



# Кибербезопасность. Постквантовая криптография

Антон Гугля,  
Генеральный директор

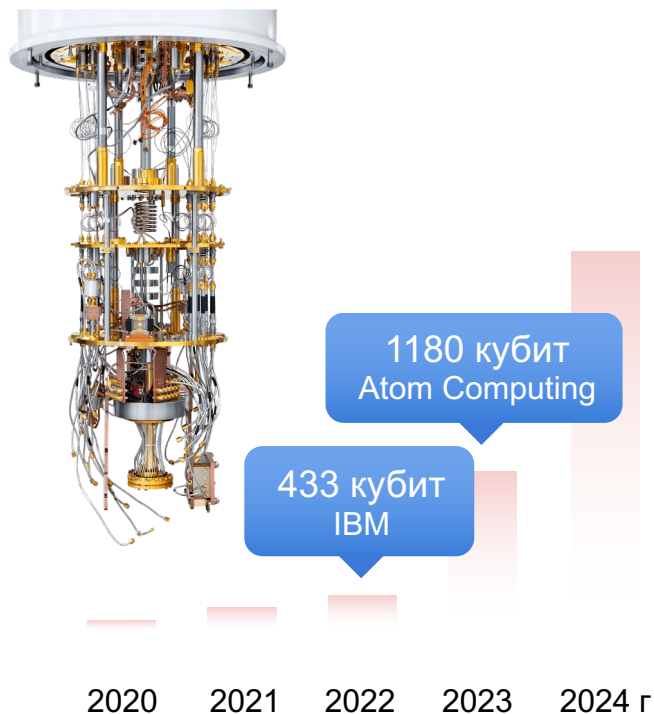


# Квантовая угроза — новый риск для кибербезопасности, который становится актуальнее с каждым годом



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

Квантовые компьютеры уже доступны через облако



## 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.



Не требуется привнесение специализированных аппаратных решений в инфраструктуру в рамках пилотных проектов  
Высокая скорость и простота интеграции



Поддержка популярных платформ и протоколов



Совместимость с отечественными процессорами



Отечественная реализация постквантовых алгоритмов

## Государства признают актуальность квантовой угрозы и начинают апробацию квантово-устойчивых решений



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



Завершается международный процесс выбора наиболее стойких постквантовых алгоритмов



Разрабатываются стандарты по постквантовым алгоритмам в рамках Технического комитета ТК26



НТЦ ЦК



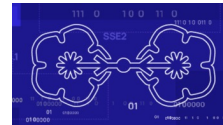
Минцифры  
России

Реализуются научно-исследовательские проекты по постквантовым алгоритмам в рамках Национального технологического центра цифровой криптографии

Опубликованы первые открытые реализации отечественных постквантовых алгоритмов



гиперикум



Финансовая отрасль, вендоры традиционного ИБ  
пилотируют постквантовые алгоритмы



Банк России



эльбрус



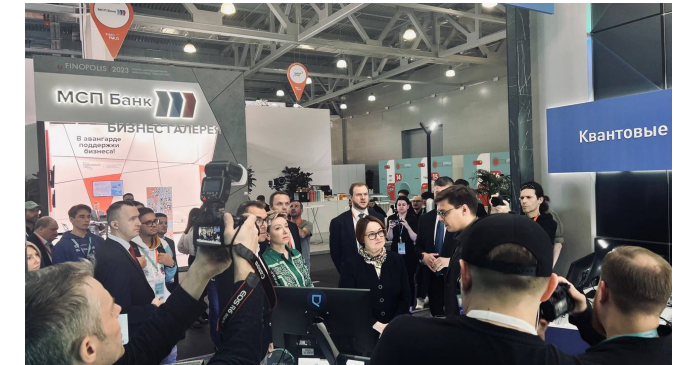
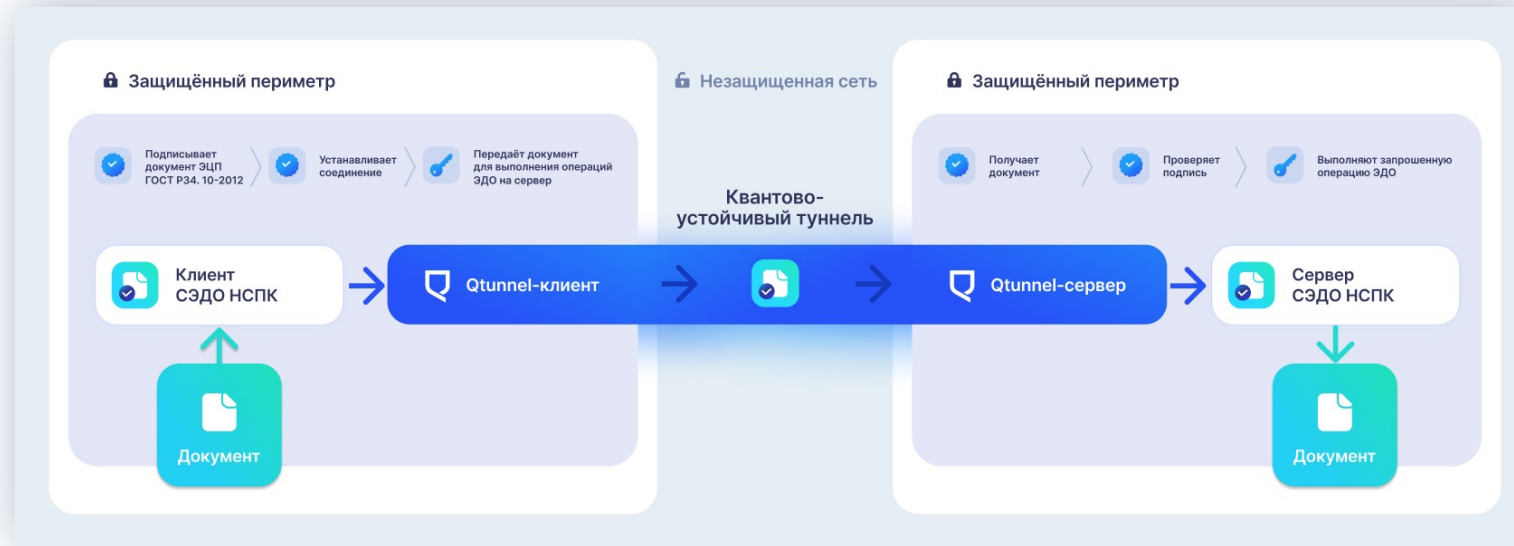
# Постквантовое шифрование документооборота Национальной системы платежных карт



Пилотный интеграционный проект завершен

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

Используемый продукт QApp: Qtunnel



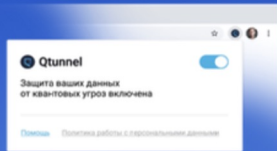
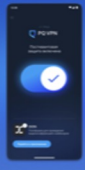
Результаты проекта представлены  
Председателю Банка России  
Набиуллиной Э.С.



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

# Примеры отечественных программных решений на основе постквантовых алгоритмов



|                                                                                   |                                                                                   |                                                                                    |                                                                                     |                                                                                     |                                                                                     |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|  |  |  |  |  |  |
| <b>Гиперикум</b>                                                                  | <b>PQLR SDK</b>                                                                   | <b>Qtunnel</b>                                                                     | <b>PQ VPN</b>                                                                       | <b>PQ PKI</b>                                                                       | <b>PQ СФ-блок</b>                                                                   |
| Постквантовый алгоритм ЭЦП (кандидат на включение в ГОСТ)                         | Библиотека постквантовых алгоритмов                                               | Квантово-устойчивое соединение в корпоративных сетях                               | Постквантовый VPN для корпоративных сетей                                           | Квантово-устойчивый удостоверяющий центр                                            | Аппаратное ускорение постквантовых алгоритмов                                       |

Продукты уже пилотируются

# Компания QApp — лидер в РФ по постквантовым алгоритмам



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)

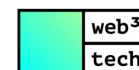


Активный участник рабочих  
групп Национального  
Технологического центра  
цифровой криптографии

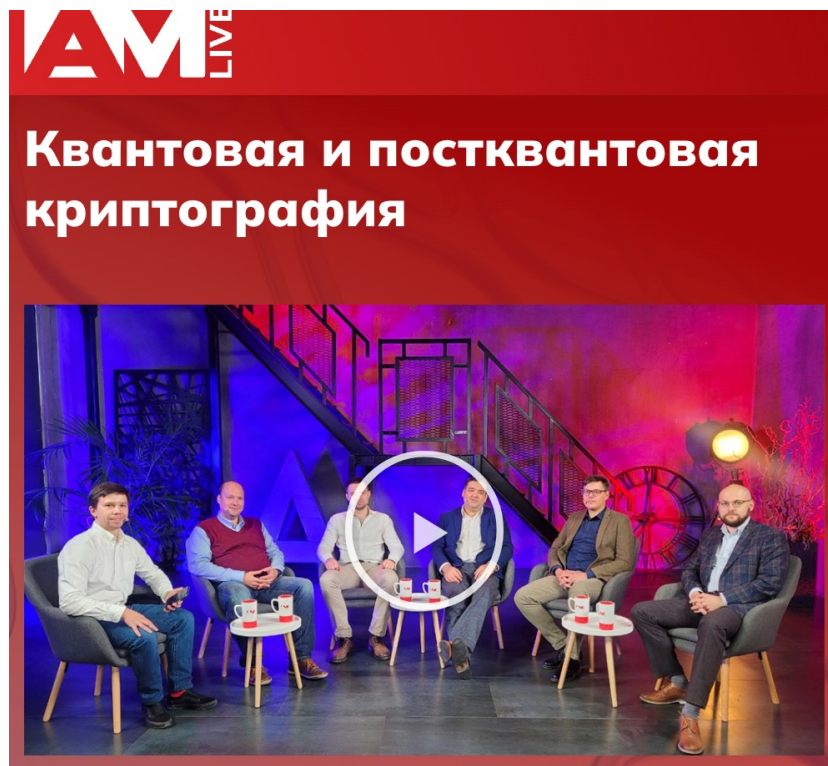
23 сотрудника

6 цифровых продуктов

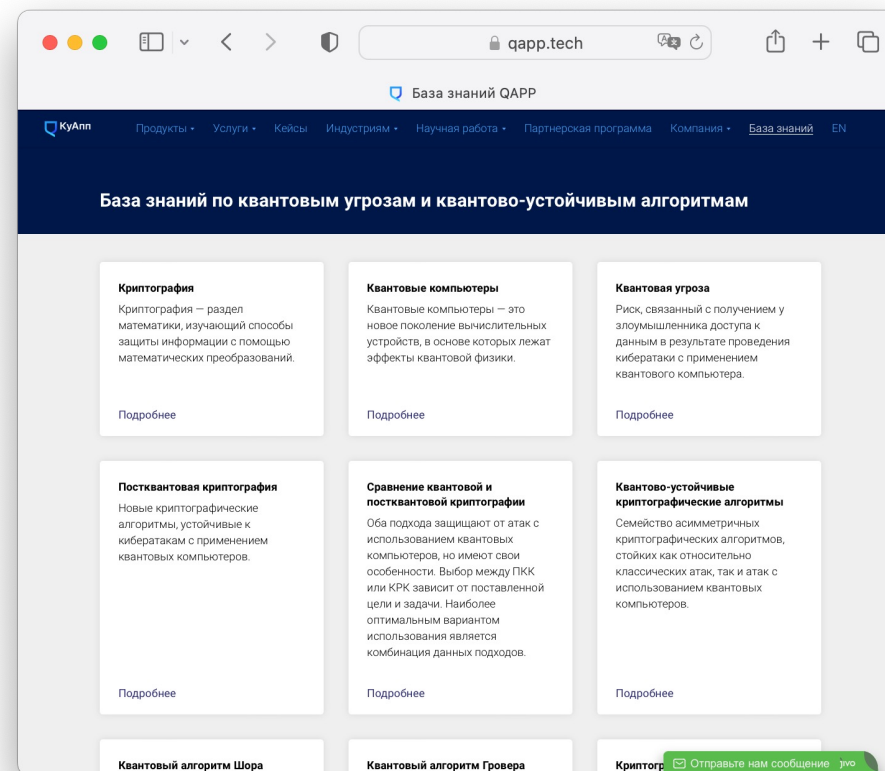
Продукты и услуги уже пилотируются



# Подробнее о постквантовых алгоритмах



[Подкаст с ведущими вендорами РФ](#)



[База знаний QApp](#)



**Антон Гугля**  
Генеральный директор

+7 925 537-71-53  
arg@rqc.ru

**QApp.tech**

