранее заданного алгоритма.

Основные определения

МОДУЛЬ УПРАВЛЕНИЯ КЛЮЧАМИ (МУК) — программно-аппаратный комплекс управления ключами, предназначенный для формирования квантово-защищенных ключей (КЗК) между узлами сети квантового распределения ключей (КРК), которые не имеют общего квантового канала, приема квантовых ключей (КК) от сопряженных с ним модулей КРК, централизованного управления жизненным циклом как КК и КЗК.

НИОКР — научно-исследовательские и опытно-конструкторские работы.

ОПТОВОЛОКОННЫЕ КВАНТОВЫЕ КОММУНИКАЦИИ — передача квантовых состояний, таких как фотоны, по оптическим волокнам для обеспечения безопасной и защищенной связи.

ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ — новые криптографические алгоритмы, устойчивые к кибератакам с применением квантовых компьютеров.

СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (СИБ) — совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

СИГНАТУРНЫЙ АНАЛИЗ — один из методов антивирусной защиты, заключающийся в выявлении характерных идентифицирующих свойств каждого вируса и поиске вирусов при сравнении файлов с выявленными свойствами.

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ) — средства, системы и комплексы, реализующие криптографическую систему. К средствам криптографической защиты информации относятся средства шифрования, имитозащиты, электронной подписи, кодирования, изготовления ключевых документов, ключевые документы.

СПУТНИКОВАЯ КВАНТОВАЯ СВЯЗЬ — технология, использующая квантовые свойства частиц, например, запутанность, для передачи защищенной информации на большие расстояния, в том числе между Землей и спутником.

УГТ — метрика, используемая для оценки зрелости технологий в процессе их разработки и внедрения, регулируемая национальным стандартом ГОСТ Р 58048-2017.

ЭКСПЕРИМЕНТАЛЬНЫЙ ПРАВОВОЙ РЕЖИМ (ЭПР) — применение в отношении участников ЭПР в течение определенного периода времени специального регулирования по направлениям разработки, апробации и внедрения цифровых инноваций.

CISA (Cybersecurity and Infrastructure Security Agency) — Агентство по кибербезопасности и защите инфраструктуры США.

IaaS (Infrastructure as a Service) — это тип инсталляции, при котором компания арендует вычислительные мощности IT-инфраструктуры у провайдера.

Основные определения

KaaS (Kubernetes as a Service) — это управляемый облачный сервис оркестрации контейнеров, который автоматизирует развертывание, масштабирование и обновление микросервисов и приложений на основе Kubernetes (платформа с открытым исходным кодом).

NIST (The National Institute of Standards and Technology) — Национальный институт стандартов и технологий США.

On-premise («на территории» или «в помещении») — модель локального развертывания программного обеспечения и IT-инфраструктуры.

PaaS (Platform as a Service) — это тип облачных сервисов, который предоставляет виртуальную инфраструктуру для разработки и развертывания приложений.

POSTURE MANAGEMENT (управление состоянием защит) — система управления текущим уровнем киберзащищенности, которая постоянно проверяет, соответствует ли инфраструктура принципам Zero Trust, и автоматически устраняет отклонения.

QUBO-решатель — вычислительная машина, предназначенная для решения задач квадратичной бинарной оптимизации без ограничений QUBO (Quadratic Unconstrained Binary Optimization).

QUBO-решатель семейства SB — специализированный решатель на основе улучшенного алгоритма моделирования адиабатических бифуркаций в нелинейных гамильтоновых системах с теоретико-игровой фазой (GdSB). Используется для решения оптимизационных задач обеспечения устойчивости функционирования национальных блокчейн-экосистем и платформ в условиях появления новой квантовой угрозы безопасности информации.

RSA — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших полупростых чисел.

SaaS (Software as a Service) — тип инсталляции программного обеспечения, при котором доступ к программе предоставляется через интернет.

SLA (SERVICE LEVEL AGREEMENT) — соглашение об уровне сервиса между заказчиком и исполнителем.

STACK-BASED — это принцип работы языка программирования или виртуальной машины, где основная обработка данных выполняется с использованием стека для хранения временных значений, аргументов и возвращаемых результатов.

TLS (Transport Layer Security) — это стандартный интернет-протокол, обеспечивающий шифрование, аутентификацию и целостность данных при передаче информации в сети.

VPN (Virtual Private Network) — технология, которая позволяет установить безопасное зашифрованное соединение между устройством и интернетом через специальный сервер.

ZERO TRUST (нулевое доверие) — подход к информационной безопасности, в котором никому не доверяют по умолчанию: ни пользователю, ни компьютеру, ни приложению, даже если они внутри корпоративной сети.

Источники

ИСТОЧНИКИ

1. Доктрина информационной безопасности Российской Федерации. URL: https://base.garant.ru/71556224/?ysclid=makz2c5oaa387180489
2. World Economic Forum Global Cybersecurity Outlook 2025 URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
3. Quantum Economy Blueprint. 2024. URL: https://www.weforum.org/publications/quantum-economy-blueprint/
4. ГОСТ Р ИСО/МЭК 27001-2021. URL: https://base.garant.ru/403510768/
5. Gartner. URL: https://www.gartner.com/en/articles/information-security#:~:text=Information%20security%20forecast%3A%20What%20to,11.7%25%20from%202023%20to%202028.
6. Forbes. URL: https://www.forbes.ru/tekhnologii/532961-rossia-vosla-v-top-10-stran-mira-po-rashodam-na-kiberbezopasnost?ysclid=mc3d82fdrc377212240
7. Б1 «Рынок информационной безопасности России». URL: https://b1.ru/local/assets/surveys/russian-information-security-market-survey-2025.pdf
8. Центр стратегических разработок, 2025. URL: https://www.csr.ru/ru/news/tssr-v-bolshinstve-kompaniy-raschyet-investitsiy-v-informatsionnuyu-bezopasnost-provoditsya-bez-otsenki-kiberugroz/?ysclid=mei95277au60259389
9. Информзащита «Скачок к безопасности». URL: https://www.infosec.ru/press-center/smi/?PAGEN_4=4
10. Центр по лицензированию, сертификации и защите государственной тайны ФСБ России. URL: http://clsz.fsb.ru/clsz/certification.htm
11. Аналитический отчет «Перспективные сценарии применения квантовых и смежных технологий в отраслях». URL: https://xn--d1abjl7at.xn--p1ai/analytics/ano-cje-vypustila-analiticheskij-otchet-o-scenarijah-primenenija-kvantovyh-tehnologij/
12. ПНСТ 829-2023. URL: https://normadocs.ru/pnst_829-2023
13. McKinsey, Quantum Technology Monitor, 2024. URL: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/steady%20progress%20in%20approaching%20the%20quantum%20advantage/quantum-technology-monitor-april-2024.pdf
14. СберПро. URL: https://sber.pro/publication/50-kubitnii-kompyuter-shifrator-v-tsod-i-generatori-dlya-5g-kak-razvivalas-kvantovaya-industriya-v-2024-godu/
15. Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии». URL: https://digital.gov.ru/uploaded/files/07102019kvantyi.pdf
16. N + 1, 2020. URL: https://nplus1.ru/material/2020/02/06/course-quantum-technology-chapter3
17. Gartner, 2024, 2025. URL: https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends
18. NIST, 2025. URL: https://www.nist.gov/publications/status-report-fourth-round-nist-post-quantum-cryptography-standardization-process
19. SecurityLab. URL: https://www.securitylab.ru/news/542276.php, https://www.securitylab.ru/news/547233.php
20. NIST. URL: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
21. New York University. URL: https://www.nyu.edu/about/news-publications/news/2023/september/nyu-takes-quantum-step-in-establishing-cutting-edge-tech-hub-in-.html
22. Chinese Academy of Sciences. URL: https://english.cas.cn/newsroom/archive/news_archive/nu2017/201703/t20170324_175288.shtml
23. QuNET. URL: https://qunet-initiative.de/en/homepage/
24. BSI. URL: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/250121_erste_quantensichere_Smartcard.html
25. Quantinuum. URL: https://www.quantinuum.com/press-releases/cybertrust-japan-integrates-quantum-computing-hardened-private-keys-from-quantinuum-into-new-iot-authentication-platform
26. Open Quantum Safe. URL: https://openquantumsafe.org/
27. QuintessenceLabs. URL: https://info.quintessencelabs.com/hubfs/QLabs-qStream-product-sheet.pdf
28. Singtel. URL: URL: https://www.singtel.com/about-us/media-centre/news-releases/singtel-to-develop-singapore-s-first-nationwide-quantum-safe-net
29. Nokia. URL: https://www.nokia.com/newsroom/nokia-and-sk-broadband-deploy-quantum-secure-network-to-protect-korea-hydro-and-nuclear-powers-it-infrastructure/
30. Ministry of Defence. URL: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2077600
31. ID Quantique. URL: https://www.idquantique.com/id-quantique-unveils-its-4th-generation-of-quantum-key-distribution-qkd-the-cerberis-xg-the-ultimate-in-quantum-safe-security/
32. Technology Innovation Institute. URL: https://www.tii.ae/news/tii-and-uae-space-agency-unveil-pioneering-unhackable-quantum-tech-gitex-2024
33. European Commission. URL: https://digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy
34. Quantum Internet Alliance. URL: https://quantuminternetalliance.org/
35. EuroQCI. URL: https://petrus-euroqci.eu/about-euroqci/
36. Распоряжение Правительства РФ от 11 июля 2023 года № 1856-р «Об утверждении Концепции регулирования отрасли квантовых коммуникаций в РФ до 2030 года». URL: https://www.garant.ru/products/ipo/prime/doc/407297268/
37. Распоряжение Правительства РФ от 20 мая 2023 года № 1315-р «Об утверждении Концепции технологического развития на период до 2030 года». URL: https://www.garant.ru/products/ipo/prime/doc/406831204/?ysclid=mdh3e7dtio153803555
38. Национальный проект «Экономика данных и цифровая трансформация государства». URL: https://digital.gov.ru/target/naczionalnyj-proekt-ekonomika-dannyh-i-czifrovaya-transformacziya-gosudarstva
39. Приказ Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)». URL: https://base.garant.ru/187947/

ИСТОЧНИКИ

40. Пекинский комитет по управлению зонами экономического и технологического развития. URL: https://www.ncsti.gov.cn/zcfg/zcwj/202507/t20250717_210709.html
41. Quantum Twelve. URL: https://zrzyhgh.wuhan.gov.cn/dhxjskfqfj/dhxjskfqfj_xwdt/dhxjskfqfj_gzdt/202406/t20240617_2416870.shtml
42. NIST (SBIR). URL: https://www.nist.gov/tpo/small-business-innovation-research-program-sbir/sbir-past-solicitations-and-awards
43. NSF. URL: https://seedfund.nsf.gov/our-program/
44. Monetary Authority of Singapore. URL: https://www.mas.gov.sg/schemes-and-initiatives/fsti-quantum-track
45. EIC STEP Scale Up. URL: https://eic.ec.europa.eu/eic-funding-opportunities/step-scale_en
46. EIC Accelerator. URL: https://eic.ec.europa.eu/eic-funding-opportunities/eic-accelerator_en
47. EIC Accelerator Open. URL: https://eic.ec.europa.eu/eic-funding-opportunities/eic-accelerator/eic-accelerator-open_en
48. Transition to post-quantum Public Key Infrastructures. URL: https://www.euro-access.eu/en/calls/2265/Transition-to-post-quantum-Public-Key-Infrastructures
49. Horizon Europe. URL: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en
50. Security evaluations of Post-Quantum Cryptography (PQC) primitives. URL: https://www.euro-access.eu/en/calls/2252/Security-evaluations-of-Post-Quantum-Cryptography-PQC-primitives
51. Integration of PQC algorithms into high-level protocols. URL: https://www.euro-access.eu/en/calls/2251/Integration-of-Post-Quantum-Cryptography-PQC-algorithms-into-high-level-protocols
52. Security of implementations of PQC algorithms. URL: https://www.euro-access.eu/en/calls/2256/Security-of-implementations-of-Post-Quantum-Cryptography-algorithms
53. Innovate UK «Quantum Missions». URL: https://apply-for-innovation-funding.service.gov.uk/competition/2053/overview/19887003-54f6-4391-a146-a30a85b43e58#eligibility
54. BMBF. URL: https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/qktn
55. Développement des technologies innovantes critiques 4e édition. URL: https://www.entreprises.gouv.fr/espace-entreprises/appels-a-projets-et-appels-a-manifestation-d-interet/developpement-de
56. Bpifrance. URL: https://www.bpifrance.fr/nos-appels-a-projets-concours/appel-a-projets-developpement-de-technologies-innovantes-critiques-4eme-edition
57. ASTRID. URL: https://anr.fr/fileadmin/aap/2025/aap-astrid-2025.pdf
58. Quantum Delta NL SME. URL: https://www.hightechnl.nl/hightechnl/nieuws/quantum-delta-nl-sme-programme/
59. BRIDGE Quantum Call 2025. URL: https://www.bridge.ch/en/M0VBCBisNAzM6eHE/page/quantum-call-2025
60. NEDO. URL: https://www.nedo.go.jp/content/800029844.pdf
61. Проект «Приоритетные ИКТ-технологии». URL: https://www.soumu.go.jp/menu_news/s-news/01tsushin03_02000422.html
62. NSERC. URL: https://www.nserc-crsng.gc.ca/NewsDetail-DetailNouvelles_eng.asp
63. Quantum Commercialization Program. URL: https://digitalsupercluster.ca/innovate-with-us/call-for-projects/quantum/
64. Программа CTCP (Round 1/1). URL: https://business.gov.au/-/media/grants-and-programs/critical-technologies-challenge-program-stage-1/critical-technologies-challenge-program-round-1-feasibility---applicant-information-package-pdf.pdf?hash=2B57281501607BA7A1C266411B2119AB&sc_lang=en
65. Программа CTCP (Round 1/2). URL: https://business.gov.au/-/media/grants-and-programs/critical-technologies-challenge-program-stage-1/ctcp-round-1-stage-2-demonstrator-frequently-asked-questions-pdf.pdf?hash=14968A447AB392A640CC5EB9BA55FE93&sc_lang=en
66. Национальный доменный регулятор auDA. URL: https://www.auda.org.au/news-insights/statements/auda-grants-2-5m-to-protect-dns-from-quantum-risk-and-vulnerable-australians-from-scams/
67. NIDG. URL: https://www.researchgrants.gov.au/sites/default/files/2025-07/NIDG Intelligence Challenges - ID26 - July 2025_2.pdf
68. MAGNET. URL: https://innovationisrael.org.il/programs/%D7%9E%D7%A1%D7%9C%D7%95%D7%9C-%D7%9E%D7%90%D7%92%D7%93%D7%99-%D7%9E%D7%97%D7%A7%D7%A8-%D7%99%D7%99%D7%A9%D7%95%D7%9E%D7%99-%D7%A7%D7%A8%D7%9F-%D7%94%D7%9E%D7%97%D7%A7%D7%A8-%D7%94%D7%99%D7%99%D7%A9/
69. Консорциум PQC. URL: https://innovationisrael.org.il/%d7%9e%d7%90/
70. Поддержка пилотной миграции к постквантовой криптографии 2025. URL: https://www.kisa.or.kr/401/form?postSeq=3424
71. KISA. https://www.kisa.or.kr/post/fileDownload?attachSeq=2&lang_type=KO&menuSeq=401&postSeq=3424
72. ICT R&D 2025. URL: https://www.severance.healthcare/research/project/news.do?articleNo=124753&mode=view&title=%5BIITP%5D+2025%EB%85%84%EB%8F%84+%EC%A0%9C1%EC%B0%A8+%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%E2%80%A4%EB%B0%A9%EC%86%A1+%EA%B8%B0%EC%88%A0%EA%B0%9C%EB%B0%9C%EC%82%AC%EC%97%85+++%EB%B0%8F+%ED%91%9C%EC%A4%80%EA%B0%9C%EB%B0%9C%EC%A7%80%EC%9B%90%EC%82%AC%EC%97%85+%EC%8B%A0%EA%B7%9C%EC%A7%80%EC%9B%90+%EB%8C%80%EC%83%81%EA%B3%BC%EC%A0%9C+%EA%B3%B5%EA%B3%A0
73. MeitY. URL: https://www.meity.gov.in/static/uploads/2025/08/fdcd62910f9409c4ec8ddcae0fc96327.pdf
74. TTDF. URL: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2137640
75. ADGM. URL: https://www.adgm.com/media/announcements/adgm-and-adgm-academy-team-up-with-tii-hub71-and-aspire-to-launch-uaes-first-quantum-secure-communications-testbed
76. Проквант. URL: https://proquant.ru/infrastructure/net1/magistralnaya-kvantovaya-set?ysclid=mghrxuhf5z106872024

ПРИМЕРЫ ПРОЯВЛЕНИЯ ТРЕНДОВ (В ТОМ ЧИСЛЕ РЕШЕНИЯ НА БАЗЕ КВАНТОВЫХ ТЕХНОЛОГИЙ)

1. ООО «СМАРТС-Кванттелеком» (Россия), https://quanttelecom.ru/products/qualion_a#submenu:about
2. Google (США), https://security.googleblog.com/2024/09/a-new-path-for-kyber-on-web.html
3. ОАО «РЖД» (Россия), https://d-russia.ru/protjazhjonnost-kvantovyh-linij-svjazi-prevysila-7-tys-km-glavnyj-inzhener-rzhd.html
4. Квантовый интернет (Китай), https://www.nature.com/articles/s41377-023-01158-7
5. АО «ИнфоТеКС» (Россия), https://securitymedia.org/articles/interview/oleg-ivanov-infoteks-kvantovye-tekhnologii-stanovyatsya-vse-bolee-interesny-i-dostupny.html?erid=2SDnjdpztLt
6. Высокосортная квантовая связь (Китай), https://www.science.org/doi/10.1126/sciadv.adt4627
7. ООО «КуАпп» и ООО «Веб3 Технологии» (Россия), https://qapp.tech/cases/web3_tech
8. OpenQKD (ЕС), https://openqkd.eu/use_case/use-case-02-smart-grid/
9. Дорожные карты «квантовые коммуникации» и «квантовые вычисления» (Россия), https://digital.gov.ru/activity/razvitie-it-otrasli/kvantovye-kommunikaczii, https://digital.gov.ru/activity/radioelektronika/kvantovye-vychisleniya
10. NIST (США), https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
11. ОАО «РЖД» (Россия), https://www.rzd.ru/ru/9284/page/3102?id=315351
12. China Telecom Quantum Group (Китай), https://www.chinadaily.com.cn/a/202505/14/WS68246a9ba310a04af22bf4f9.html

ЭКОНОМИКА

ТЕХЛИД .РФ

минцифры_

ГАЗПРОМБАНК

© Москва, 2025 год