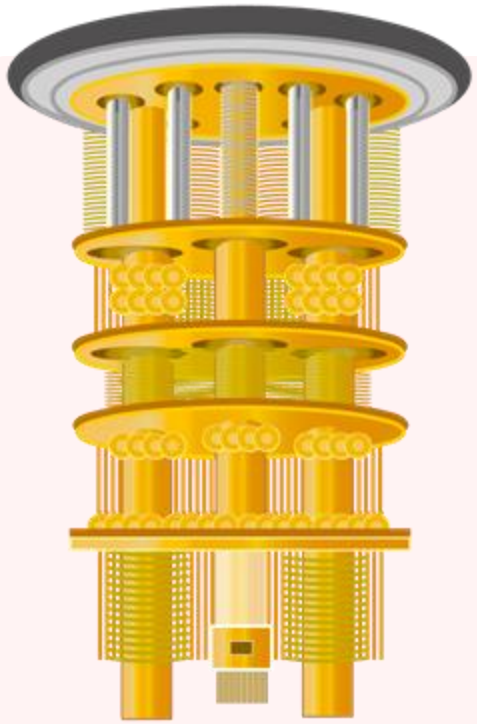
QApp

Постквантовая криптография

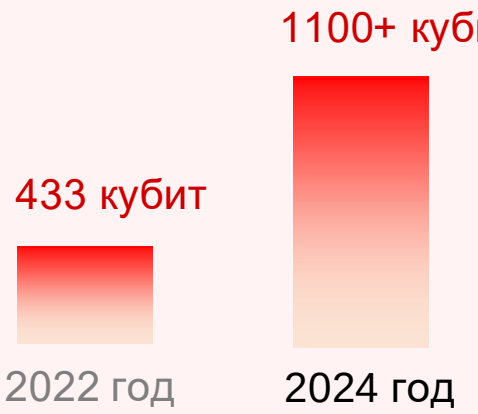
Защита данных компаний финансовой отрасли от киберугроз настоящего и ближайшего будущего

Антон Гугля
Генеральный директор QApp

Квантовый компьютер в руках злоумышленника — новый риск для кибербезопасности государства и бизнеса («квантовая угроза»)



Мощность квантовых компьютеров растет каждый год



С помощью мощных квантовых компьютеров злоумышленники смогут получить доступ к данным, защищенным традиционными алгоритмами шифрования

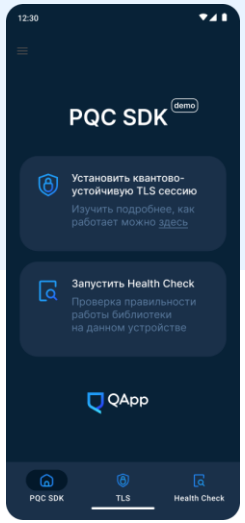
Множество существующих сегодня алгоритмов криптографии неустойчивы к «квантовой угрозе»

Распределение ключей	Асимметричное шифрование	Электронная подпись

«Квантовая угроза» становится актуальнее с каждым годом

Постквантовая криптография — научно-технологический подход защиты данных от «квантовой угрозы»

Новый класс асимметричных алгоритмов шифрования, устойчивых к кибератакам с применением как классических, так и квантовых компьютеров



Новая математика, но традиционный стек технологий реализации продуктов

Интеграция без модификации аппаратной инфраструктуры бизнес-клиента

Поддержка популярных платформ и протоколов

QApp

Постквантовая криптография позволяет защитить широкий спектр данных

Пользовательские данные

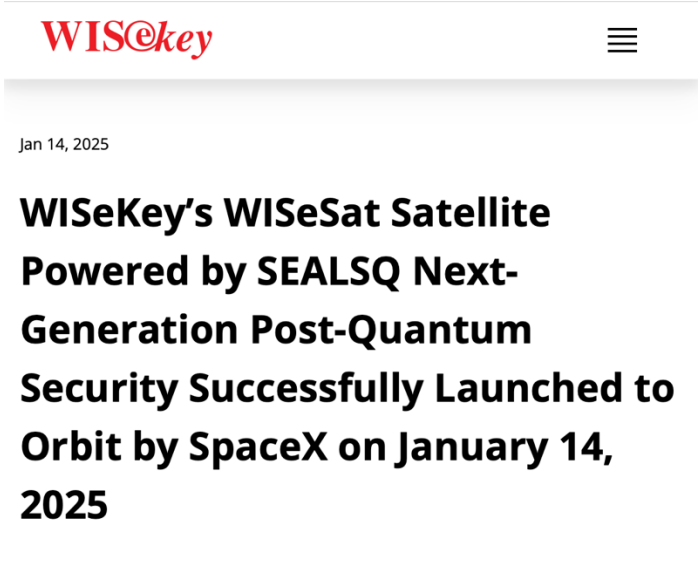
Внутренние и внешние коммуникации

Электронный документооборот

Хранение данных

Аутентификация

Яркие примеры развития регуляторики и пилотных интеграций на глобальном рынке



В США приняли первые госстандарты по постквантовым алгоритмам

Еврокомиссия разрабатывает дорожную карту по переходу на постквантовые алгоритмы

Отечественные продукты ИБ на основе постквантовой криптографии – комплексная защита от «квантовой угрозы»

Конечные продукты

- Квантово-устойчивый ВКС
- Квантово-устойчивый блокчейн
- Квантово-устойчивый TLS-шлюз

Постквантовая защита данных в процессе передачи

Квантово-устойчивые виртуальные частные сети

Образовательная платформа по постквантовой криптографии

Системные решения

Библиотека постквантовых алгоритмов и средства упрощающие их интеграцию

Аппаратное ускорение постквантовых алгоритмов

Инфраструктура квантово-устойчивого удостоверяющего центра

Постквантовые алгоритмы-кандидаты на включение в новые проекты государственных стандартов

гиперикум

Другие алгоритмы

В России проводится множество исследований по постквантовой криптографии и разрабатываются новые государственные стандарты

ТК 26

Ведется разработка новых госстандартов в Техническом комитете (ТК26) Росстандарта

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Академия криптографии Российской Федерации

Ведутся исследования

Минцифры России

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

Безопасность данных. Необходимо продолжить работу над технологиями квантовых коммуникаций и квантового шифрования. Они помогают отражать любые кибератаки, как классические, так и с применением квантовых компьютеров. Благодаря таким технологиям системы безопасности страны будут неуязвимы для взлома.

ФОРУМ БУДУЩИХ ТЕХНОЛОГИЙ

Постквантовые решения представлены **Президенту РФ**

Постквантовая криптография включена в стратегические сессии по перспективным ИБ-технологиям

МОСКВА 2030 умный город

Московский инновационный кластер

ЦИФРОВАЯ ЭКОНОМИКА

A2024

SafeNet

QApp

Финансовый сектор России проводит наибольшее количество пилотных проектов и прикладных исследований по постквантовой криптографии

Банк России

СБЕР БАНК

ГАЗПРОМБАНК

ВТБ

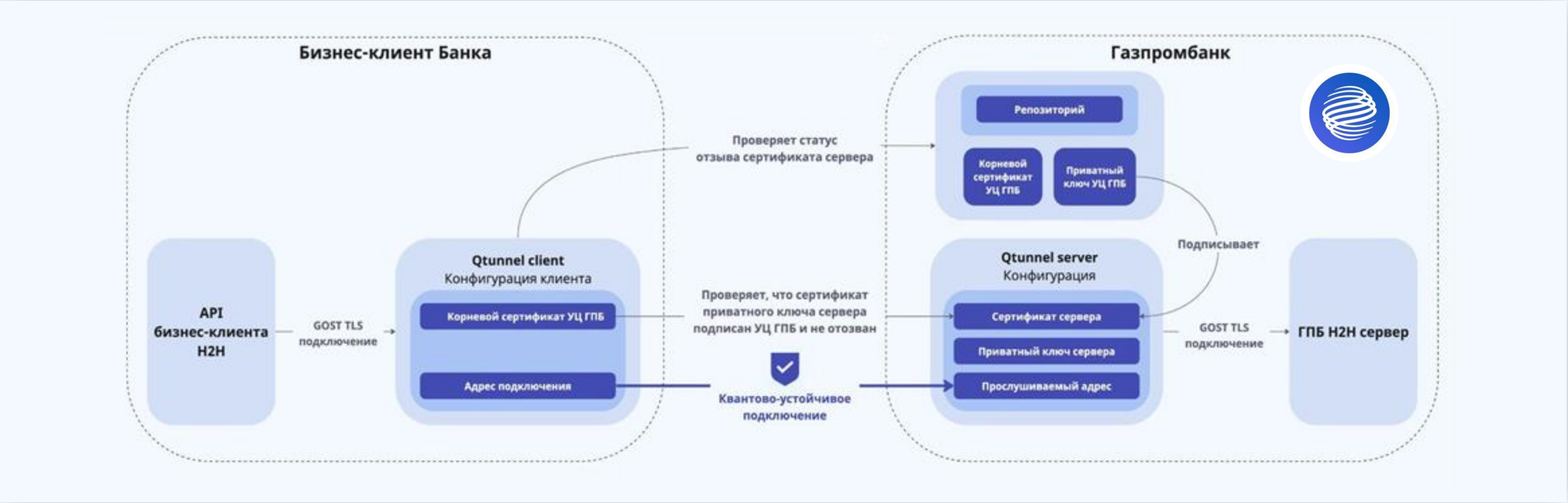
АССОЦИАЦИЯ ФИНТЕХ

НСПК

MOEX МОСКОВСКАЯ БИРЖА

Пилотный проект завершен. Масштабирование опыта

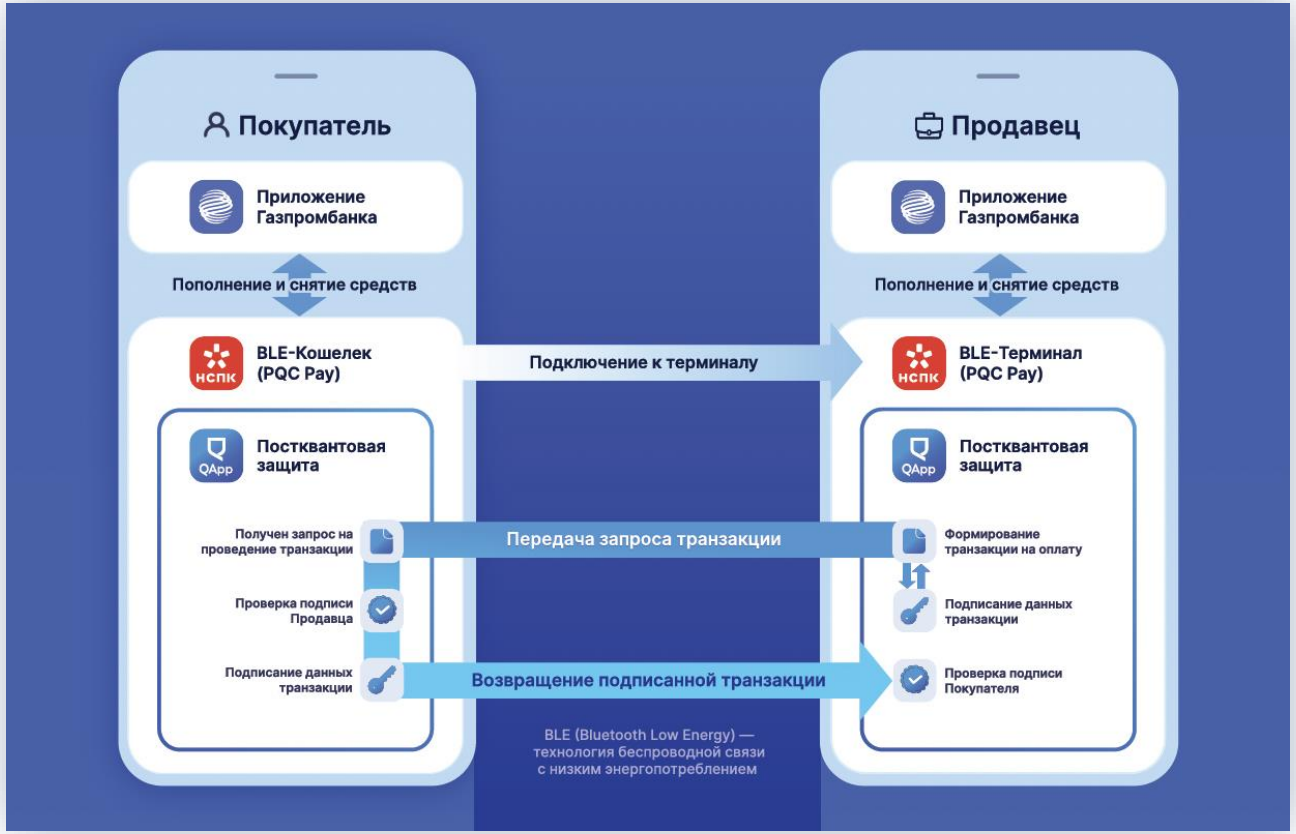
Постквантовое шифрование каналов host-to-host Газпромбанка и его бизнес-клиентов



Проект-победитель всероссийской премии
RB Digital Award

Пилотный проект завершен

Квантово-устойчивые мобильные BLE-платежи Национальной системы платежных карт

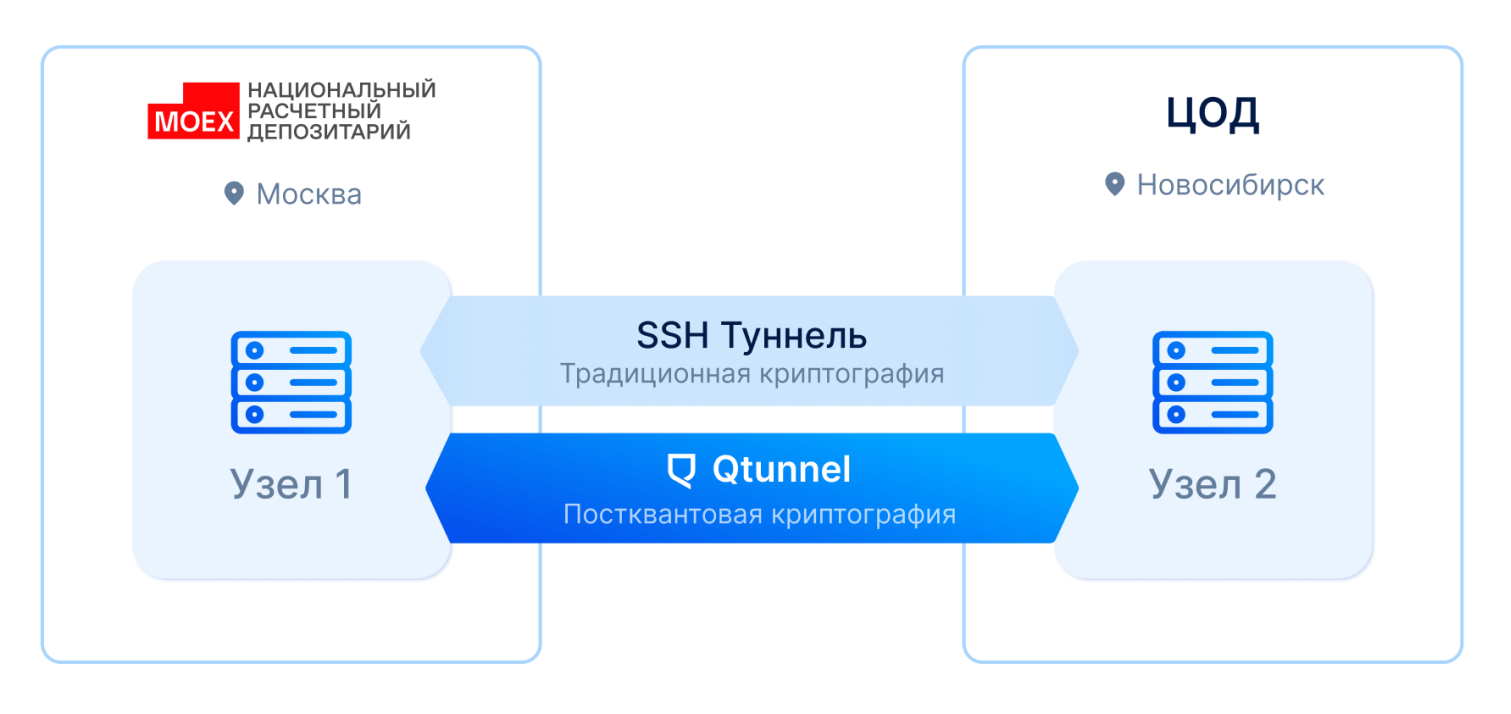


FINOPOLIS

Результаты проекта представлены
Председателю Банка России Набиуллиной Э.С.
в рамках FINOPOLIS 2024

Пилотный проект завершен

Постквантовое шифрование канала передачи резервных копий данных Московской биржи



Реализация квантово-устойчивого туннеля между двумя удаленными площадкам Московской биржы для передачи зашифрованных резервных копий данных больших размеров

QApp

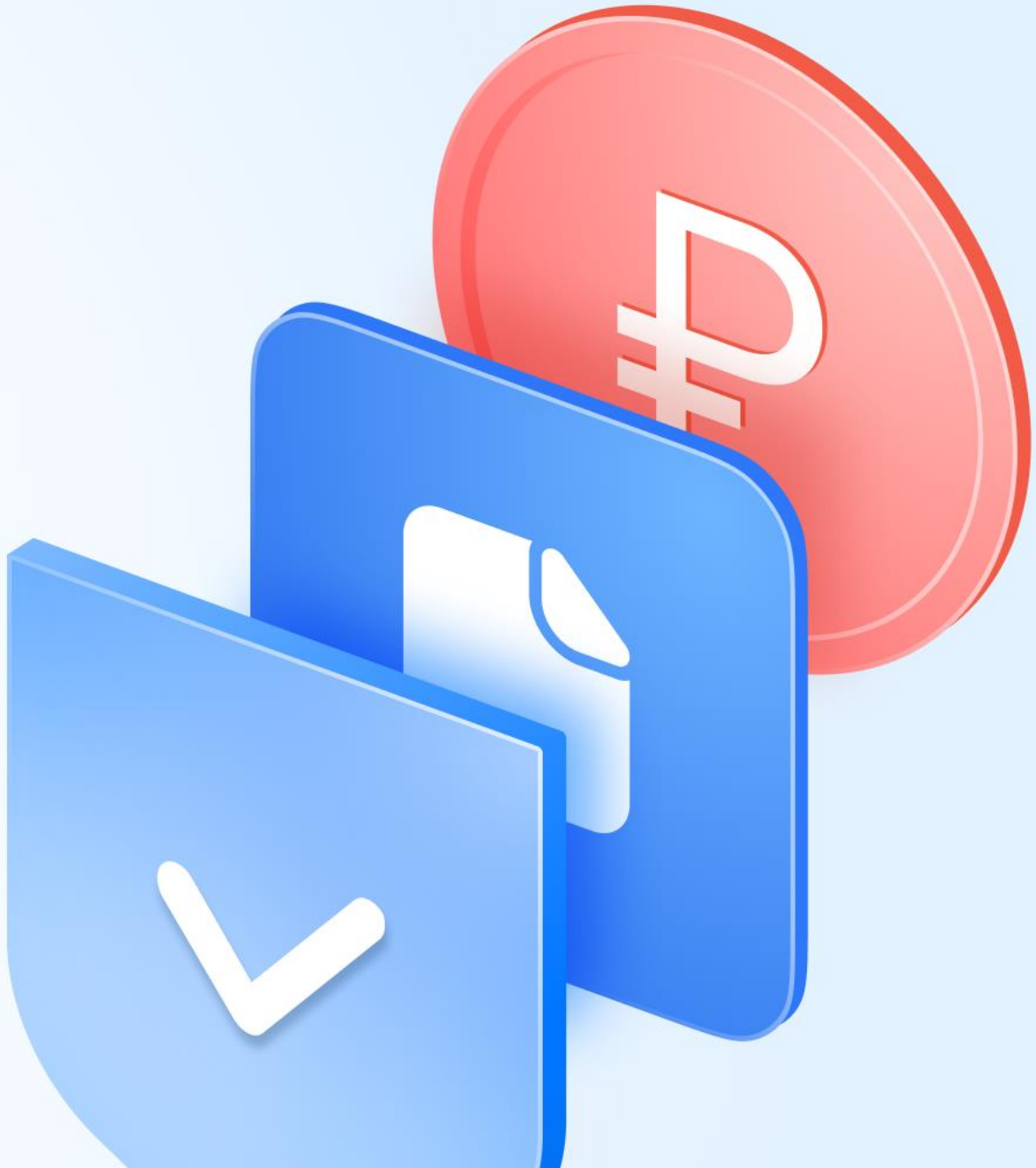
Антон Гугля
Генеральный директор QApp

Email: apg@rqc.ru

Телефон: +7 925 537-71-53

qapp.tech

Sk Участник



Компания QApp — разработчик программных решений кибербезопасности на основе постквантовых алгоритмов и конфиденциальных вычислений

Спинофф Российского квантового центра

Лауреат всероссийских премий и конкурсов ИТ-продуктов

Участник КиберХаба Сколково

При стратегической поддержке Газпромбанка

Разработчик новых госстандартов по постквантовой криптографии в РФ (ТК26 Росстандарта)

Активный участник рабочих групп Национального Технологического центра цифровой криптографии

Получена лицензия регулятора

34 сотрудника

8 цифровых продуктов

Продукты и услуги уже пилотируются

Банк России, СБЕР, ГАЗПРОМБАНК, ВТБ, эльбрус, Baikal Electronics, s•terra, QRATE, НСПК, T1, web3 tech, Ассоциация ФинТех, positive technologies, MOEX Московская Биржа