



РОССИЙСКИЙ ФОРУМ
МИКРОЭЛЕКТРОНИКА 2025



ФЕДЕРАЛЬНАЯ
ТЕРРИТОРИЯ
«СИРИУС»

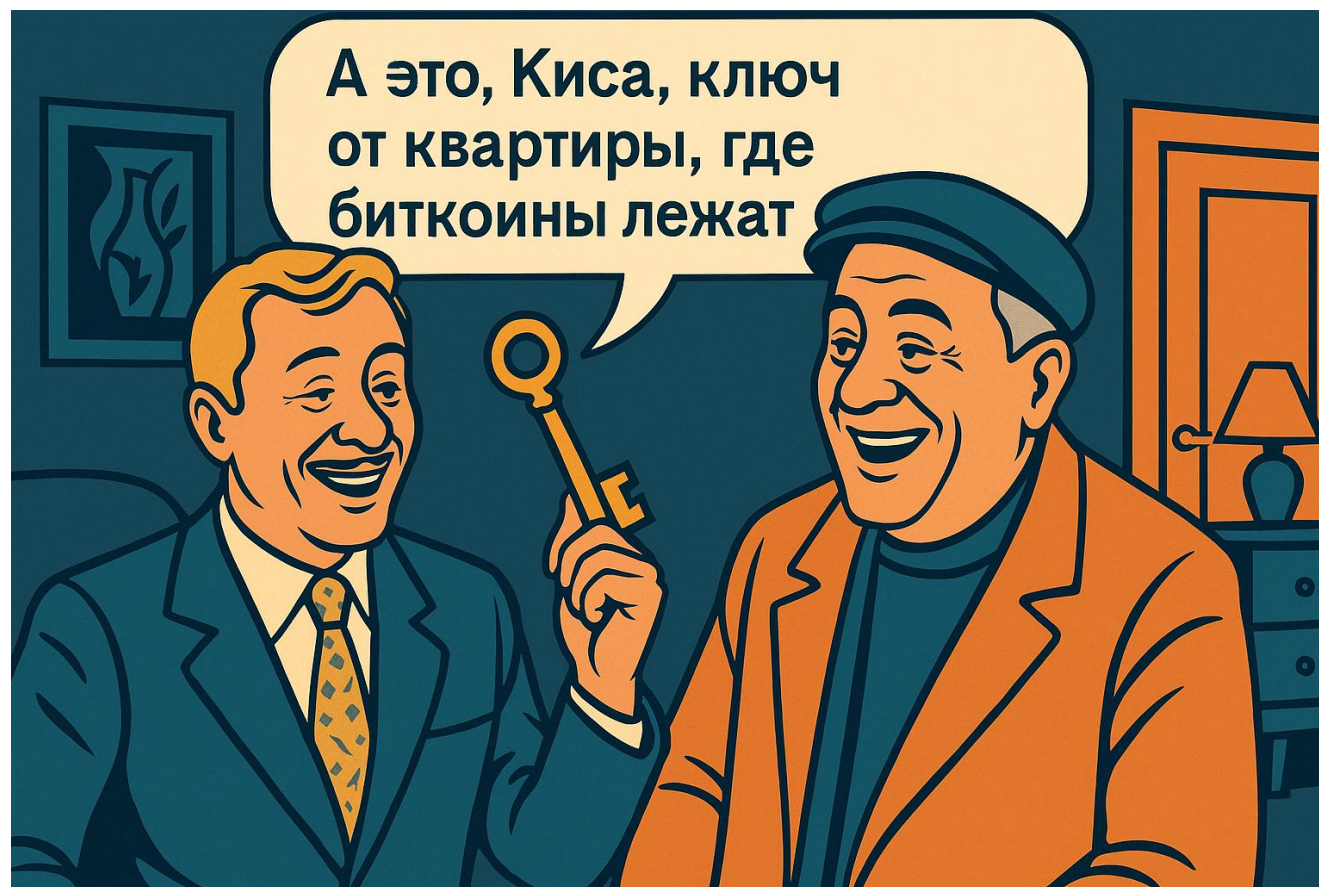


21–27
сентября 2025

Квантовая угроза.
Вызовы и решения для
корпоративной кибербезопасности



Мотивация



Капитализация криптовалют превышает 3 трлн \$

Угрозы. Алгоритм Шора



Угрозы. Алгоритм Гровера



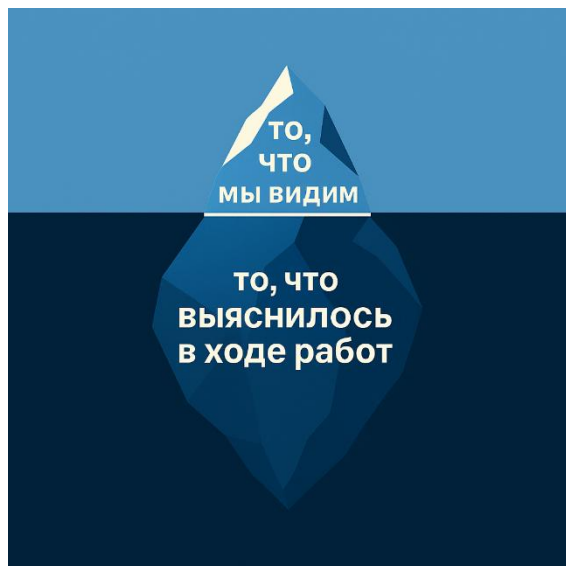
Угроза. Сбор трафика



Контекст внутри компании



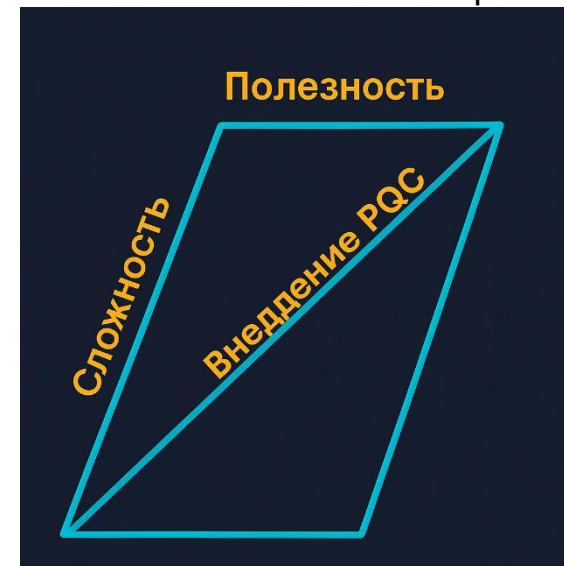
Zero Trust



Блокчейн



Постквантовая защита



Угрозы не работают. Квантовое распределение ключей (КРК) и постквантовая криптография (PQS):

- Хуже в эксплуатации;
- Дороже стоят;
- Трудно внедрить повсеместно;
- PQS не достаточно изучены;
- Атаки пока что только теоретические.

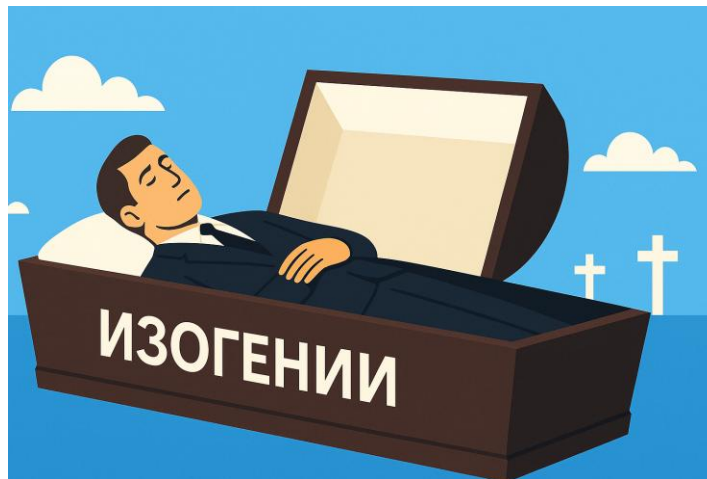
Текущее состояние отрасли



Технологии:

- Алгоритмы (подпись + инкапсуляция ключа);
- SDK (мобильное + десктоп);
- Оборудование КРК;
- Квантовые ДСЧ.

Реальный мир



Неизученность PQC + Позиция Регулятора =
Нужна дополнительная ценность у решений,
Использующих PQC.

Как внедрять



Покупать отдельно решения PQC – не всегда понятна выгода и велики риски не справиться с проектом.

Выход – купить качественное решение, закрывающее бизнес-потребность, куда PQC встроено как отдельная функциональность

Криптография в организациях



Внешние сервисы:

- Клиенты (браузер + веб-сервер);
- Удаленный доступ (RA);
- Удаленный доступ (Site-to-Site)

Внутренние сервисы:

- ЭДО (УНЭП + УКЭП);
- Домен;
- Enterprise CA;
- IdP;
- Корпоративный мессенджер

Клиенты. Браузер + веб-сервер



- Криптонабор X25519Kyber768 в TLS 1.3;
- Сертификат НУЦ на Dilithium.

Удаленный доступ



Двойной режим:

Сначала ГОСТ, внутри
PQC



ZTNA = VPN + Compliance;

SASE = ZTNA + SD WAN;

SDP = SPA + UDP + HOTP + доступ до конкретного сервиса

Криптография внутри компании



Сертификаты



ЭДО:

- CSP с двойной криптографией;
- УЦ с двойной криптографией.

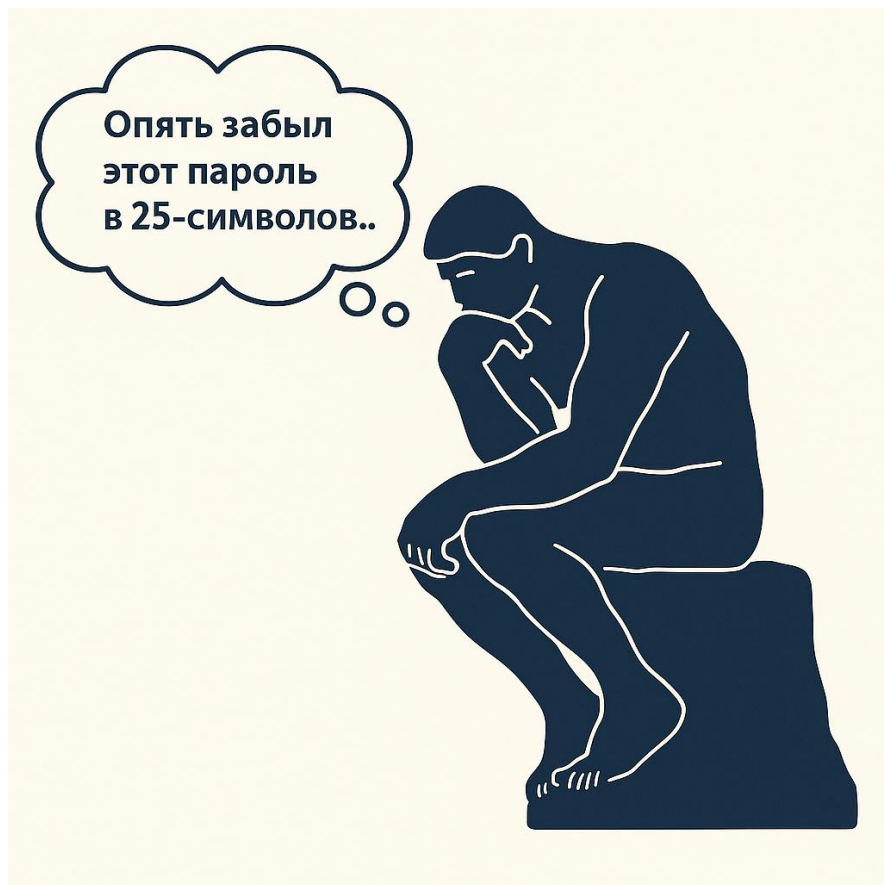
microelectronica.pro



Enterprise CA:

- Поддержка в операционных системах;
- УЦ с двойной криптографией.

Провайдеры аутентификации



Нужны доменные системы, в которых у учетных записей нет обязательной парольной сущности.



Нужны отечественные IdP с PQC подписью токенов доступа.

Заключение. Прогресс в отрасли



Квантовые технологии в России в 2020 году



Программа развития квантовых технологий



Квантовые технологии в России в 2025 году

Заключение. Выводы



Россия 2025:

- Квантовые компьютеры всех типов;
- Постквантовые алгоритмы всех типов;
- Системы КРК;
- Квантовые ДСЧ.



Государство и бизнес 20X:

- Готовы противостоять квантовой угрозе;
- Используют квантовые компьютеры для новых достижений.

СПАСИБО ЗА ВНИМАНИЕ!

Кузьмин Дмитрий Сергеевич

Директор, «Цифровая крепость ВЭБа»

Государственная корпорация развития
ВЭБ.РФ



+7 (927) 380-41-93



KuzminDS@veb.ru



MICROELECTRONICA.PRO



ПОДПИСЫВАЙТЕСЬ И БУДЬТЕ В КУРСЕ
ВСЕХ ПОСЛЕДНИХ НОВОСТЕЙ!



ВАШ ЛИЧНЫЙ
КАБИНЕТ



Rutube



VK Видео



РОССИЙСКИЙ ФОРУМ
МИКРОЭЛЕКТРОНИКА 2025



21–27
сентября 2025