



РОССИЙСКИЙ ФОРУМ
МИКРОЭЛЕКТРОНИКА 2025



ФЕДЕРАЛЬНАЯ
ТЕРРИТОРИЯ
«СИРИУС»



21–27
сентября 2025

ANGARA SECURITY

Применение квантовой
криптографии для повышения
киберустойчивости компаний

Перехват и взлом каналов передачи данных



- ▶ **Оптоволокно:** прослушка через врезку сплиттера или микроперегиб; возможно скрытное копирование всего спектра на участке. Реальные кейсы перехвата на магистралях подтверждаются исследованиями и отчётами.
- ▶ **Маршрутизация:** перехват трафика через prefix hijacking с прозрачной переотправкой владельцу; демонстрации на реальном трафике и инциденты в дикой природе.
- ▶ **Госпрограммы:** перехват на узлах и ВОЛС оператора, доступ к международным каналам.
- ▶ **Вывод:** защищать нужно не только алгоритм, но и **канал распределения ключей и маршруты.**

Классическая криптография: как и зачем используется



- ▶ **TLS:** KEM/KE для установления секрета, симметричное шифрование для данных, AEAD для целостности.
- ▶ **Подписи и PKI:** аутентификация узлов, цепочки доверия.
- ▶ **Ключевой менеджмент:** жизненный цикл ключей, ротация, сегрегация, аппаратные корни доверия (HSM/KMS).
- ▶ **Почему работает:** масштабируемость, интероперабельность, производительность, проверяемость.

Ключевая идея: сочетать PQS и QKD против HNDL



- ▶ **HNDL/«собери сейчас — расшифруй позже»:** противник копит шифротрафик и архивы для будущего взлома.
- ▶ **PQS:** стандартизованные постквантовые алгоритмы для замены публично-ключевых примитивов.
- ▶ **QKD:** физически гарантированное распределение ключей и истинная случайность.
- ▶ **Гипотеза:** для каналов с долгим сроком секретности и высокой ценой компрометации — гибрид **PQS+QKD**.

Практика: государство и бизнес



- ▶ **Госструктуры:** каналы межведомственных сетей, ЦОД ↔ ЦОД, магистральные узлы; требования к сертификации и суверенности.
- ▶ **Бизнес:** банки/биржи, телеком и энергетика, транспорт и дата-центр.
- ▶ **Метрики пилота:** secure key rate (бит/с) при заданном затухании (дБ), стабильность, доля «заполнения» ключом MACsec/IPsec.

Перспективы



Стандарты и профили
совместимости,
сертификация устройств.

Прогресс MDI-/TF-QKD,
спутниковые каналы.

Развитие квантовых
ретрансляторов и снижение
CAPEX.

СПАСИБО ЗА ВНИМАНИЕ!

Хараск Максим Александрович

Коммерческий директор

Angara Security

Краткое резюме



Ваш номер телефона +7(960)1717-960



m.kharask@angarasecurity.ru



21–27
сентября 2025



MICROELECTRONICA.PRO



ПОДПИСЫВАЙТЕСЬ И БУДЬТЕ В КУРСЕ
ВСЕХ ПОСЛЕДНИХ НОВОСТЕЙ!



ВАШ ЛИЧНЫЙ
КАБИНЕТ



Rutube



VK Видео

