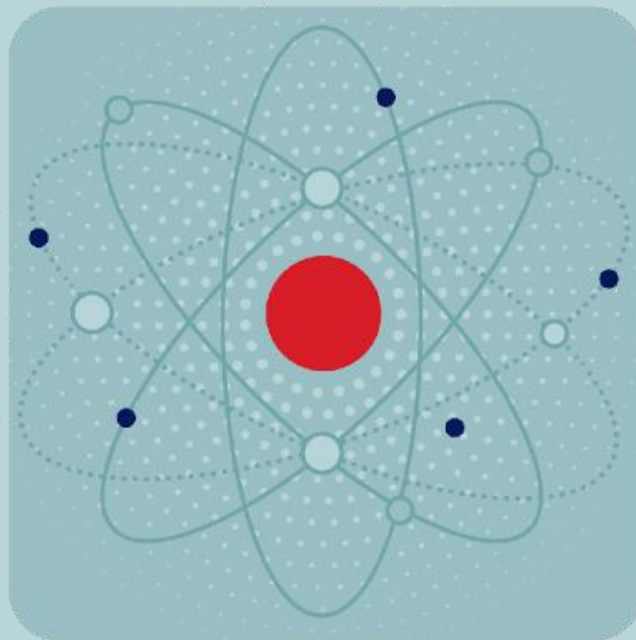


ТЕХНОЛОГИЧЕСКАЯ
ПАРТНЕРСКАЯ КОНФЕРЕНЦИЯ

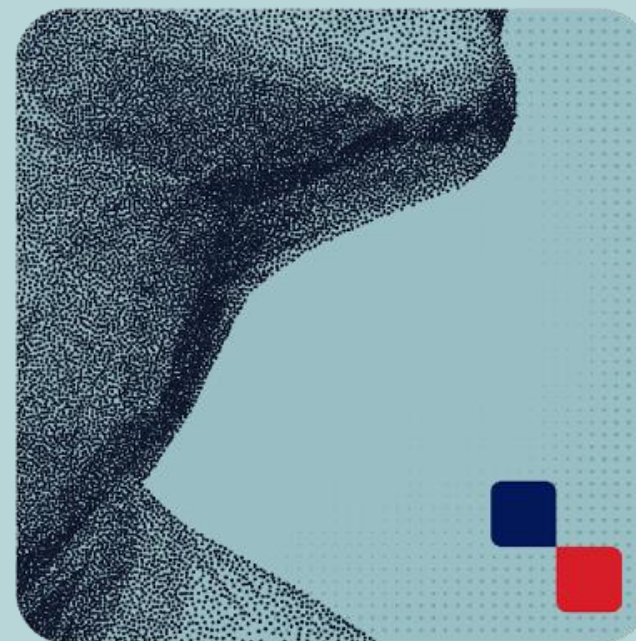
РУТОКЕН ОАЧ ТЕХНОЛОГИИ ДОВЕРИЯ



Мировой рынок постквантовой криптографии: текущий статус и перспективы развития

Ирина
Полтавская

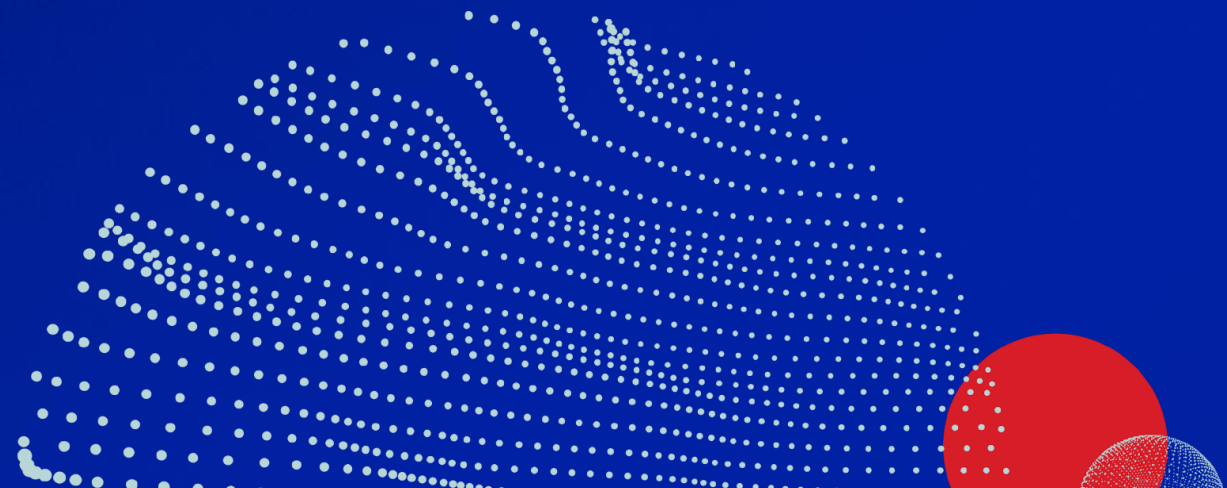
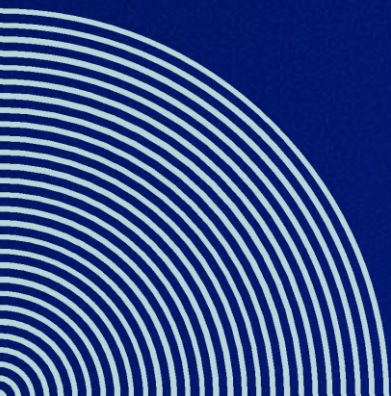
Коммерческий директор QApp,
Российский университет
дружбы народов





1. Постквантовая криптография как объект экономической политики
2. Экономические и регуляторные предпосылки постквантовой миграции
3. Инвестиционный анализ конкурентной среды
4. Образование
5. Индекс готовности к постквантовой миграции
6. Рекомендации для участников рынка

1. Постквантовая криптография как объект экономической политики



Современная криптография с открытым ключом неустойчива к квантовым кибератакам

Сферы под угрозой:



Банковская сфера



Государственные сервисы



Облачные платформы



IoT и блокчейн



Телеком сфера



Киберфизические системы

Оценки показывают значительное снижение требуемой вычислительной мощности для криптографического взлома

1 млрд
кубит ¹



2012 год

1 млн
кубит ²

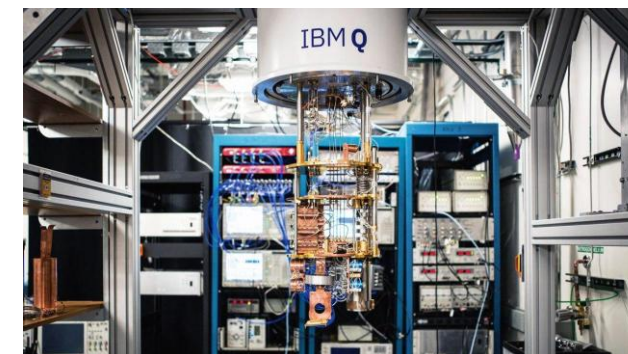


2025 год

10 тыс
кубит ³



2026 год



4

Экономическое значение сбоев защищенных соединений

 **Рост транзакционных издержек**

 **Расходы на ИБ**

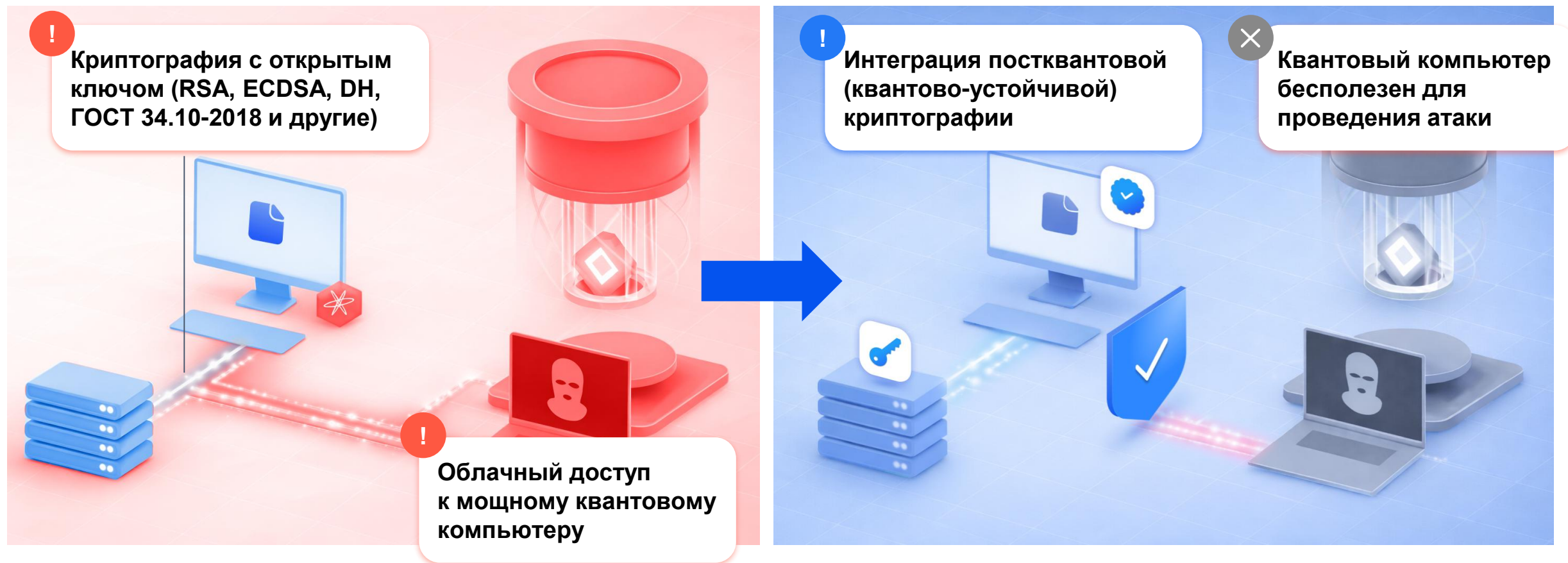
 **Страхование**

 **Аудит**

 **Юридические риски**



Решение: переход на постквантовую защиту данных



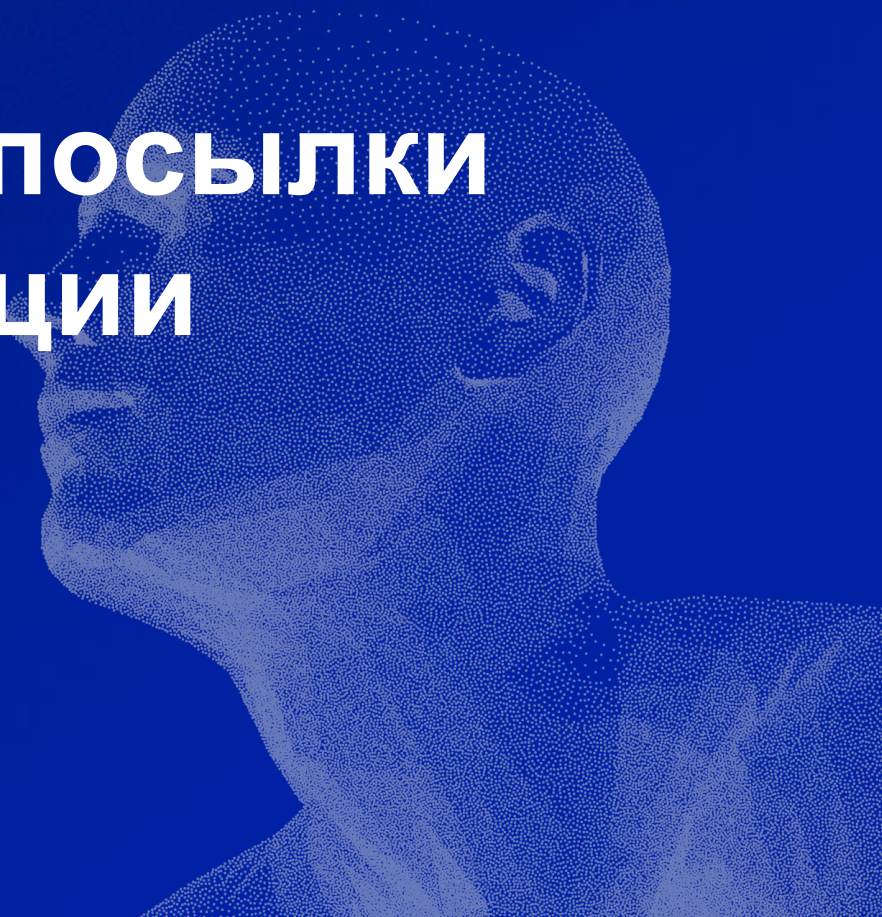
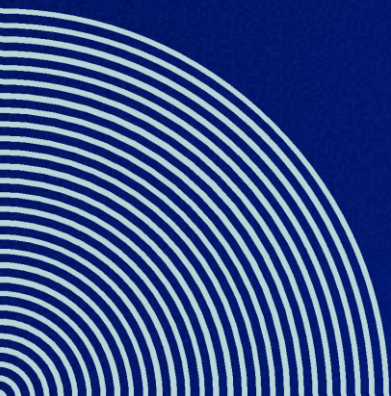
Постквантовая (квантово-устойчивая) криптография — область криптографии, связанная с разработкой и анализом схем асимметричной криптографии, устойчивых к атакам с применением как квантового, так и классического компьютера. Постквантовая криптография реализуется на классических вычислительных устройствах.

Данные и устройства с длинным жизненным циклом нуждаются в новых методах защиты уже сегодня

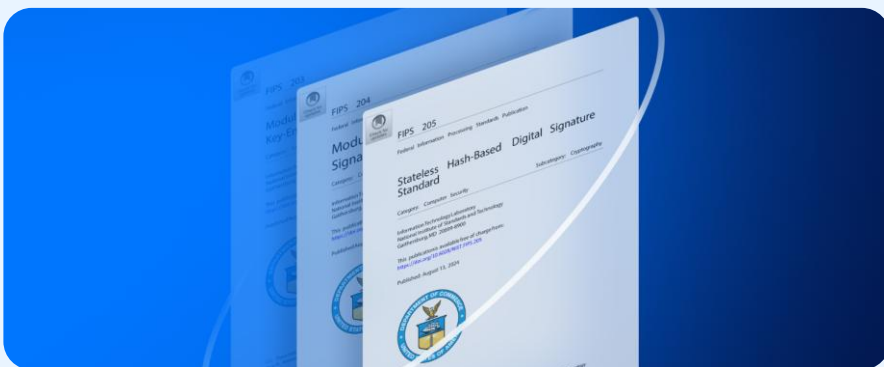


^{*} Атака, при которой злоумышленник может собирать удаленно данные с вашего устройства, а расшифровать их при получении доступа к квантовому компьютеру (провайдеры типа Amazon предоставляют облачный доступ к новому классу этих вычислителей)

2. Экономические и регуляторные предпосылки постквантовой миграции



Постквантовая (квантово-устойчивая) криптография становится стандартом



13 августа 2024 года Национальный институт стандартов США (NIST) опубликовал первые стандарты в области постквантовой криптографии*:

- FIPS 203 (ML-KEM)
- FIPS 204 (ML-DSA)
- FIPS 205 (SLH-DSA)

Экономическое значение стандартов:

Госзакупки

Требования
к продуктам

Бюджетирование обновления ИТ-систем

Регуляторный сдвиг:

Ведущие экономики мира переводят вопрос постквантовой защиты из научной повестки в управленческую практику



Отсутствие постквантовой криптографии в продуктах — риск несоответствия требованиям закупок

* [NIST Releases First 3 Finalized Post-Quantum Encryption Standards](#)

Оценка затрат на постквантовую миграцию

- Инвентаризация криптографических средств:
 - ИТ-ландшафт
 - цепочки поставок

Без инвентаризации невозможно обосновать очередность проектов, оценить CAPEX и OPEX и управлять зависимостями от поставщиков в многоуровневых системах

- Обновление компонентов программного оборудования
- Капитальные затраты на замену физических устройств без возможности удаленного обновления (смарт-карты, HSM, встраиваемые модули)
- Рост сетевой и вычислительной нагрузки

Стоимость потенциальных рисков существенно превышает затраты на постквантовую миграцию

Кейс: Блокчейн



>10 млн

биткоин-адресов, использующих неустойчивое к квантовым атакам шифрование



6,2 млн BTC

Общий баланс биткоин-адресов



\$648 млрд









Стоимость потенциальных потерь от квантовой кибератаки

Project Eleven¹ привлекли \$6 млн на внедрение защиты Bitcoin от квантовых кибератак²

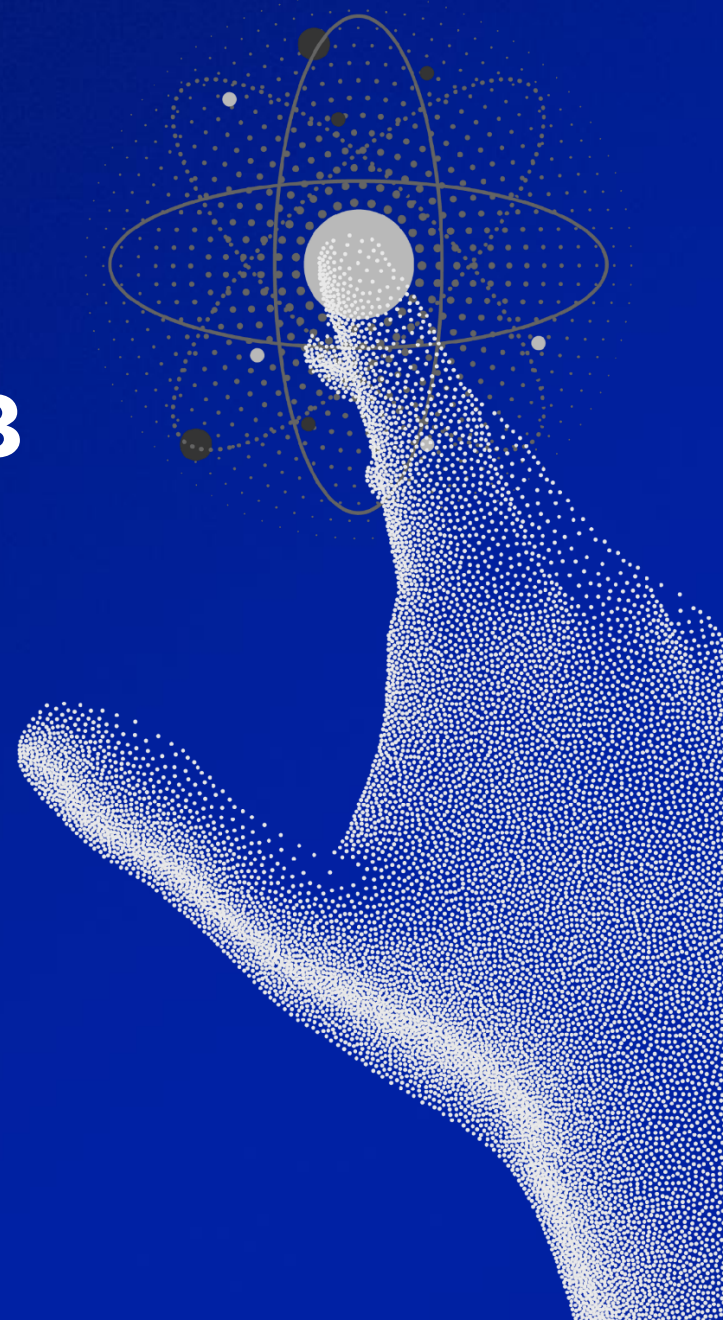
Ethereum Foundation создал команду по постквантовой криптографии со стартовым бюджетом \$2 млн³

[1] Компания-разработчик, специализирующаяся на постквантовой криптографии, [2] [Project Eleven raises \\$6M to defend Bitcoin from quantum attacks. 19.06.2025.](#) [3] [thequantuminsider](#)

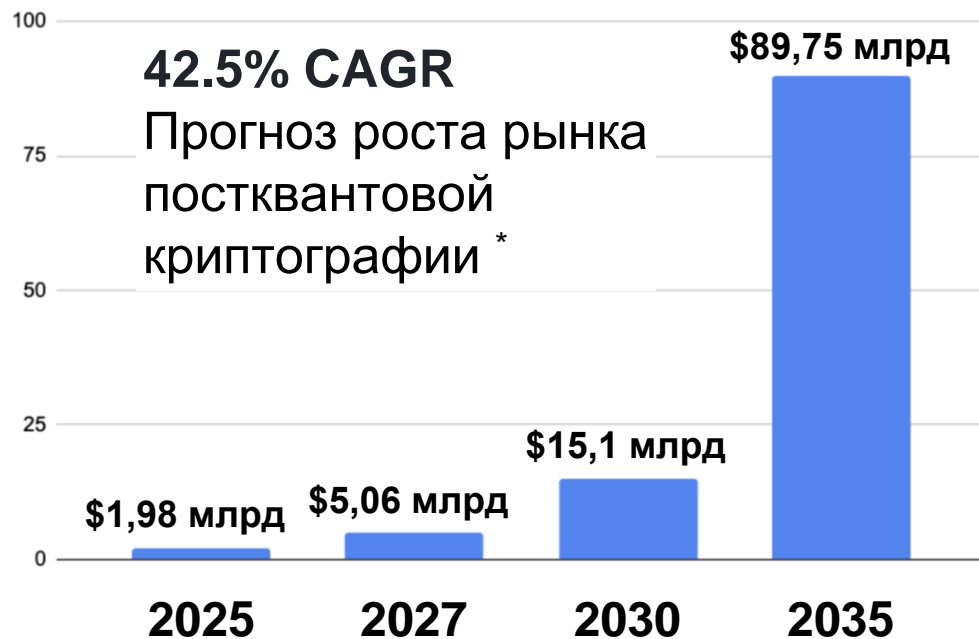
Готовность стран к постквантовой миграции

География	Ключевые документы и инициативы	Статус и контрольные сроки
Северная Америка	 США: Стандарты NIST; меморандум OMB M-23-02; директива CNSA 2.0., NIST. IR 8547  Канада: Дорожная карта ITSM.40.001	<ul style="list-style-type: none"> • до апреля 2026 г. Подготовка систем • до 2031 г. Приоритетный переход • к 2035 г. Завершение миграции, запрет классической криптографии
Европа	 Великобритания: Рекомендации национального центра кибербезопасности (NCSC)  ЕС: Координированная дорожная карта, Директива NIS2 <ul style="list-style-type: none"> • Германия: Рекомендации ведомства BSI • Франция: Позиция агентства ANSSI • Нидерланды: Руководство «PQC Migration Handbook» • Италия: Материалы агентства по кибербезопасности (ACN) 	<ul style="list-style-type: none"> • к 2028 г. Идентификация критических сервисов • до 2031 г. Приоритетный переход • к 2035 г. Завершение миграции <p>Ведется разработка национальных стандартов постквантовой миграции</p>
Азиатско-Тихоокеанский регион	 Австралия: Опубликовано руководство ACSC/ASD  Китай: Объявление SCA № 46; работа комитета TC260 по стандартизации коммерческий постквантовых алгоритмов  Южная Корея: Конкурс KpqC завершен	<ul style="list-style-type: none"> • Китай: Запуск многолетних проектов с государственным бюджетированием. • 2025 – 2028 гг. Южная Корея: Реализация пилотных проектов в критических отраслях
 Россия	Разработка стандартов постквантовых алгоритмов (с 2019 г.), реализуются прикладные интеграционные проекты	<ul style="list-style-type: none"> • 2027-2028: прогноз выхода первых стандартов по постквантовой криптографии в РФ • Отсутствуют: профильная дорожная карта, официальные документы со сроками миграции и инвентаризации информационных систем

3. Инвестиционный анализ конкурентной среды



Оценка объема рынка постквантовой криптографии



Уже внедрили постквантовую криптографию



Gartner.

в топ-10
технологических трендов



Рекомендации
по применению

РQS: Инвестиции и выручка: Северная Америка

Страна	Компания	Суммарный объем инвестиций	Сумма инвестиций последнего раунда	Оценка Post-money	Выручка 2024	Мультипликатор к выручке
США	PQSecure Technologies	\$3 310 000	\$2 230 000	—	\$1-5 M	—
	AgilePQ	—	\$5 620 000	—	\$510 000	—
	SandboxAQ	\$1 100 000 000	\$95 000 000	\$5 800 000 000	\$17 800 000	—
	QuSecure	\$28 000 000	\$28 000 000	\$54 000 000	\$11 200 000	4,8
	Quantum Xchange	\$45 600 000	\$3 000 000	\$68 000 000	\$2 400 000	28,3
	Keyfactor	\$218 000 000	\$125 000 000	\$1 300 000 000	\$100 000 000	13
	Rambus	\$500 000 000	\$200 000 000	\$10 600 000 000	\$557 000 000	19
Канада	01 Communique Labo...	\$2 350 000	\$2 350 000	\$36 000 000	\$303 000	118
	Crypto4A Technologies	\$3 750 000	\$3 750 000	—	\$3 300 000	—
	Quantropi	\$10 000 000	\$10 000 000	—	—	—
	ISARA	\$21 500 000	\$7 200 000	—	\$2 000 000	—
	evolutionQ	\$5 490 000	\$5 490 000	\$33 000 000	\$3 486 000	9,5
	Agnostiq	\$8 900 000	\$6 100 000	\$37 000 000	\$3 000 000	12,3

РQS: Инвестиции и выручка: Европа

Страна	Компания	Суммарный объем инвестиций	Сумма инвестиций последнего раунда	Оценка Post-money	Выручка 2024	Мультипликатор к выручке
Великобритания	PQ Shield	\$65 300 000	\$37 000 000	\$222 000 000	\$5 000 000	44,4
	Post-quantum	\$14 000 000	\$3 800 000	\$62 000 000	\$1 000 000	62
	Arqit	\$517 000 000	\$13 600 000	\$547 000 000	\$293 000	1 867
	Miracl	\$264 000	\$200 000	\$2 000 000	\$1 500 000	1,3
	Crypta Labs	\$4 680 000	\$2 140 000	\$13 000 000	<\$5 000 000	—
	Cryptoquantique	\$8 000 000	N/A	\$48 000 000	\$3 500 000	13,7
	QUANTUM DICE	\$7 800 000	\$2 000 000	\$8 000 000	\$507 000	15,8
Великобритания + Франция	Quantinuum (ex. Cambr...	\$2 300 000 000	\$594 000 000	\$10 000 000 000	\$115 100 000	86,9
	Cryptosense	\$5 600 000	\$4 800 000	\$29 000 000	\$65 000	446
Франция	CryptoNext Security	\$2 202 000 000	\$582 000 000	\$53 000 000 000	\$17 420 000 000	3
Германия	Infineon Technologies	\$13 000 000	\$13 000 000	—	—	—
Словакия	Decent Cybersecurity	—	\$6 000 000	\$36 000 000	—	—
Швейцария	Securosys	—	\$1 240 000	\$6 000 000	\$5 900 000	1
	SEALSQ	—	\$60 000 000	\$689 000 000	\$10 981 000	62,7
Швейцария + Бразилия	Kryptus	—	\$3 700 000	\$22 000 000	\$6 400 000	3,4
Испания	Quside	\$14 900 000	\$11 500 000	\$66 000 000	\$5 000 000	13,2

RQC: Инвестиции и выручка: Азиатско-Тихоокеанский регион

Страна	Компания	Суммарный объем инвестиций	Сумма инвестиций последнего раунда	Оценка Post-money	Выручка 2024	Мультипликатор к выручке
Индия	QNu Labs	\$22 200 000	\$7 000 000	\$43 000 000	\$11 208 000	3,8
Сингапур	SpeQtral	—	\$1 500 000	\$16 500 000	—	—
Австралия	Crypto4A Technologies	\$66 900 000	\$13 000 000	\$97 000 000	—	—

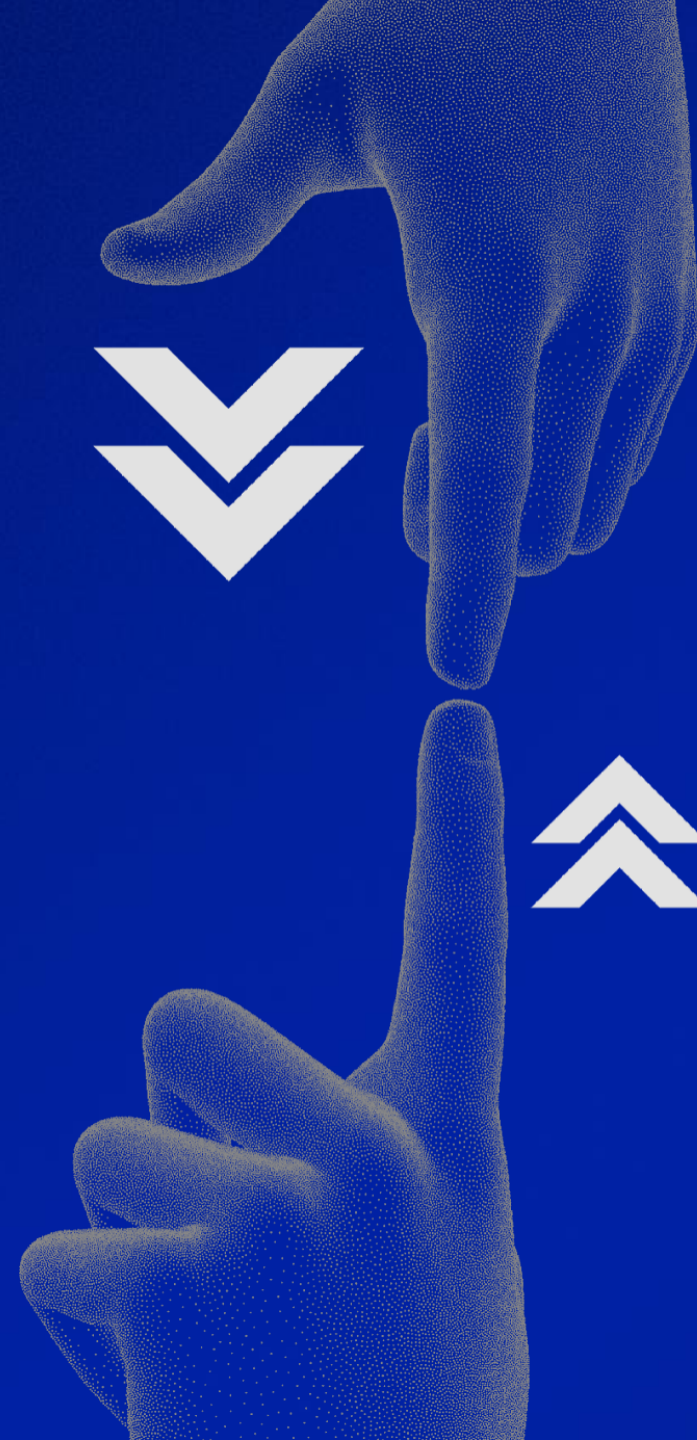
Количество компаний,
занимающихся прикладным
развитием постквантовой
криптографии:

Северная Америка — более 50
Европа — около 30 шт
АТР — более 10 шт

Мультипликатор постквантового рынка ИБ*	Медиана	14,7
	Среднее значение	187,5
Мультипликатор классического рынка ИБ**	Медиана	5,2
	Среднее значение	6,4

*Базы данных Tracxn, PitchBook, Crunchbase, Dealroom ** [Cybersecurity Quarterly Update](#)

4. Образование



Образование в области постквантовой криптографии

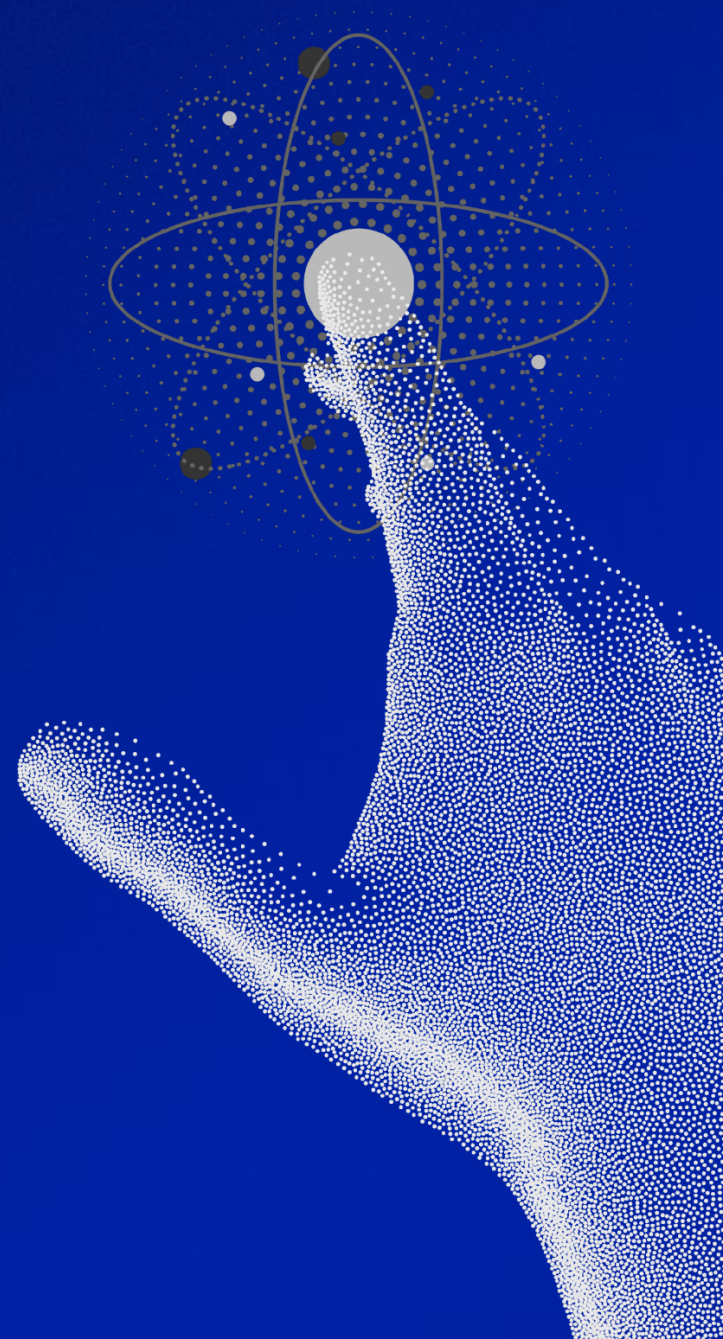
>10 университетов России преподают
базовые основы постквантовой
криптографии

 ИТМО	 МГУ	 МИСИС
 МФТИ	 ВШЭ МИЭМ	 МГТУ им. Баумана
 ННГУ им. Лобачевского	 ЮФУ	 МИРЭА
 ИрГУПС	 БФУ им. Канта	И другие

В мире: консолидация экспертизы и совместное участие университетов разных стран в грантовых программах по постквантовой криптографии

Университет	Страна	Проект
Университет Ватерлоо	Канада	Open Quantum Safe (OQS)
Рурский университет	Германия	
Университет Радбауд	Нидерланды	PQClean
MIT	США	
Queen's University Belfast	Великобритания	SAFEcrypto
University of Patras	Греция	
Université de Versailles Saint-Quentin-en-Yvelines	Франция	
University of Warsaw	Польша	
Ruhr-Universität Bochum	Германия	SAFEcrypto, PQ-REACT
University of Ljubljana	Словения	PQ-REACT
DTU	Дания	PQ-REACT, SHARCS
University of Bologna	Италия	PQ-REACT, HECTOR
KU Leuven	Бельгия	HECTOR
University of Bristol	Великобритания	HECTOR, SHARCS
Radboud University	Нидерланды	HECTOR
Graz University of Technology	Австрия	SHARCS

5. Индекс готовности к постквантовой миграции (PQCSR-индекс)



Индекс готовности к постквантовой миграции (PQCR-индекс)



Индекс PQCR (Post-quantum cryptography Readiness Index) позволяет сопоставить готовность стран, регионов и отраслей к переходу на постквантовую защиту

$$\text{PQCR} = w_1 \times S + w_2 \times G + w_3 \times I + w_4 \times O + w_5 \times C + w_6 \times U$$

S — зрелость стандартов и участие в межведомственных или межотраслевых проектах

G — государственные стимулы и наличие дорожных карт по миграции

I — наличие сформированных бюджетов на уровне стран и отраслей (или отдельных компаний-заказчиков) и участие крупных институциональных инвесторов

O — наличие отраслевых объединений и организаций (или ответственных лиц), обеспечивающих координацию миграции

C — наличие конкурентной среды поставщиков (вендоров) решений

U — уровень внедрения в индустрии, наличие готовых программных и программно-аппаратных решений и открытых реализаций постквантовых алгоритмов




w₁...w₆ — весовые коэффициенты, подбираются под задачу сравнения

Расчет готовности к постквантовой миграции на примере России, США и Китая

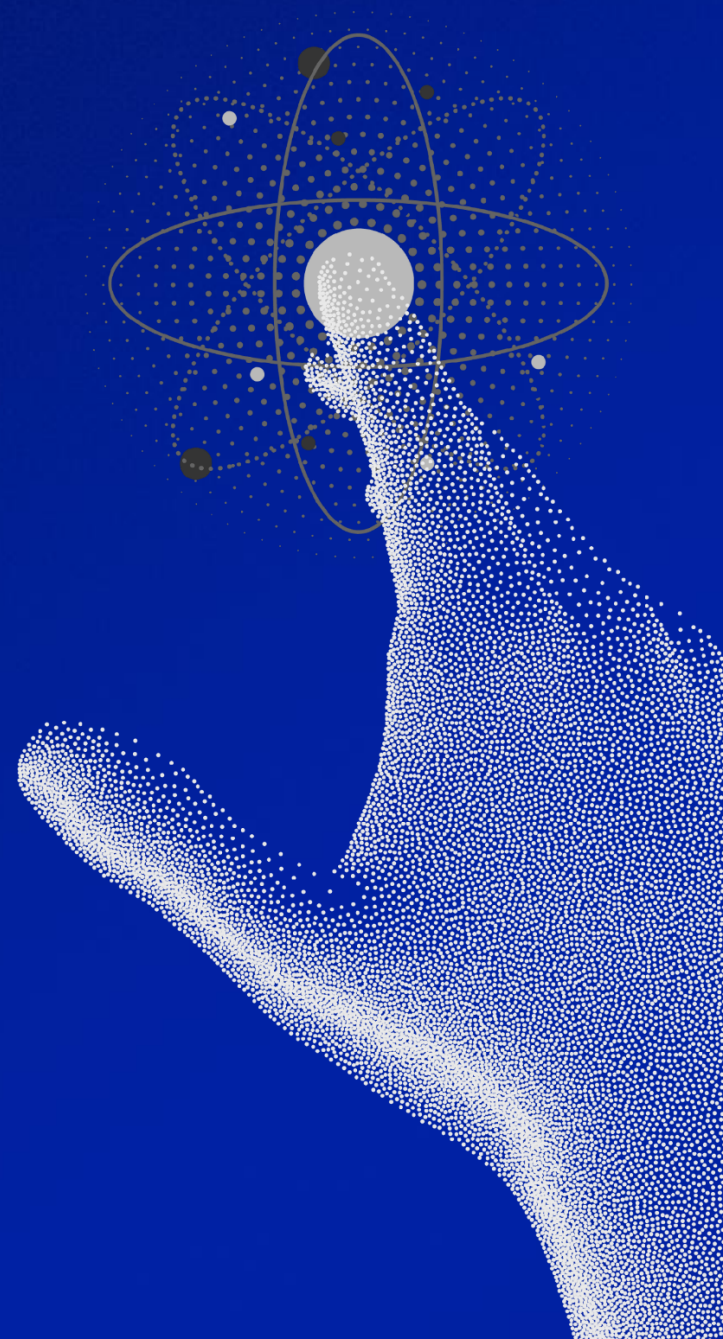
Выбор значений компонентов для расчета PQCR-индекса

Компонент	Значение		
S	⊗ Отсутствуют	🕒 В разработке	✅ Приняты
G	⊗ Отсутствуют	🕒 В разработке	✅ Приняты
I	⊗ Отсутствуют	🕒 В разработке	✅ Приняты
O	⊗ Отсутствуют	🕒 В разработке	✅ Приняты
C	⊗ Отсутствуют	🕒 Менее 3х	✅ 3 и более
U	⊗ Отсутствуют	Пилотные проекты	Промо эксплуатация
	0	1	2

Расчет PQCR-индекса стран

 США	 РФ	 Китай
2	1	2
2	0	1
1	0	1
2	0	1
2	1	2
2	1	1
11	3	8

6. Рекомендации для участников рынка



Рекомендации для коммерческих компаний и государственных организаций

- Инвентаризация криптографических средств: алгоритмы, протоколы, вендоры, просчитать риски и CAPEX/OPEX
- Планирование поэтапной миграции на 5–7 лет с учетом обновления инфраструктуры
- Резервирование отдельных бюджетов на переход и долгосрочное сопровождение
- Обеспечение криптографической гибкости
- Пилотирование проектов и тестирование на совместимость с оценкой производительности
- Обновление требований к контрагентам с учетом постквантовых стандартов





Ирина Полтавская
Коммерческий директор QApp

@ivpoltavskaya
ipoltavskaya@qapp.tech



[QApp.tech](https://qapp.tech)