QApp

Protection for financial data from quantum attacks

Post-quantum cryptography

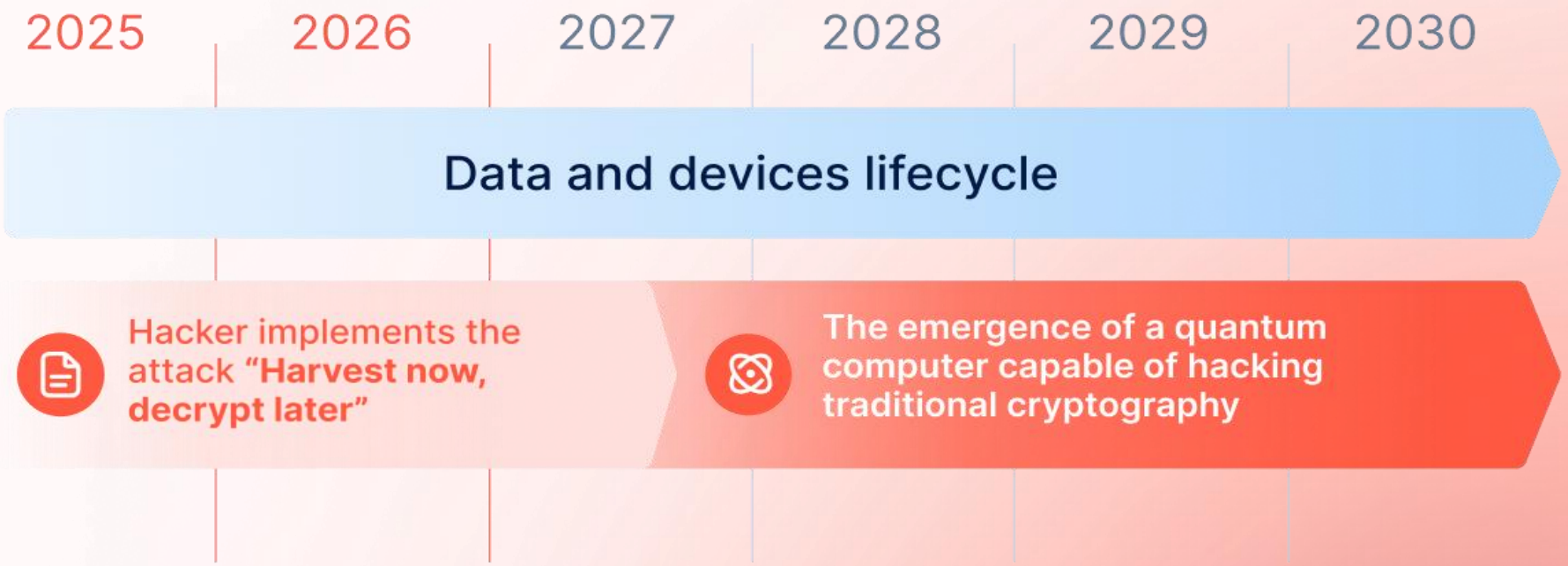
Anton Guglya
CEO

Quantum threat — is a new cybersecurity risk to both the business and the government

Most encryption algorithms in use today are not resistant to cyber attacks using powerful quantum computers алгоритмов

- Key distribution
- Asymmetric encryption
- Digital signature

Data with a long lifecycle needs protection today



Most traditional information systems are under quantum threat

QApp

- Network infrastructure
- Internet of things
- Common software
- Blockchain solutions

The quantum threat increases the cybersecurity risks of blockchain projects

QApp

- **Forgery of the digital signature of the participants in the process** (block authors and those conducting transactions)
- Accelerating the production of new blocks and, thus, **the implementation of the « 51% attack»**
- Unauthorized **modification of smart contracts** by digital signature forgery
- Hacking authentication and encryption protocols for **unauthorized online access to user** wallets (storage of internal tokens of the blockchain project)

QApp

Hacking any of the components of a blockchain product inevitably leads to compromising data **All components at different levels must be protected**

Post-quantum cryptography — is the optimal method of protection

QApp

A new class of asymmetric encryption algorithms

- Software solutions
- Does not require modification of the hardware infrastructure
- Protection against quantum and classical cyber attacks

Post-quantum cryptography is easy to integrate

QApp

Communications

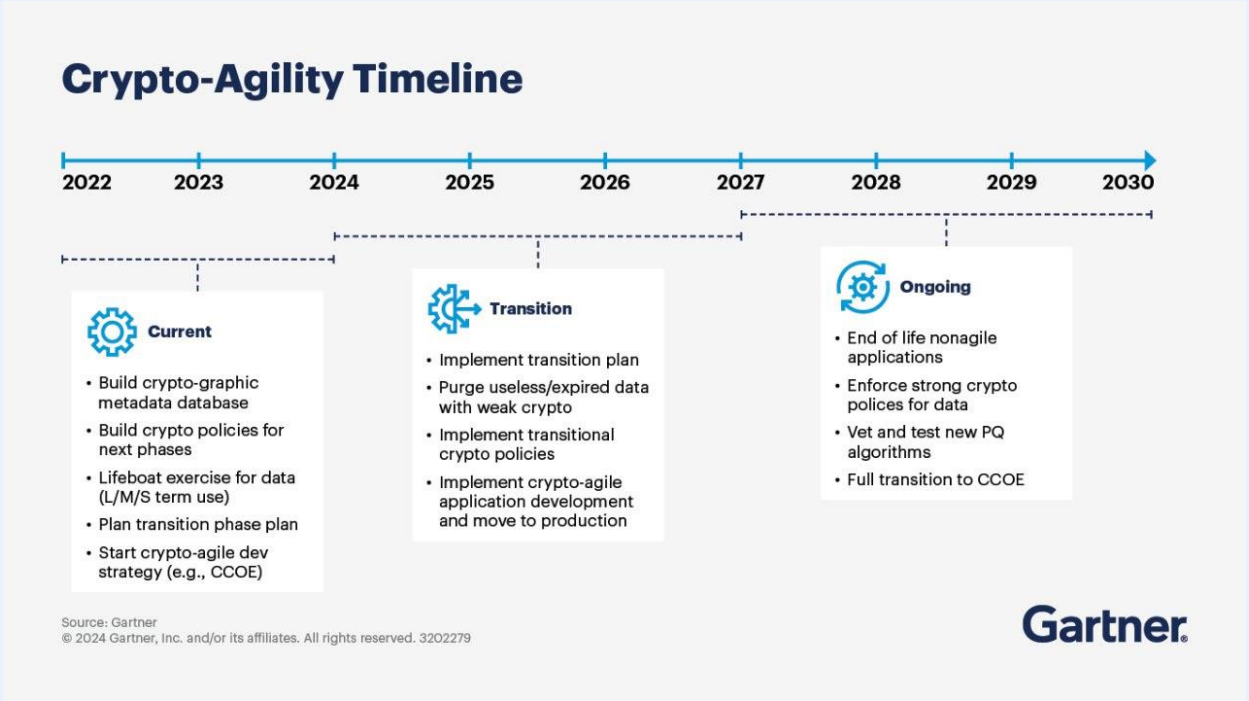
Authentication

Storage of data

Document management

Support for popular platforms and protocols

Post-quantum cryptography in the technological trends of 2025



Gartner recommends companies to create quantum security departments, structure encrypted metadata, prescribe mechanisms for the transition to post-quantum solutions, and implement post-quantum encryption now

International experience. Countries

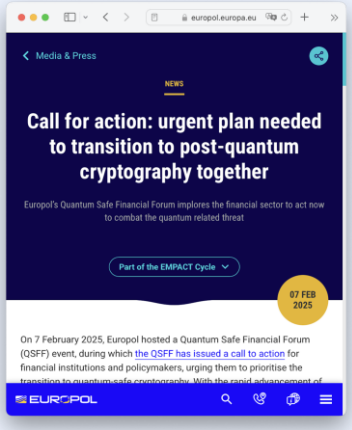
The quantum threat is included in the national cybersecurity strategy

New government standards for post-quantum cryptography have been accepted

The European Commission has issued recommendations for developing a roadmap for the transition to post-quantum cryptography

Europol has called on the financial institutions of the European Union to work together to counter the quantum threat

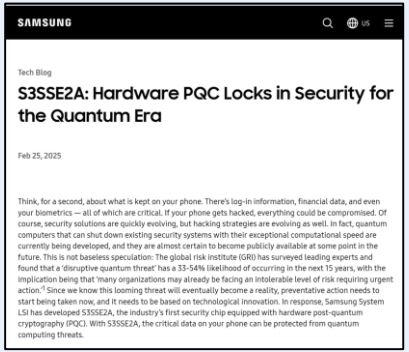
A national competition for the development of post-quantum algorithms has been announced



Europol has called on the financial institutions of the European Union to work together to counter the quantum threat

International experience. IT-gients

QApp



Post-quantum cryptography is rapidly developing in Russia

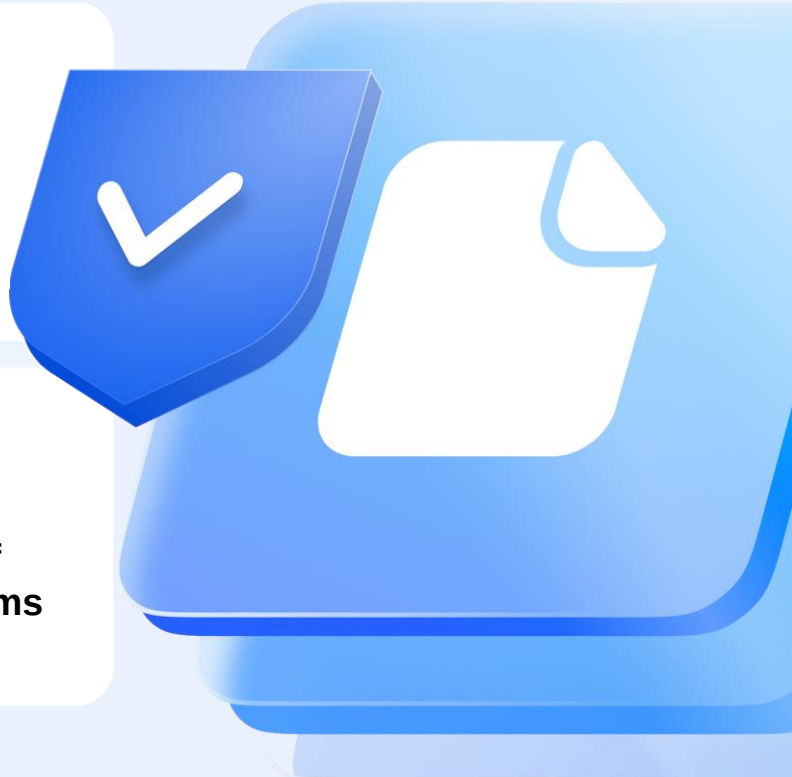
QApp

Russia has completed dozens of pilot projects

>5 domestic software products have already been developed

New government standards are being developed

The first realizations of post-quantum algorithms appeared



Post-quantum cryptography is being actively researched and piloted

QApp

Банк России

АССОЦИАЦИЯ ФИНТЕХ

НСПК

СБЕР

ГАЗПРОМБАНК

ВТБ

MOEX МОСКОВСКАЯ БИРЖА

СПББИРЖА

The value of piloting Post-Quantum Cryptography

- **Estimating the costs of putting the technology into commercial operation in the future**
- **Developing cryptographic agility**
- **Wide-coverage media effect**

Priority data types to be protected

- Financial
- Personal
- Engineering secrets
- Blockchain projects data

…

Priority sectors of the economy

- Finance
- Telecommunication
- Energy
- Medicine

…

Domestic software solutions based on post-quantum cryptography

QApp

End products

PQC CHAIN — quantum resistant blockchain

PQC TLS — quantum resistant TLS Gateway

PQC GATE — post-quantum data protection during transmission

PQ VPN — quantum resistant virtual private networks

System software

PQC SDK — a library of post-quantum algorithms and tools to simplify their integration

PQC IP — hardware acceleration of post-quantum

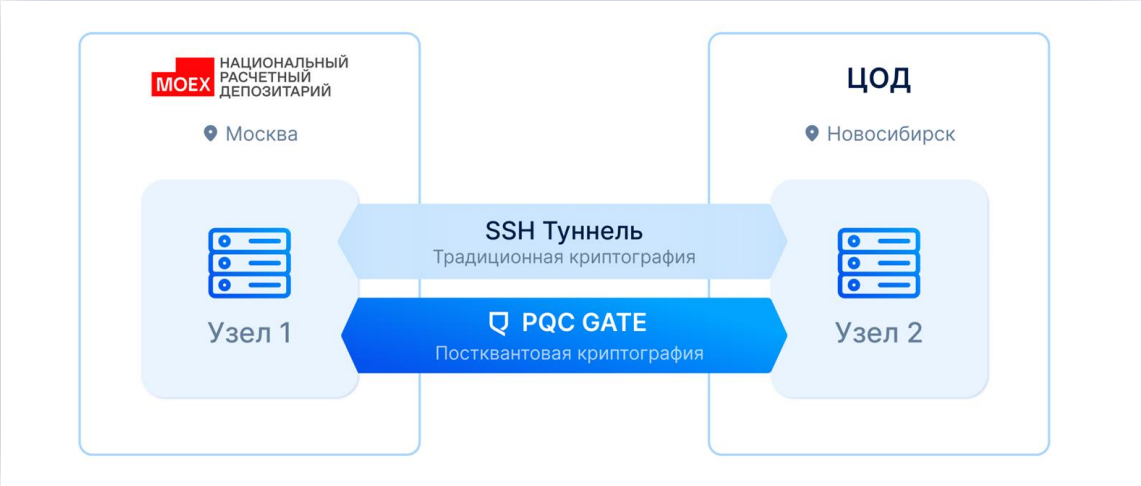
PQC PKI — infrastructure of the certification center

Algorithms
in the interests of society

гиперикум

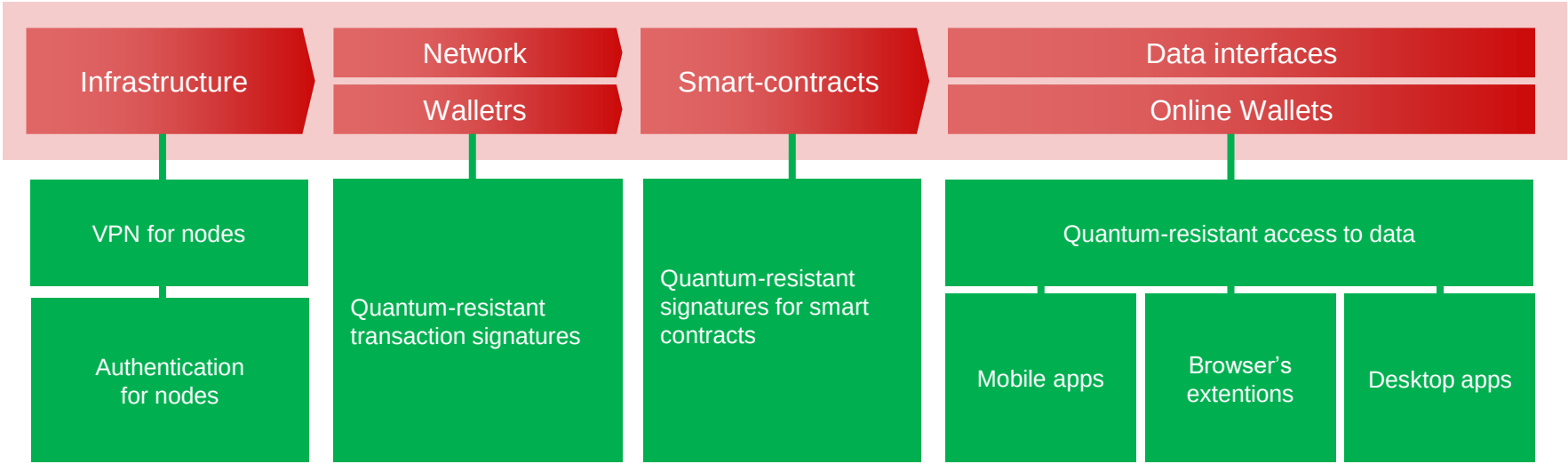
New post-quantum digital signature algorithm.
Candidate for inclusion in the government standards in Russia

Post-quantum encryption of the Moscow Exchange's backup data transmission channel



Implementation of a quantum-resistant tunnel between two remote data centers of the Moscow Exchange for transferring encrypted backup copies of large-sized data

Post-quantum cryptography will also improve the security of blockchain projects



QApp

QApp.tech

Anton Guglya
CEO

+7 925 537-71-53

apg@rqc.ru