QApp

Кибербезопасность. Постквантовые алгоритмы шифрования

QApp.tech

SkКиберХаб

Компания QApp — лидер в РФ по постквантовым алгоритмам

QApp

Спинофф Российского квантового центра

Лауреат всероссийских премий и конкурсов ИТ-продуктов

Участник КиберХаба Сколково

При стратегической поддержке Газпромбанка

Разработчик стандартов постквантовой криптографии в РФ (участник ТК26 Росстандарта)

Активный участник рабочих групп Национального Технологического центра цифровой криптографии

26 сотрудников

8 цифровых продуктов

Продукты и услуги уже пилотируются

Банк России · СБЕР · ГАЗПРОМБАНК · ВТБ · эльбрус · Baikal Electronics · s•terra · QRATE · НСПК · T1 · web3 tech · ФИНТЕХ АССОЦИАЦИЯ

Квантовая угроза — новый риск для кибербезопасности, который становится актуальнее с каждым годом

С помощью мощных квантовых компьютеров злоумышленники могут атаковать данные, защищенные традиционными методами шифрования

2026 год — прогноз первых квантовых атак

McKinsey & Company

Распространенные сегодня алгоритмы криптографии неустойчивы к квантовой угрозе

Распределение ключей	Асимметричное шифрование	Электронная подпись

Квантовая угроза усиливает ключевые риски кибербезопасности по ряду направлений

- Сетевая инфраструктура
- Стандартное программное обеспечение
- Интернет вещей
- Блокчейн решения

Постквантовые алгоритмы — оптимальный метод защиты от квантовой угрозы

Новый класс асимметричных алгоритмов шифрования, устойчивых к кибератакам с применением как классических, так и квантовых компьютеров. Постквантовая криптография может быть легко интегрирована с серверной инфраструктурой, мобильными и веб-сервисами

- Пользовательские данные
- Внутренние и внешние коммуникации
- Хранение данных
- Электронный документооборот
- Аутентификация

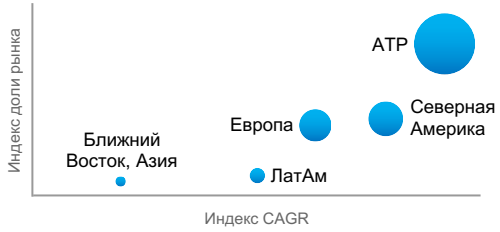
- Высокая скорость и простота интеграции
- Поддержка популярных платформ и протоколов
- Совместимость с отечественными процессорами
- Отечественная реализация постквантовых алгоритмов-кандидатов на включение в госстандарты

За 2023 год в мире возросла актуальность квантовой угрозы. Государства и бизнес переходят на постквантовые решения

Прогнозируется рост объема глобального рынка постквантовых решений с 2024 года [1]

$158 млн
в 2024

$8,8 млрд
в 2030
CAGR 95,2%



1 марта 2023 принята обновленная «Стратегия национальной кибербезопасности США» [2]

STRATEGIC OBJECTIVE 4.3: PREPARE FOR OUR POST-QUANTUM FUTURE

Конкурс NIST вошел в финальную фазу [3]
Алгоритмы-кандидаты на включение в стандарты QApp уже реализованы

€150 млн выделено на развитие постквантовой криптографии во Франции [4]

НАТО успешно завершил пилоты по постквантовым решениям [5]

Google Microsoft IBM

Активно развиваются профильные RnD департаменты ИТ-гигантов и более 14 стартапов

CLOUDFLARE

19% мировых веб-ресурсов

Крупнейший в мире провайдер экспериментально обеспечил постквантовой криптографией работающие с ним веб-ресурсы

[1] Growth Market Reports [2] National Cybersecurity Strategy [3] NIST [4] France Diplomacy [5] Information Age [6] Silicon Angle

Рынок постквантовых решений в РФ активно формируется. Разработка госстандартов вышла на новый уровень

Разработка новых госстандартов в Техническом комитете по стандартизации «Криптографическая защита информации»

Курируется ФСБ России и Росстандартом

В 2023 году появились первые открытые реализации постквантовых алгоритмов

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Академия криптографии Российской Федерации

Курируется Минцифрой [3]

Выполняются НИРы

ФОРУМ БУДУЩИХ ТЕХНОЛОГИЙ

Постквантовые решения QApp представлены **Президенту РФ** [4]

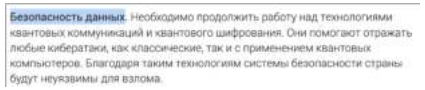
ПРАВИТЕЛЬСТВО МОСКВЫ

Определены приоритетные направления пилотов [5]

Постквантовая криптография включена в стратегические сессии по перспективным технологиям ИБ для России и Москвы

Минцифры России

Квантово-устойчивая защита данных включается в новый нацпроект «**Экономика данных**» [6]



НСПК АСТРА web3 tech

Крупные отраслевые компании заинтересованы в ускорении разработки новых госстандартов

[1] ТК26 [2] Научная Россия [3] НТЦ ЦК [4] Форум Будущих Технологий [5] Росконгресс [6] Минцифры

Правительством Москвы определены **приоритетные направления апробации квантовых технологий**

ПРАВИТЕЛЬСТВО МОСКВЫ

РКЦ Российский Квантовый Центр

Подробнее

Отрасли экономики	Постквантовые алгоритмы
Медицинская промышленность	✓
Авиа- и ракетостроение	✓
Информационные технологии	✓
Биохимия	✓
Автомобильная промышленность	✓
Микроэлектроника	✓
Московская электронная школа	✓

Ценность пилотирования квантово-устойчивых решений защиты данных

Оценка затрат на ввод в промышленную эксплуатацию

Оценка затрат по переводу ИТ-инфраструктуры на новый вид криптографии в проекции на срок принятия стандартов в РФ

Выработка криптографической гибкости

Исследование уровня криптографической гибкости и точек привязки к определенному поставщику криптографических решений, ограничивающих возможности поддержки и адаптации инфраструктуры к новым типам угроз и уязвимостей

Приоритетные типы данных к защите:

- Финансовые
- Персональные
- Инженерная тайна
- Данные блокчейн-проектов

…

Приоритетные отрасли экономики РФ:

- Финансы
- Телеком
- Энергетика
- Медицина

…

Отечественные разработки по постквантовым алгоритмам

QApp

Конечные продукты

PQ CHAIN — квантово-устойчивый блокчейн

web3 tech

PQ GATE — квантово-устойчивый TLS-шлюз

s•terra

Qtunnel — постквантовая защита данных в процессе передачи

PQ VPN — квантово-устойчивые виртуальные частные сети

PQ EDU — теория и практика по постквантовой криптографии

Системные решения

PQLR SDK — библиотека постквантовых алгоритмов и средства упрощающие их интеграцию

PQC IP — аппаратное ускорение постквантовых алгоритмов

PQCA — инфраструктура удостоверяющего центра

Алгоритмы в интересах общества

гиперикум

Новый постквантовый алгоритм цифровой подписи.
Кандидат на включение в госстандарты РФ

Сопроводительные услуги

Семинары и консалтинг

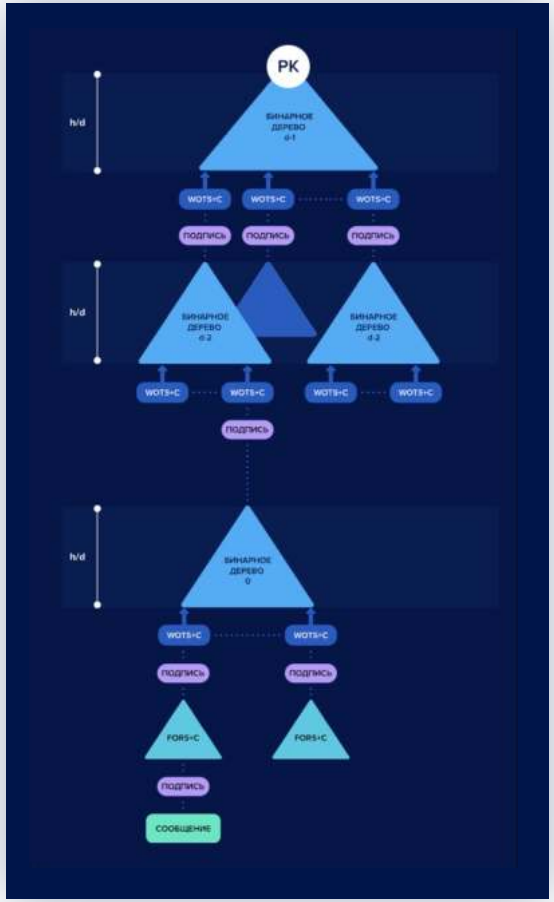
НИРы

ОКРы и пилоты

Разработан новый постквантовый алгоритм цифровой подписи «Гиперикум»

гиперикум

QApp



«Гиперикум» — алгоритм-кандидат на включение в госстандарты.
Ведётся разработка спецификации с учётом замечаний ТК26

Реализовано аппаратное ускорение алгоритма

Опубликована первая в России открытая реализация алгоритма

GitHub

Алгоритм представлен на профильных мероприятиях

конференция РусКрипто

ФОРУМ РОССИЯ 2023

Музей криптографии

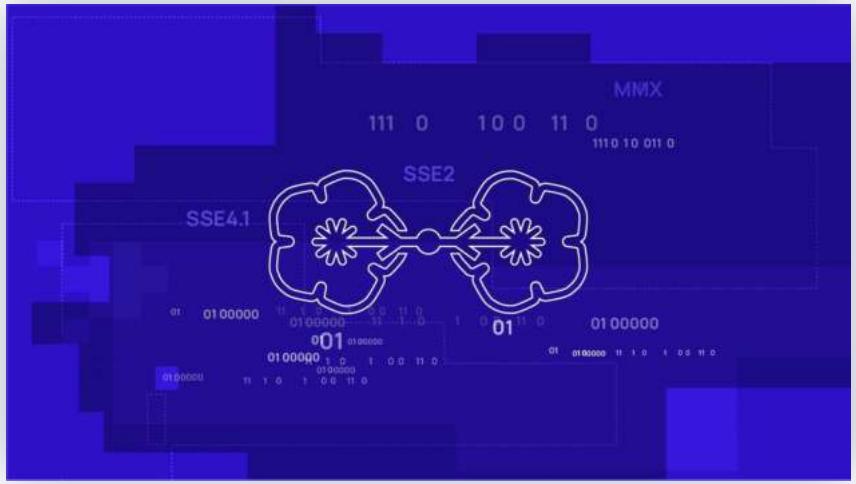
НФО Берег

Подробнее о проекте

Подготовлена открытая реализация нового постквантового алгоритма «Шиповник»

КРИПТОНИТ QApp

«Шиповник» — алгоритм-кандидат на включение в госстандарты.
QApp совместно с компанией «Криптонит» ведёт разработку проекта стандарта в рамках деятельности ТК26



Опубликована вторая в России открытая реализация постквантового алгоритма

GitHub

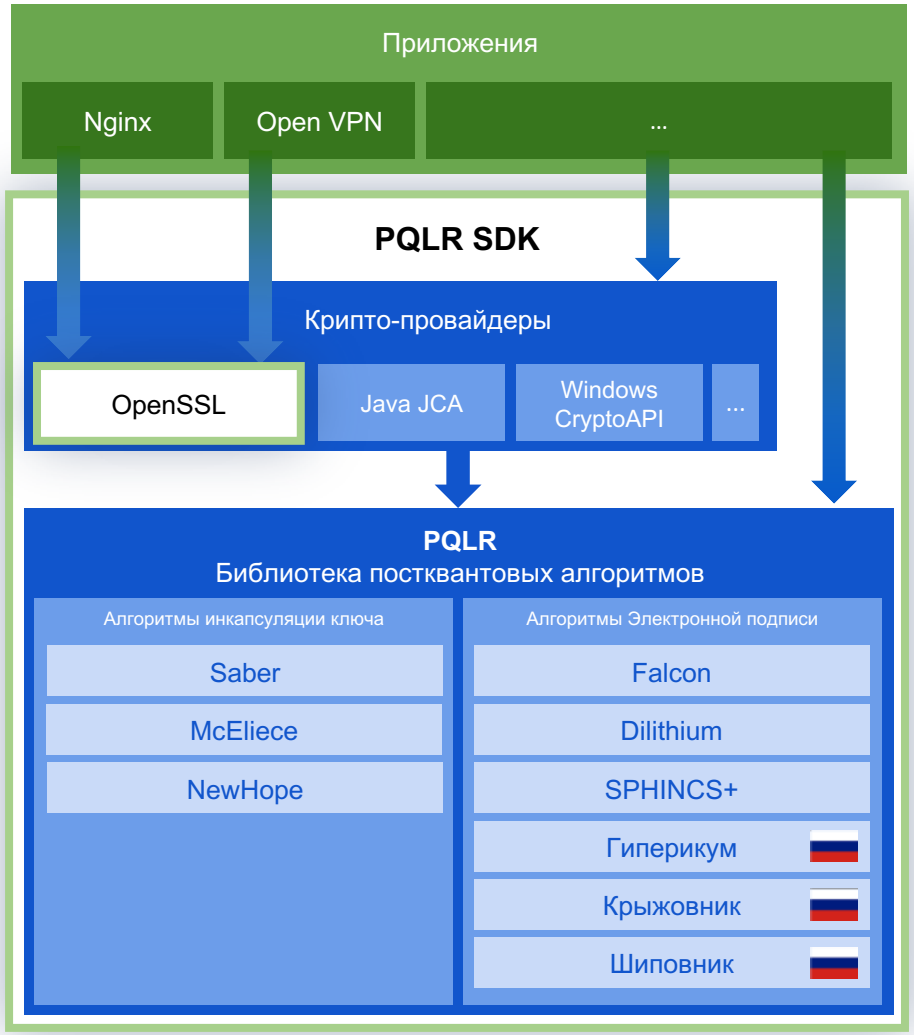
Проект получил большой резонанс в медиа:

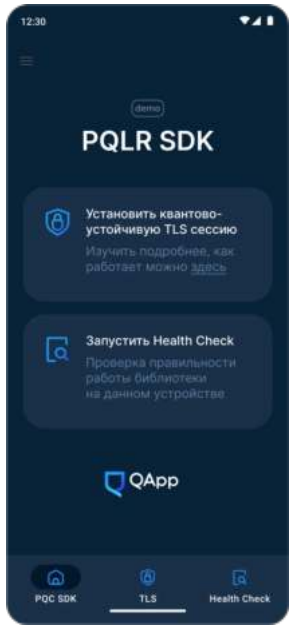
- 8 статей опубликовано
- Более 264,000 возможных контактов с аудиторией
- 17 материалов в соцсетях с общим количеством просмотров более 10,000

Подробнее

PQLR SDK — библиотека постквантовых алгоритмов и средства, упрощающие их интеграцию в конечные продукты

QApp





Реализованы новые алгоритмы-кандидаты в госстандарты РФ:

- ЭЦП «Крыжовник»
- ЭЦП «Гиперикум»
- ЭЦП «Шиповник»

Поддержка протоколов:

Реализована интеграция в протокол OpenVPN

Поддержка новых платформ:

- Добавлена поддержка ЭЦП в Android
- Добавлена экспериментальная поддержка Java JCA и WASM
- Демонстрационное мобильное приложение в процессе реализации

9

реализованных постквантовых алгоритмов в PQLR SDK

Продукт уже пилотируется

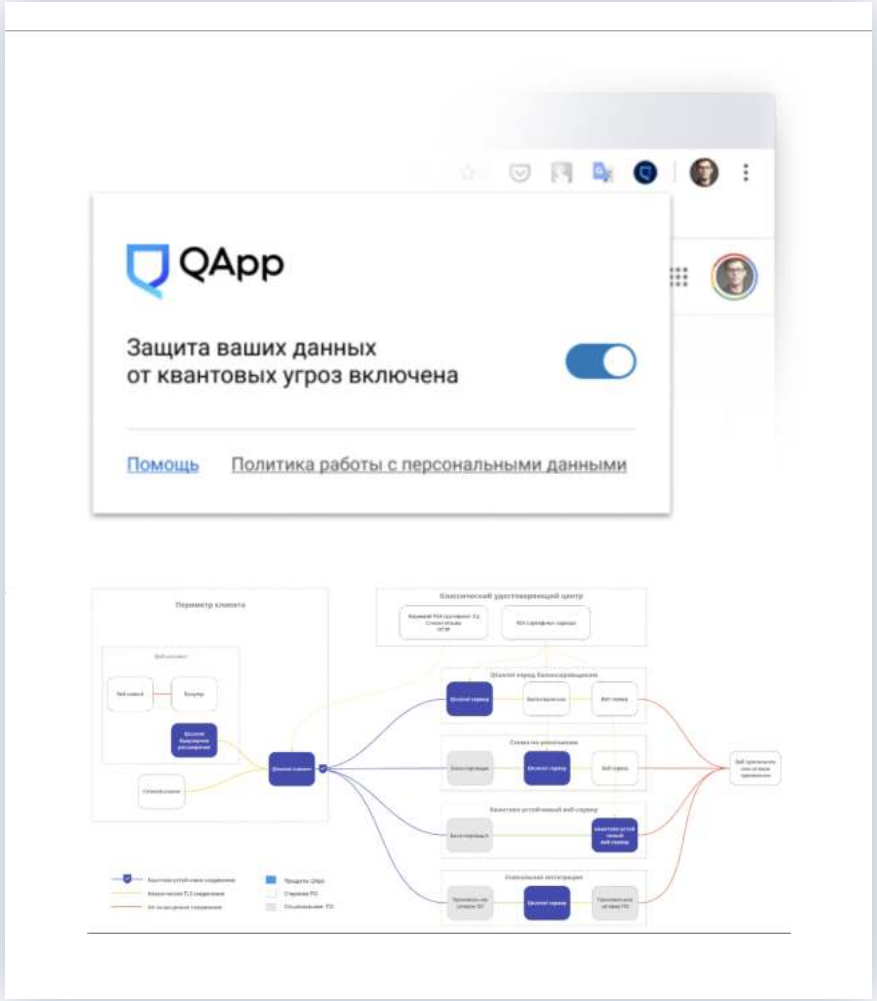
ГАЗПРОМБАНК НСПК web3 tech s•terra

Доказана совместимость

эльбрус Baikal ELECTRONICS

Подробнее о продукте

Qtunnel — ПО для реализации квантово-устойчивых соединений в сетях различных топологий



Сделано в 2023:

Добавлена возможность конфигурации клиентских приложений:

- Реализован серверный функционал Qtunnel API
- Произведена автоматизация регрессионного тестирования Qtunnel API
- Проводится тестирование Qtunnel API

По другим направлениям:

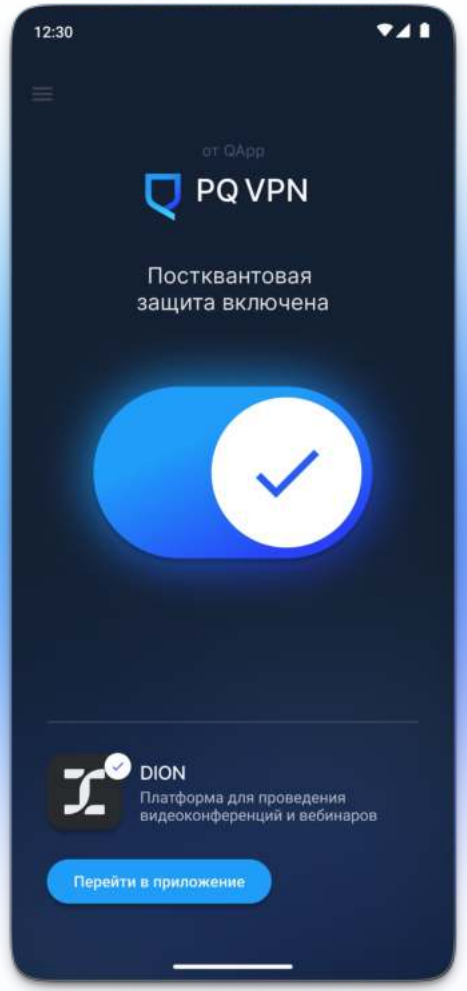
- Проведена доработка продукта в связи с изменениями в архитектуре браузеров на основе Chromium
- Стабилизирован код

Продукт уже пилотируется

ГАЗПРОМБАНК НСПК Ростех

Подробнее о продукте

PQ VPN — ПО для построения квантово-устойчивых виртуальных частных сетей



Решаемые продуктом задачи:

- шифрование трафика на сетевом уровне с помощью ключа получаемого на основе постквантовых алгоритмов распределения ключей
- защита канала с применением как классических, так и постквантовых алгоритмов ЭЦП от атаки посредника
- аутентификация доступа к виртуальной частной сети с применением классических и постквантовых ЭЦП

Комплект поставки включает: серверную часть, отвечающую за приём входящих соединений и контроль доступа к сети, и клиентскую часть, реализованную в виде мобильного приложения для ОС Android и настольного приложения для ОС семейства Windows и ОС на основе gnu/linux(включая Astra linux)

Продукт уже пилотируется

ВТБ

Т1

Продукт представлен на профильных мероприятиях

ФОРУМ БУДУЩИХ ТЕХНОЛОГИЙ

КИБЕРБЕЗОПАСНОСТЬ В ФИНАНСАХ

конференция РусКрипто

FINOPOLIS

МУЗЕЙ КРИПТОГРАФИИ

НФО БЕРЕГ

STARTUP VILLAGE

PQCA — автоматизация работы квантово-устойчивого удостоверяющего центра

Решаемые продуктом задачи:

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

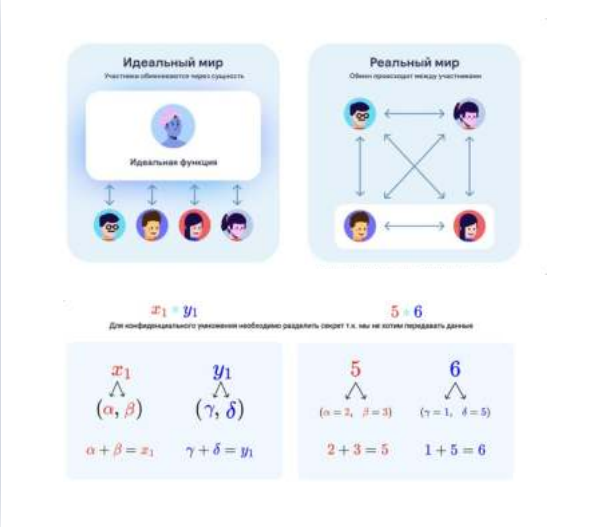
Разрабатывается как для решения задач внешних клиентов, так и для внутреннего использования в QApp

Сделано:

- Разработана продуктовая концепция
- Разработаны требования предъявляемые к решению и его архитектура
- Работоспособный прототип продукта подготовлен к пилотированию
- Пакет поставки продукта готов к передаче заказчикам
- Подана заявка на РИД

PQCompute — ядро платформы конфиденциальных вычислений

Конфиденциальные вычисления позволяют совместно проводить вычисления над данными различных участников без фактической передачи данных другим участникам вычислений



ГАЗПРОМБАНК

Наработки уже используются
в коммерческом проекте
в интересах Банка ГПБ

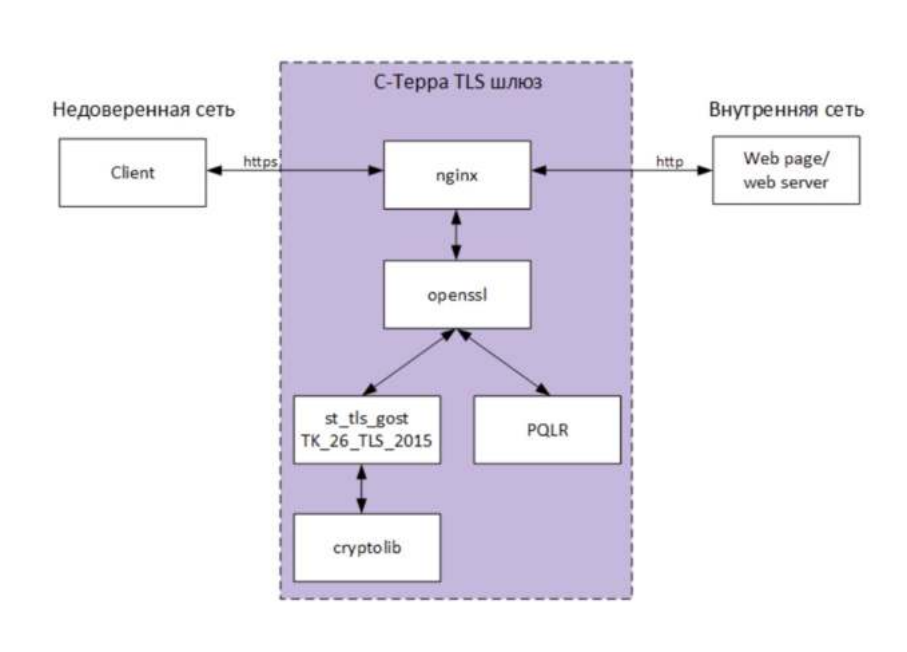
Решаемые продуктом задачи:
Ведение конфиденциального обмена данными с внешними поставщиками
для решения задач Банка ГПБ и других компаний Группы Газпром, включая:

- решение задач выдачи кредитных предложений без запроса согласия пользователей на обработку персональных данных
- упрощение проведения пилотных проектов с внешними поставщиками данных
- возможность монетизировать данные без их передачи

Сделано в 2023:

- Разработана продуктовая концепция
- Продуктовая концепция свалидирована с представителями Банка ГПБ
- Разработан прототип, показывающий реализуемость решения
- Проведена оценка пределов вертикального масштабирования решения
- Выполнена оценка производительности решения и требований к инфраструктуре
- Подготовлена заявка на РИД

PQ GATE — квантово-устойчивый TLS-шлюз



Решаемые продуктом задачи:

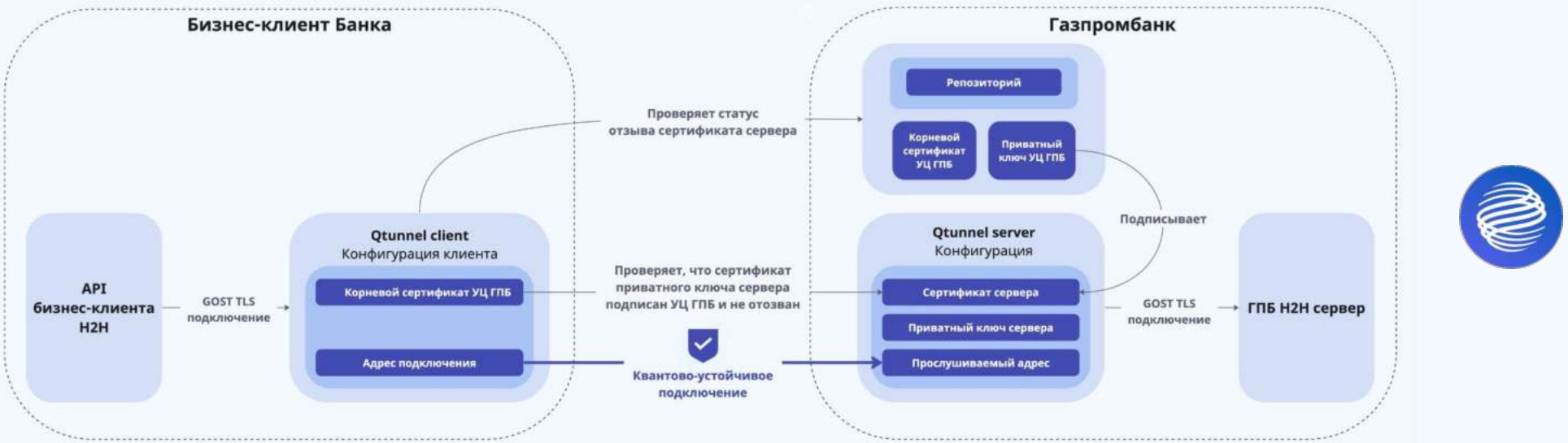
Квантово-устойчивая защита доступа к веб-порталам и корпоративным приложениям

Сделано 2022-2023:

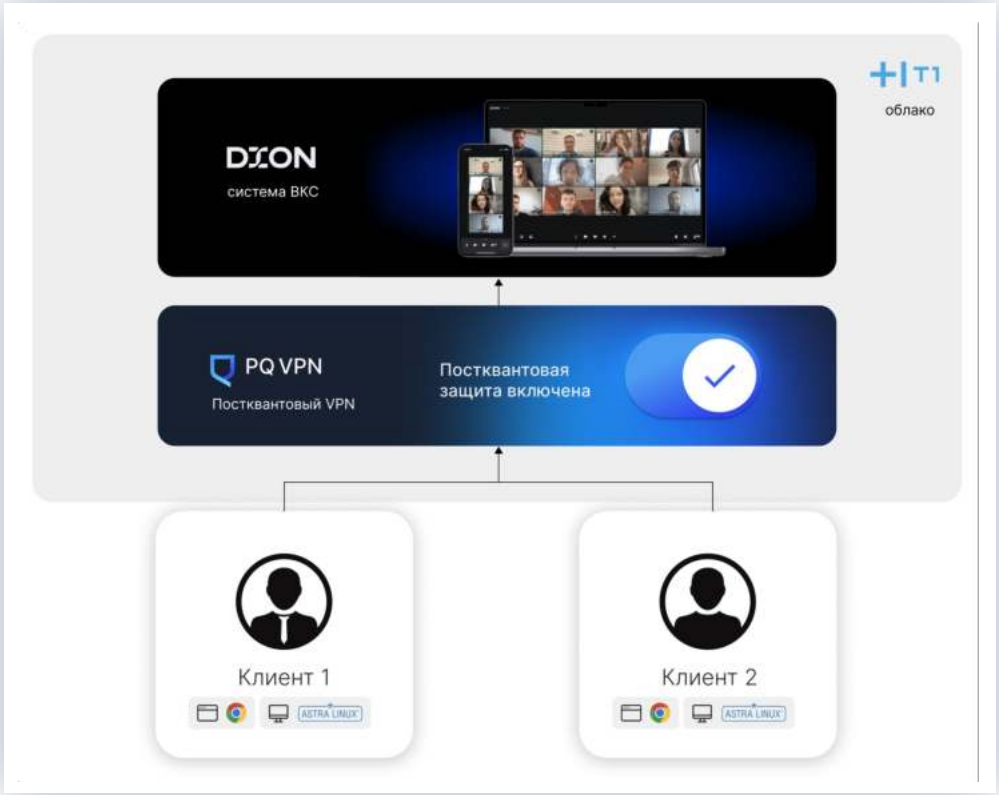
- Разработана продуктовая концепция
- Разработан прототип совместного решения
- Валидируется спрос

Квантово-устойчивая защита каналов host-to-host Газпромбанка и ГК Ростех

Защищаемые данные: платёжные поручения



Постквантовое шифрование в платформе видеоконференций «DION» Группы Т1



Защищаемые данные: видео и аудио-коммуникации

КИБЕРБЕЗОПАСНОСТЬ В ФИНАНСАХ
УРАЛЬСКИЙ ФОРУМ

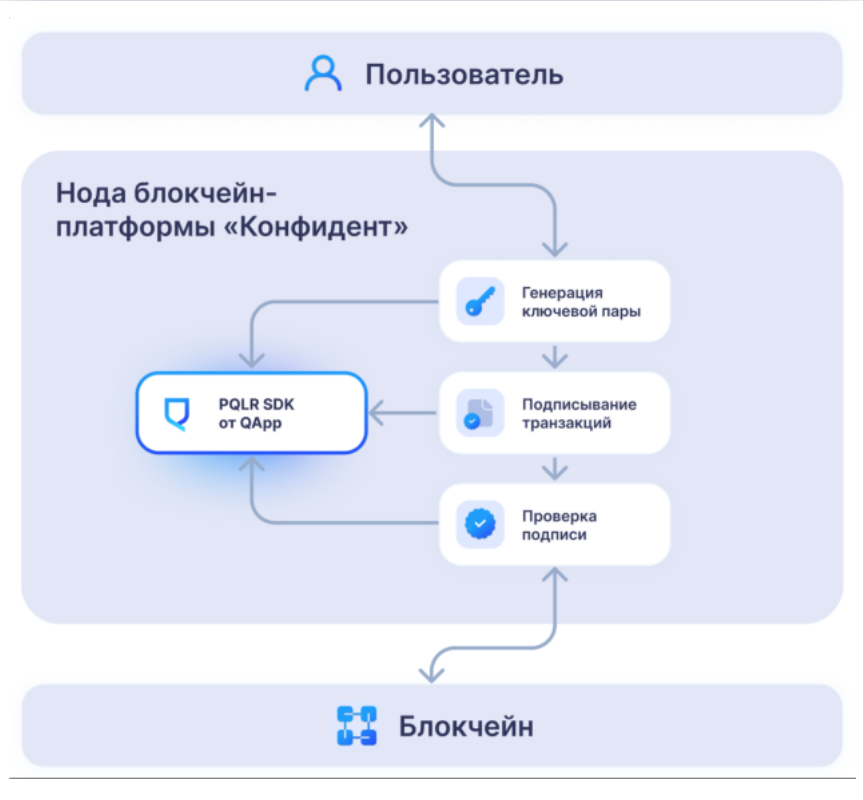
FINOPOLIS

Результаты проекта представлены
Председателю Банка России Набиуллиной Э.С.

[Пресс-релиз]

[Подробнее о проекте]

Постквантовое шифрование в блокчейн-платформе «Конфидент»



Защищаемые данные: данные государственных и корпоративных информационных систем

АССОЦИАЦИЯ БАНКОВ РОССИИ

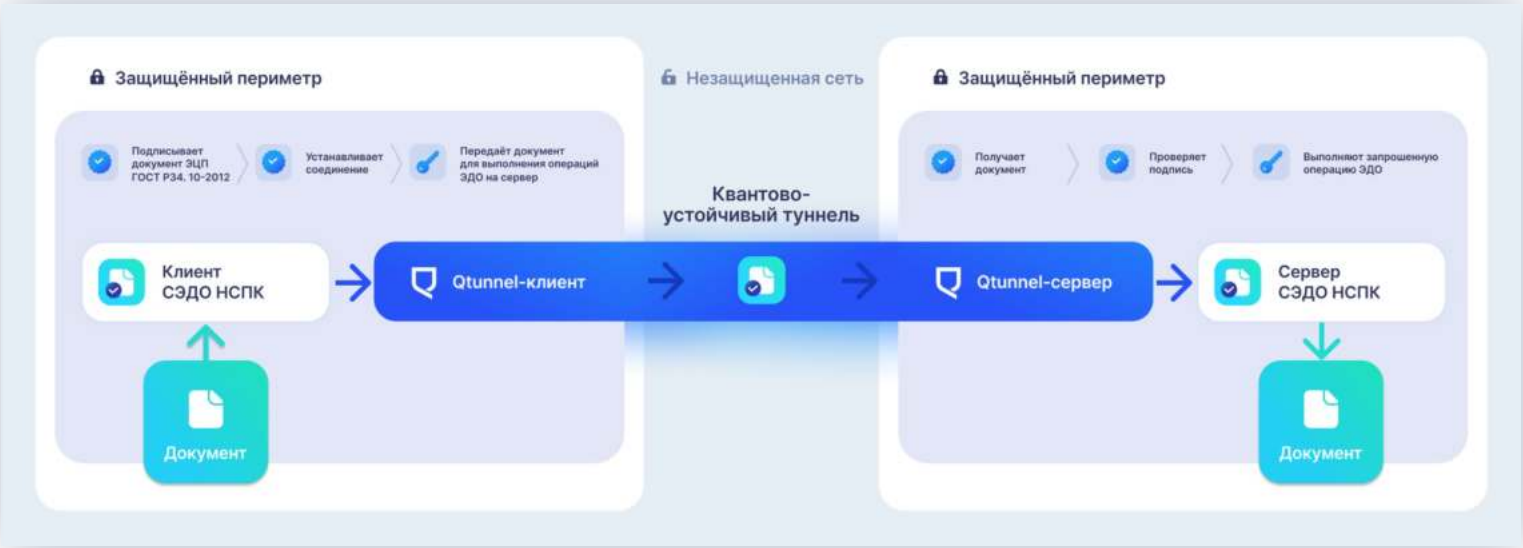
Результаты проекта представлены на XX Международном банковском форуме 2023

ТАСС

Пресс-релиз Подробнее о проекте

Постквантовое шифрование документооборота Национальной системы платежных карт

Защищаемые данные: Клиринг, транзакционные отчеты, отчеты по нетто-позиции, диспутная и другая информация



FINOPOLIS

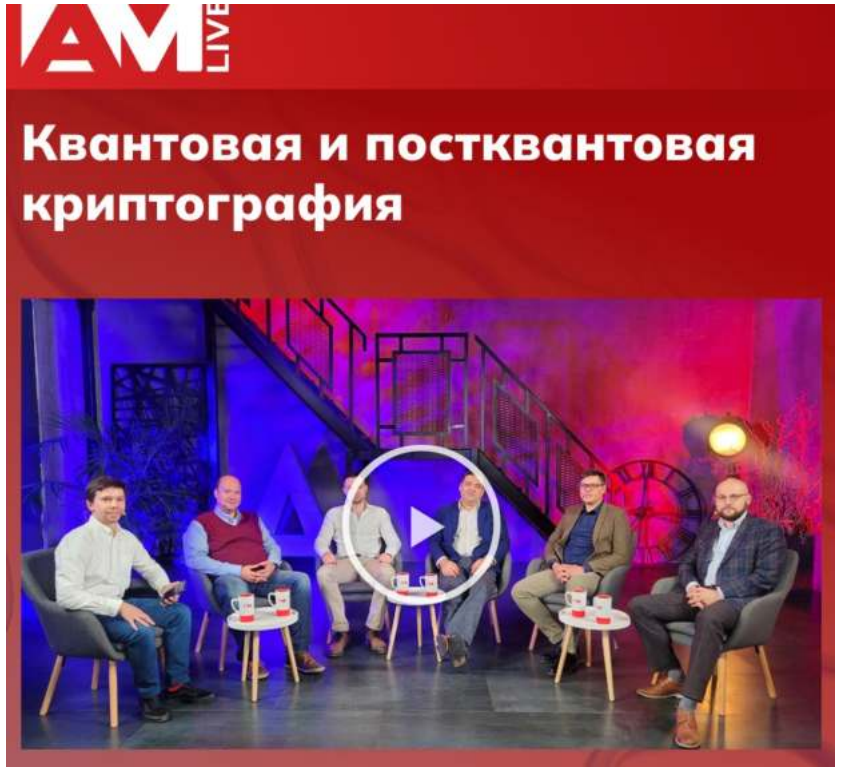
Результаты проекта представлены Председателю Банка России Набиуллиной Э.С.

[Пресс-релиз](#) [Подробнее о проекте](#)

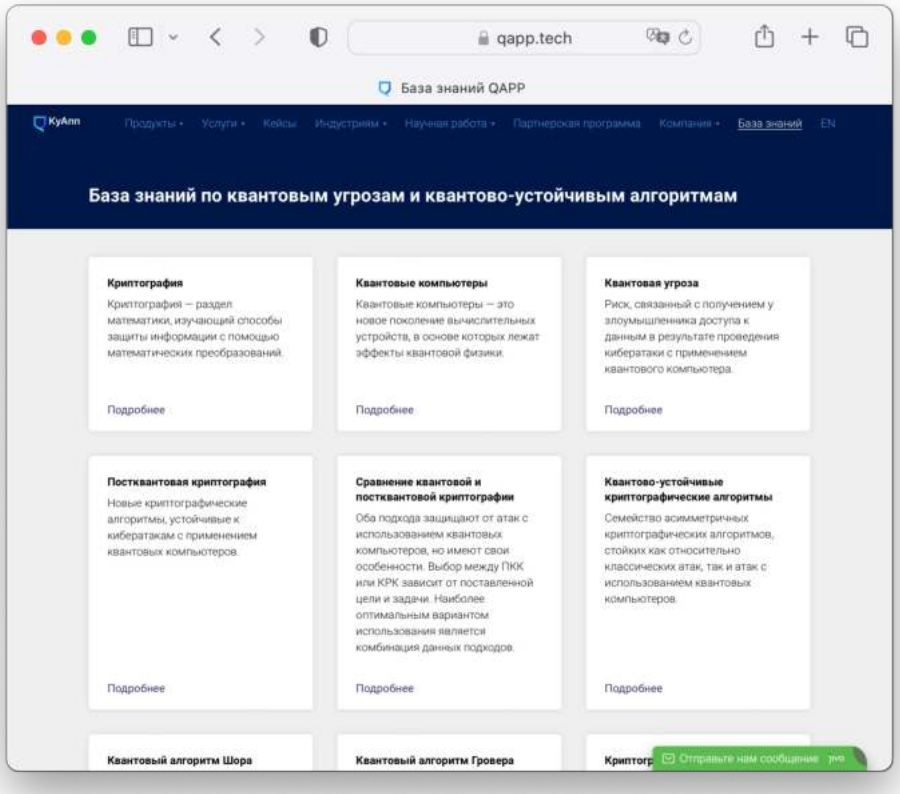
Отличие постквантовой криптографии от квантовой криптографии

	Квантовая криптография	Постквантовая криптография
Область применения	Распределение симметричного ключа	Асимметричное шифрование, схемы цифровой подписи, механизмы инкапсуляции ключа
Безопасность	Основана на законах квантовой механики	Основана на математических предположениях, проверенных временем
Реализация	Аппаратная	Программная, но может быть ускорена аппаратно
Стоимость	Высокая цена из-за использования специализированного оборудования	Невысокая, так как основные решения являются программными
Сертификация	Проекты ETSI, ISO, ITU-T	Технический комитет 26 и конкурсы NIST, CACR
Коммуникация	В основном используются волоконно-оптические линии связи (ВОЛС). На данный момент соединение между двумя точками ограничено 100 км при использовании оптоволоконных линий связи и практически не ограничено при использовании атмосферных оптических линий связи (АОЛС)	Может использоваться в любых цифровых типах коммуникации (беспроводные сети, оптические каналы и т.д.) на любом расстоянии

Подробнее о постквантовых алгоритмах



Подкаст с ведущими вендорами РФ



База знаний QApp

QApp

Антон Гугля
Генеральный директор

Email: apg@rqc.ru

Телефон: +7 925 537-71-53

Telegram: @tonguglya

QApp.tech

Sk КиберХаб