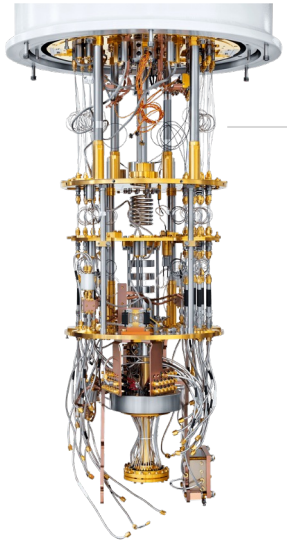
QApp

Квантово-устойчивая защита данных финансовой отрасли

Антон Гугля, генеральный директор QApp

QApp.tech

КВАНТОВАЯ УГРОЗА – НОВЫЙ РИСК КИБЕРБЕЗОПАСНОСТИ ФИНАНСОВОЙ ОТРАСЛИ



Квантовые компьютеры активно развиваются год от года

Уже доступны через облако

16 кубит в РФ

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

Распространенные сегодня алгоритмы шифрования неустойчивы к квантовой угрозе:

Распределение ключей	Асимметричное шифрование	Электронная подпись

КВАНТОВАЯ УГРОЗА УСИЛИВАЕТ КЛЮЧЕВЫЕ РИСКИ КИБЕРБЕЗОПАСНОСТИ ФИНАНСОВЫХ ИНСТИТУТОВ

Сетевая инфраструктура

Стандартное программное обеспечение

Блокчейн-решения

- Финансовые риски при судебных издержках при обнаружении кражи данных
- Упущенная коммерческая выгода
- Репутационные риски, включая шантаж организации расшифрованным трафиком
- Фрод по платежам, подмена реквизитов…

ДАННЫЕ С ДЛИННЫМ ЖИЗНЕННЫМ ЦИКЛОМ УЖЕ СЕЙЧАС ПОДВЕРЖЕНЫ КВАНТОВОЙ УГРОЗЕ

ГОСУДАРСТВА ПРИЗНАЮТ АКТУАЛЬНОСТЬ КВАНТОВОЙ УГРОЗЫ И НАЧИНАЮТ АПРОБАЦИЮ КВАНТОВО-УСТОЙЧИВЫХ РЕШЕНИЙ

Мир

Президент Байден подписал меморандум о рисках квантовых компьютеров для криптографических систем и о мероприятиях по управлению этими рисками

Правительство США опубликовало меморандум о подготовке к переходу всех госорганов на квантово-устойчивые решения

Центр кибербезопасности НАТО завершил тестирование квантово-устойчивого VPN

NCCoE отобрал компании на глобальном рынке, ответственные за «национальную миграцию» на квантово-устойчивые решения

Россия

Разрабатываются стандарты по постквантовой криптографии в рамках Технического комитета ТК26

НТЦ ЦК

Минцифры России

Реализуются научно-исследовательские проекты по постквантовой криптографии в рамках Национального Центра Цифровой Криптографии РФ

ЦЕННЫЕ ДАННЫЕ ТРЕБУЮТ ЗАЩИТЫ НОВЫМИ ИНСТРУМЕНТАМИ

Пользовательские данные

Внутренние и внешние коммуникации

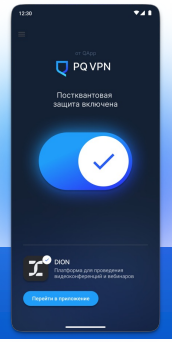
Хранение данных

Электронный документооборот

Аутентификация

КВАНТОВАЯ КРИПТОГРАФИЯ

Аппаратные решения квантового распределения ключей. Безопасность обеспечивается законами физики



ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ

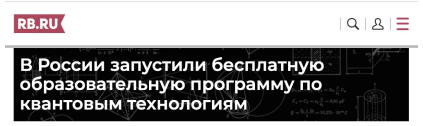
Программные решения защиты данных. Безопасность обеспечивается новыми математическими подходами

СИНЕРГИЯ ТЕХНОЛОГИЙ — КВАНТОВО-УСТОЙЧИВАЯ КИБЕРБЕЗОПАСНОСТЬ НА ВСЕХ УРОВНЯХ РАБОТЫ С ДАННЫМИ

УРОВНИ ЗАЩИТЫ ДАННЫХ		КВАНТОВАЯ КРИПТОГРАФИЯ	ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ
ПЛАТФОРМЫ	Комплексные IT-системы	✓	✓
ДАТА-ЦЕНТРЫ	Критическая инфраструктура	✓	✓
ИНФРАСТРУКТУРА	Каналы коммуникации, VPN, 5G	✓	✓
ПРИЛОЖЕНИЯ	Мобайл, Веб, Десктоп		✓

ОПЫТ ИНДУСТРИИ. ПИЛОТИРОВАНИЕ ТЕХНОЛОГИЙ КВАНТОВЫХ КОММУНИКАЦИЙ И ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

Банк России



Квантовые коммуникации

СБЕР БАНК

ГАЗПРОМБАНК

Постквантовая криптография

ГАЗПРОМБАНК

ВТБ

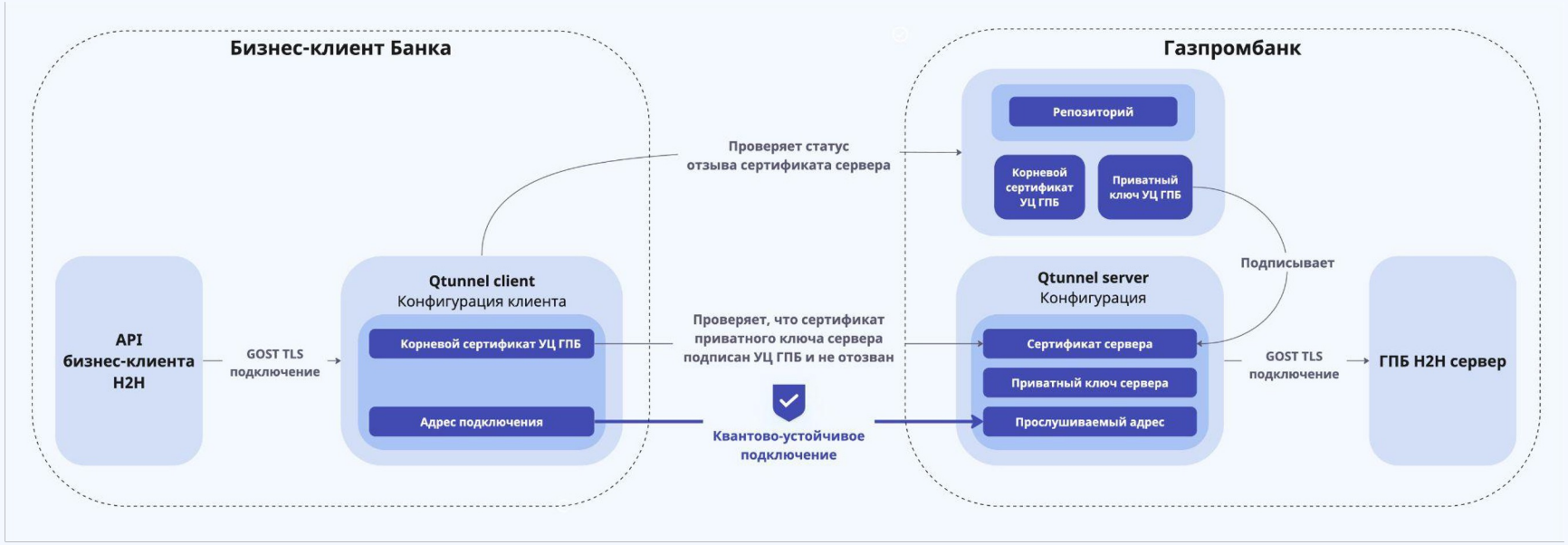
+I

НСПК

waves

MASTER CHAIN

ОПЫТ ИНДУСТРИИ. ПИЛОТ ПО КВАНТОВО-УСТОЙЧИВОЙ ЗАЩИТЕ КАНАЛОВ HOST-TO-HOST ГАЗПРОМБАНКА



Пилотировалось решение:

Qtunnel — программный продукт компании QApp для реализации квантово-устойчивых соединений в сетях различных топологий

Результаты пилотного проекта удостоены всероссийских наград

ОПЫТ ИНДУСТРИИ. ПИЛОТ ПО КВАНТОВО-УСТОЙЧИВОМУ ВКС-СЕРВИСУ С ГРУППОЙ Т1/ДИОН И БАНКОМ ВТБ

Пилотировалось решение:

Qtunnel — программный продукт компании QApp для реализации квантово-устойчивых соединений в сетях различных топологий

КИБЕРБЕЗОПАСНОСТЬ В ФИНАНСАХ
УРАЛЬСКИЙ ФОРУМ

ЦЕННОСТЬ ПИЛОТИРОВАНИЯ КВАНТОВО-УСТОЙЧИВЫХ РЕШЕНИЙ ДЛЯ ФИНАНСОВОЙ ОТРАСЛИ

- **Оценка затрат на ввод в промышленную эксплуатацию**

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

Считаю необходимым продолжить работу над технологиями квантовых коммуникаций и квантового шифрования. Такие технологии обеспечивают устойчивость информационных систем к кибератакам с применением как классических, так и квантовых компьютеров, позволяют создать неуязвимые для взлома системы, а также развивать защищённую квантовую связь. Кстати, по этому направлению Россия в числе лидеров.

Владимир Владимирович Путин
Президент Российской Федерации

ФОРУМ БУДУЩИХ ТЕХНОЛОГИЙ

В рамках пленарного заседания Форума будущих технологий «Вычисления и связь. Квантовый мир»

QApp

Антон Гугля

Генеральный директор QApp

Email: apg@rqc.ru

Телефон: +7 925 537-71-53

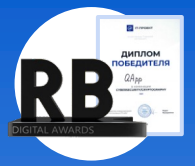
Telegram: @tonguglya

QApp.tech

Sk КиберХаб

РКЦ | Российский Квантовый Центр

КУАПП — РАЗРАБОТЧИК ПРОГРАММНЫХ РЕШЕНИЙ НА ОСНОВЕ ПОСТКВАНТОВОГО ШИФРОВАНИЯ

- Спинофф Российского квантового центра
- 

Лауреат всероссийских премий и конкурсов ИТ-продуктов
- Участник Кибекластера Сколково
- При стратегической поддержке Газпромбанка
- Разработчик стандартов постквантовой криптографии в РФ
- Научная деятельность поддержана институтами развития РФ

23 сотрудника

6 цифровых продуктов

Продукты и услуги уже пилотируются

Банк России · СБЕР · ГАЗПРОМБАНК · ВТБ · Baikal Electronics · МЦСТ Эльбрус · s•terra · QRATE · T1

ОТЛИЧИЕ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ ОТ КВАНТОВОЙ КРИПТОГРАФИИ

	Квантовое распределение ключей	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