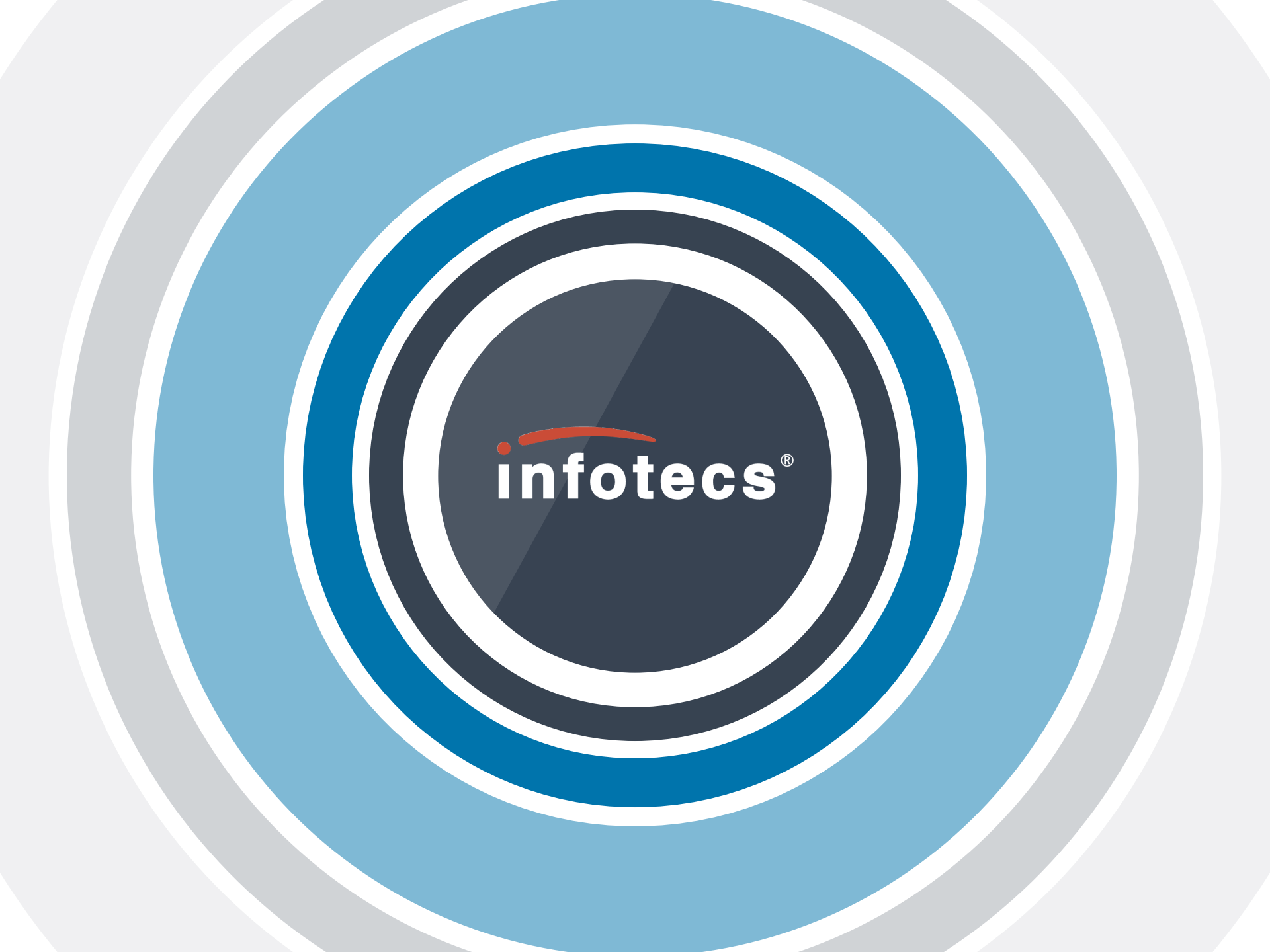
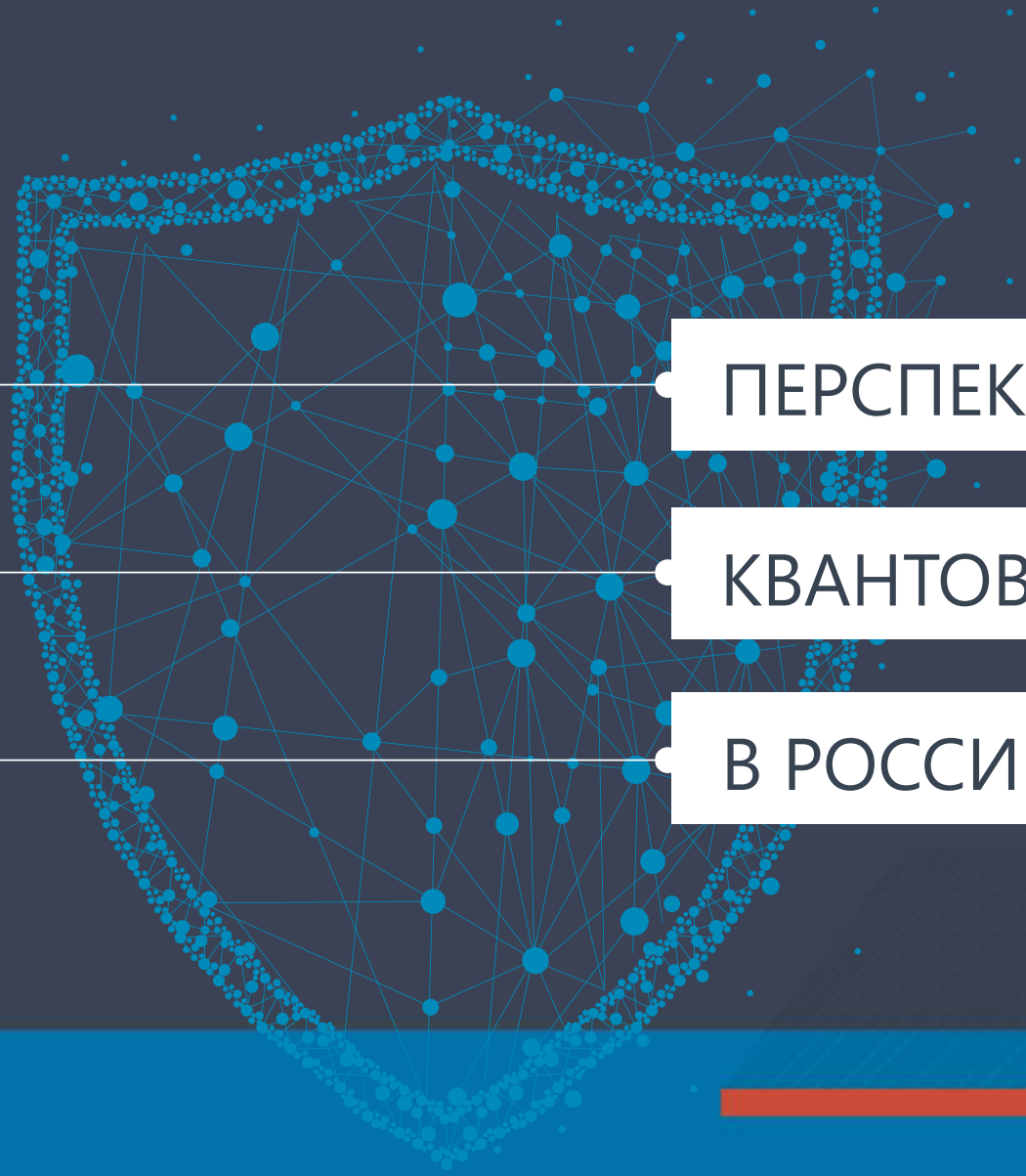

infotecs®



ПЕРСПЕКТИВЫ РАЗВИТИЯ КВАНТОВОЙ КРИПТОГРАФИИ В РОССИИ

Дмитрий Гусев, ОАО «ИнфоТеКС»

infotecs®

ПОЧЕМУ МЫ

РАССМАТРИВАЕМ ЭТУ ТЕМУ?

Тенденции в развитии сетей связи и угрозы ИБ

Увеличение скоростей ШПД: 10Гбит/с → 100 Гбит/с

Увеличение объемов передаваемой информации на 20-25% ежегодно

Оптика не только на магистральных каналах, но и на «последней миле»

Рост числа известных уязвимостей в ПО и аппаратном обеспечении

Значительное удешевление вычислительных ресурсов для выполнения ресурсоемких атак

Возможность появления эффективного квантового компьютера

Администратор мой – враг мой

А если мы все передаваемые данные зашифруем…

ЧТО ГРОЗИТ ДАННЫМ

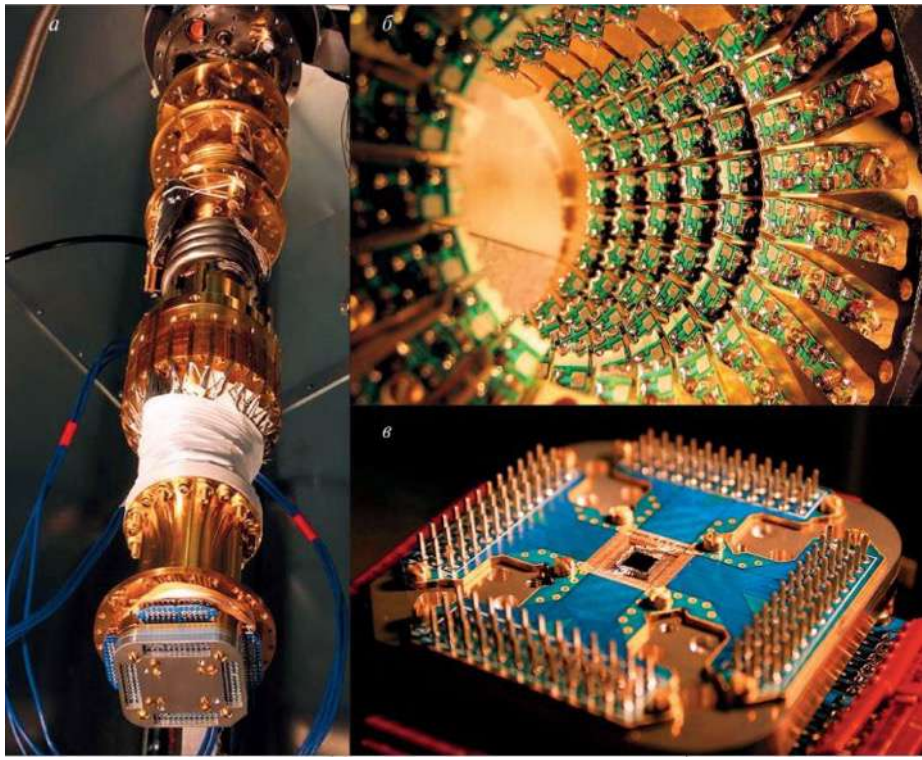
- Расшифрование (в т.ч., в будущем)
- Подмена

ИСТОЧНИКИ УГРОЗ

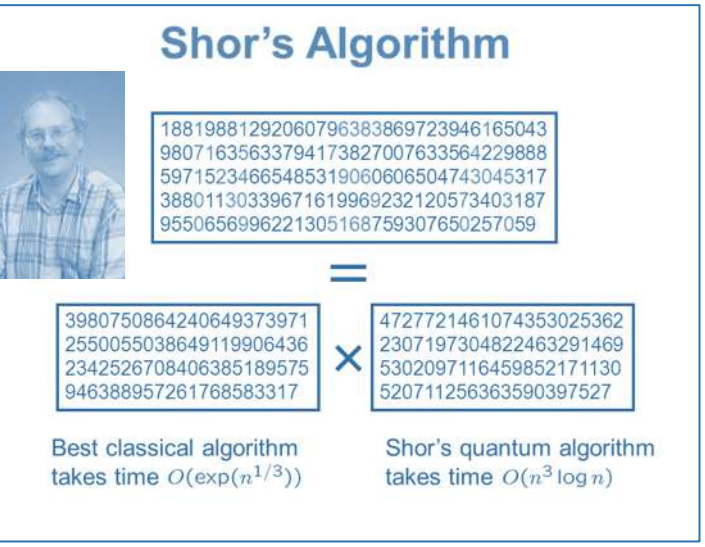
- Вычислительные ресурсы злоумышленника
- Побочные каналы утечки информации о ключах

Квантовые компьютеры

- D-Wave, IBM, Google, РКЦ (?)
- 18-кубитный КвК для исследований от IBM
- 51-кубитный в ближайшей перспективе от Google
- 1000-кубитный КвК в 20-30 летней перспективе
- КвК D-Wave 2000Q (2048-кубит/6016 связей)…
- Гибридные КвК: КвК + классические суперкомпьютеры



Квантовые компьютеры и алгоритм Шора



УГРОЗЫ

- Компрометация всех распространенных ассиметричных криптографических алгоритмов и протоколов на их основе (DH, RSA, ECDSA TLS/SSL, HTTPS, IPsec, X.509)
- Понижение стойкости симметричных криптоалгоритмов

Борьба за криптостойкость

Два подхода

УВЕЛИЧЕНИЕ ДЛИНЫ КЛЮЧА

- Большая ресурсоемкость

ЧАСТАЯ СМЕНА ОБЩЕГО СЕКРЕТНОГО КЛЮЧА

- Способы согласования общего секретного ключа:

Переход к постквантовой криптографии?

- Нет стандартизованных алгоритмов
- Большая ресурсоемкость

Подходы к выработке общего секретного ключа

Зарубежные разработки

IDQ

国盾量子 QuantumCTek

TOSHIBA
Leading Innovation

MagiQ

Известные проекты квантовых сетей связи

Китай

США

= +Европа, Япония = что в России?

Атаки на аппаратуру КРК.
Завершение периода иллюзий

QUANTUM HACKING LAB

www.vad1.com/lab/

под руководством Вадима Макарова

Реалистичный взгляд на аппаратуру КРК требует применения подходов, аналогичных сертификационным исследованиям криптографических средств защиты

- Успешные атаки на реализацию протокола КРК в продуктах ID Quantique (Clavis 2)
- В настоящее время работает в Российском квантовом центре (РКЦ)

Квантовая криптография

Современный уровень развития науки и технологии квантового распределения ключей (КРК) позволяет переходить к коммерциализации и практическому внедрению.

НО ПРИ УСЛОВИИ, ЧТО ОБЕСПЕЧИВАЮТСЯ:

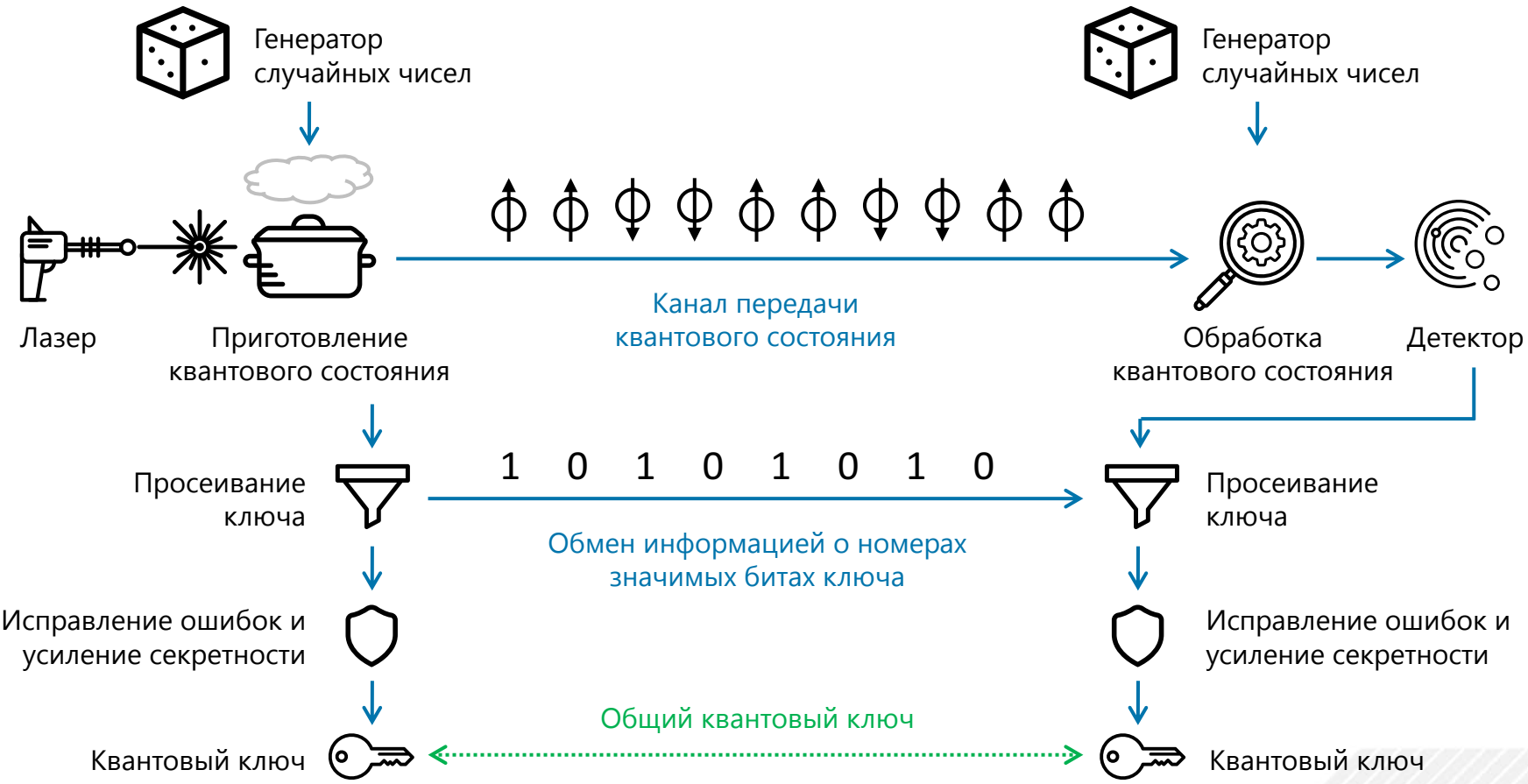
- ✓ Доказуемая стойкость квантового протокола
- ✓ Аппаратные методы генерации случайных чисел и защиты от атак
- ✓ Системный подход к защите информации

Квантовая криптография = Секретность в классической криптографии + Квантовое распределение ключей (QKD)

infotecs®

КАК ЭТО ВСЕ РАБОТАЕТ?

Квантовое распределение ключей. Принцип действия



Квантовое распределение ключей. Текущий уровень

При выполнении требований криптографической стойкости (нарушитель не должен узнать ни одного бита итогового секретного ключа при любых атаках на каналы связи)

При существующем уровне развития оптоволоконных линий связи

И

При использовании коммерчески доступных оптических компонентов

И

Квантовое распределение ключей. Текущий уровень

на **200 000 000**
квантовых отсчетов

400 бит секретного ключа
на линии связи **100** км

256 бит секретный ключ/минута

infotecs®

РАЗРАБОТКИ АППАРАТУРЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ В РОССИИ

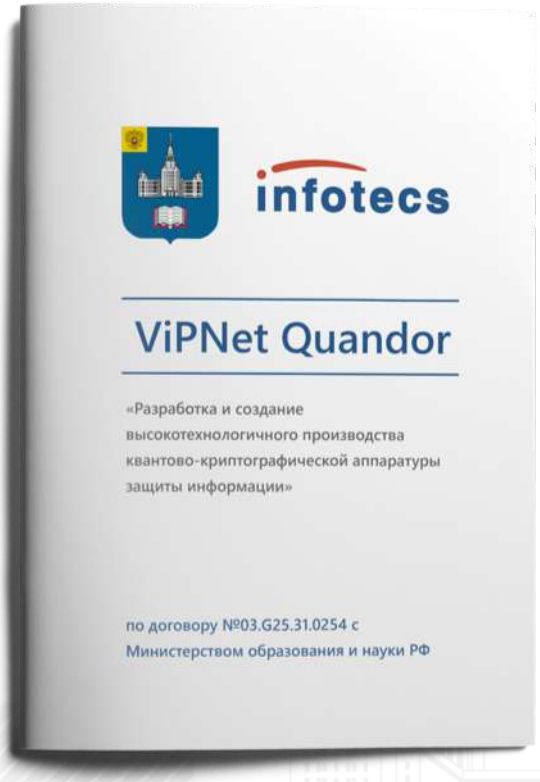
Российская лабораторная QKD-аппаратура

Физфак МГУ	Российский квантовый центр	Национальный университет ИТМО	Компания «Сконтел»

СОВМЕСТНЫЕ ПРОЕКТЫ

МГУ И ИнфоТеКС

Партнерство МГУ и ИнфоТеКС

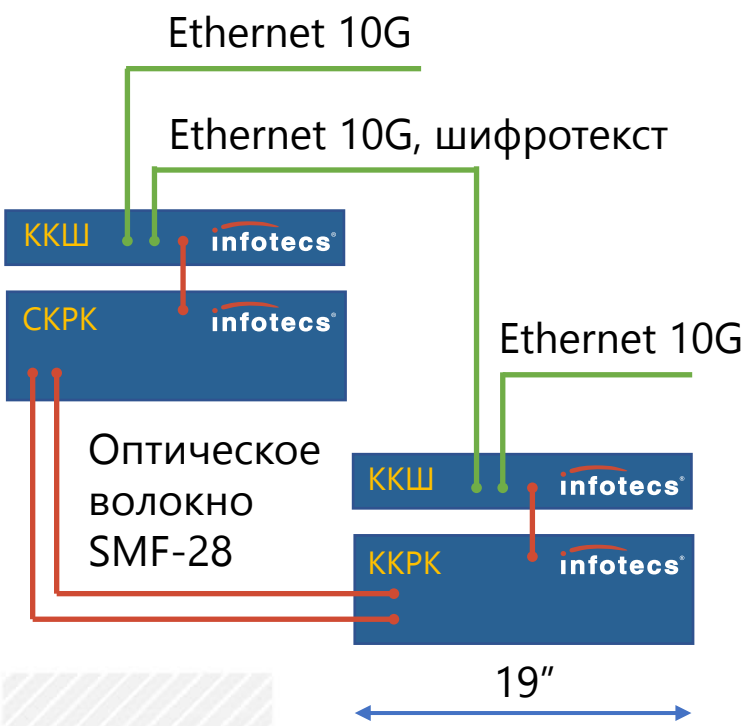


ViPNet Quandor

«Разработка и создание высокотехнологичного производства квантово-криптографической аппаратуры защиты информации»

по договору №03.G25.31.0254 с Министерством образования и науки РФ

Состав и характеристики ViPNet Quandor



ККШ - квантово-криптографический шифратор

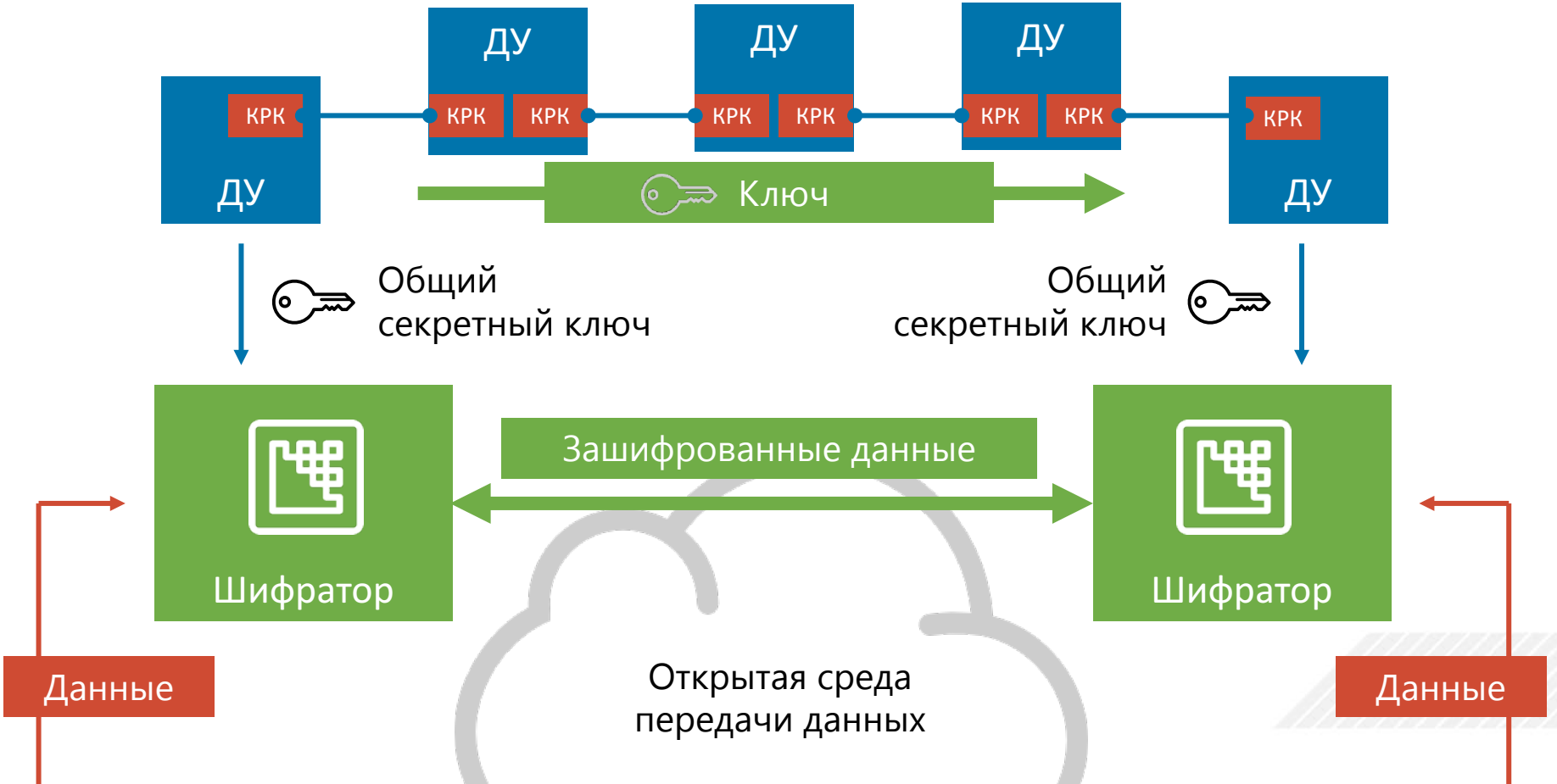
- скорость шифрования по ГОСТ 34.12-2015 «Кузнечик»:
  - До 20 Гбит/с
- имитозащита
- задержка ~15 мкс

СКРК – сервер, ККРК – клиент КРК

- длина линии квантовой связи 100 км
- воздушное охлаждение
- автоматический режим работы
- доказуемая секретность протокола

Квантовая сеть для распределения ключей

через цепочку доверенных узлов



Квантовый телефон ViPNet

Квантовый телефон ViPNet

Интеграция двухпроходной аппаратуры квантового распределения ключей и системы криптографической защиты сетевого трафика

ViPNet VPN ViPNet Client

ViPNet Connect

Квантовый телефон ViPNet

- Квантовое оборудование проверено на реальной телекоммуникационной линии Ростелекома длиной 25 км
- Устойчивая работа лабораторного образца в течение месяца
- Есть потенциал для миниатюризации
- Успешно осуществлена пилотная интеграция с VPN ViPNet
- Подготовлен демо-стенд

Квантовый телефон ViPNet

Принципы построения ключевой системы

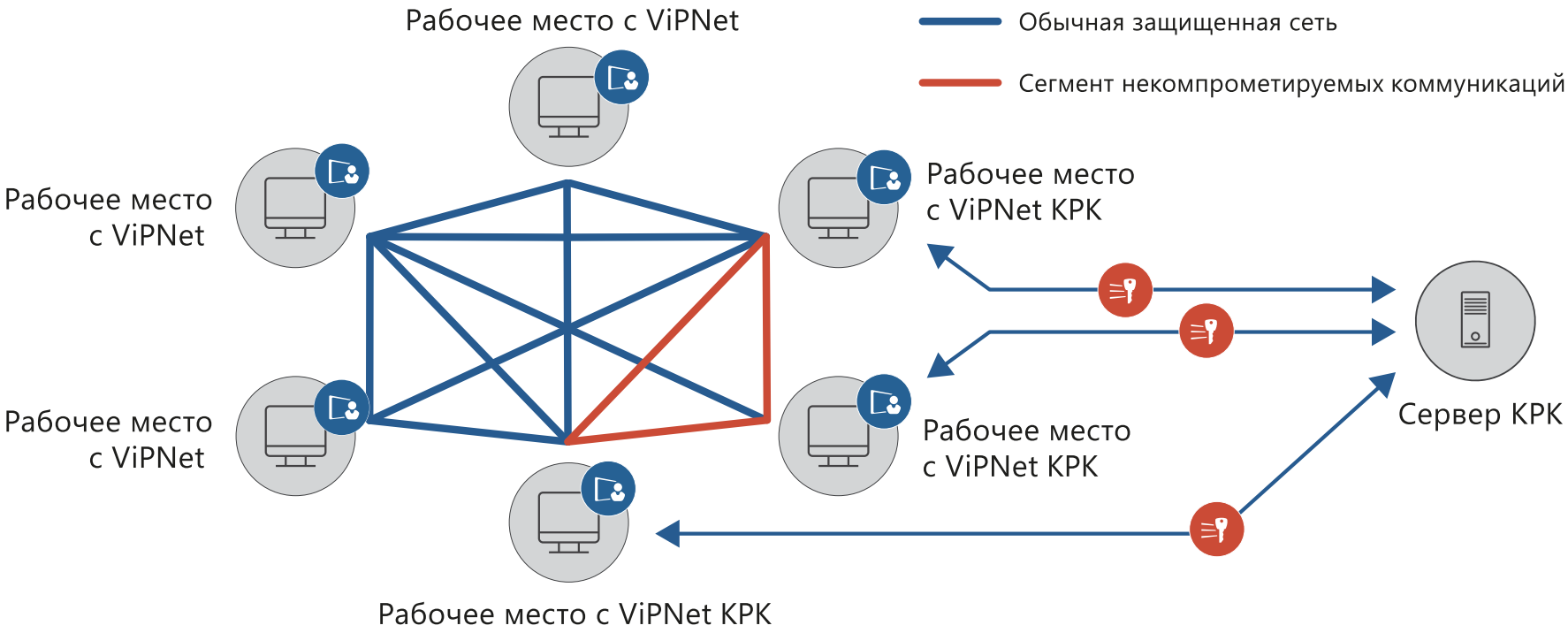
Переход от квантовых ключей к квантово-защищенным классическим ключам

Экономически обоснованное решение при небольшом трафике

Некомпрометируемое согласование ключей парной связи

Квантовый телефон ViPNet

Принципы построения ключевой системы



ViPNet VPN

- Российский VPN – 20 лет развития и успешной эксплуатации
- Доверие крупнейших заказчиков
- Централизованное управление сетью
- Широкая продуктовая линейка
- Сертификаты ФСБ, ФСТЭК

Системный подход ИнфоТеКС к защите информации с КРК

- Интегрированный комплекс квантовой и криптографической аппаратуры, а также программного обеспечения
- Следование требованиям регулятора при реализации аппаратных и программных средств защиты информации
- Криптографически стойкая аутентификация сторон
- Корректное использование квантовых ключей для шифрования данных
- Практически ценные целевые сценарии применения интегрированного комплекса

ТК 26

В ТК26 ведется работа по разработке и стандартизации квантового-криптографического протокола


infotecs®
ВЗГЛЯД В БУДУЩЕЕ:
ВЫЗОВЫ И ВОЗМОЖНОСТИ

Этапы развития технологии КРК на рынке сетевых средств защиты информации

Разработка тиражируемой аппаратуры КРК
2018-2019

Сертификация и первые внедрения шифраторов с аппаратурой КРК
2019-2020

Этапы развития технологии КРК на рынке сетевых средств защиты информации

Получение опыта эксплуатации, формирование рынка и разработка второго поколения продуктов повышенной надежности, оптимизированных габаритов и стоимости
2019-2021

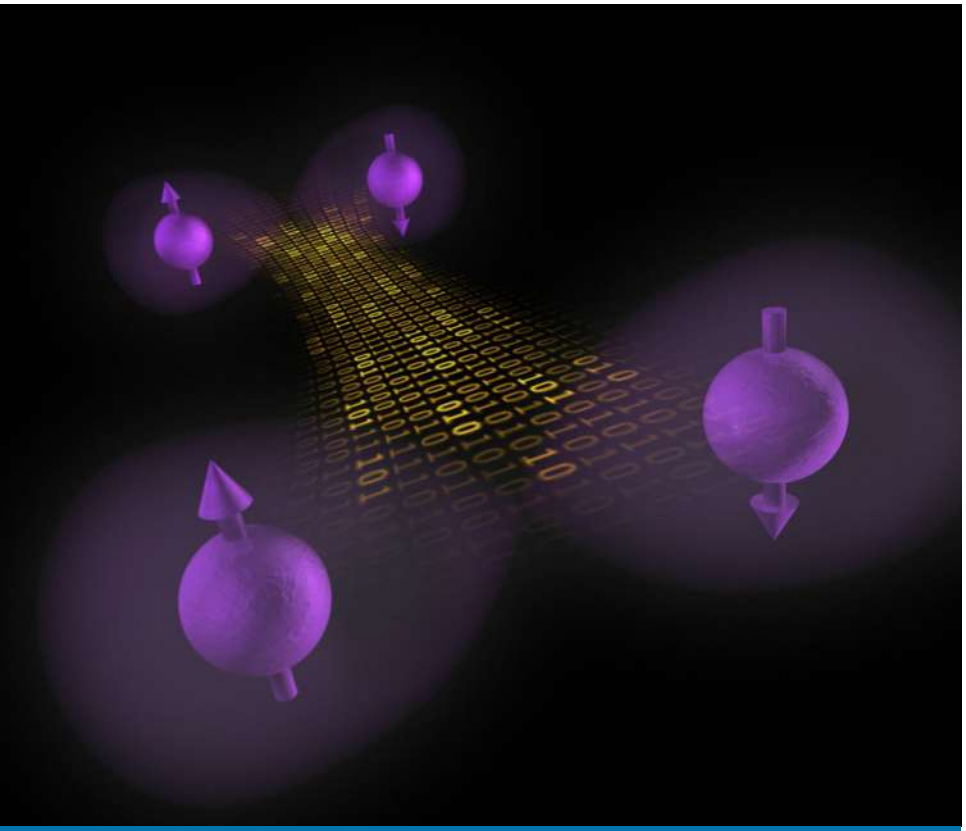
Построение географически распределенных сетей КРК и сервисов на их основе –
2020-2024

Этапы развития технологии КРК на рынке сетевых средств защиты информации

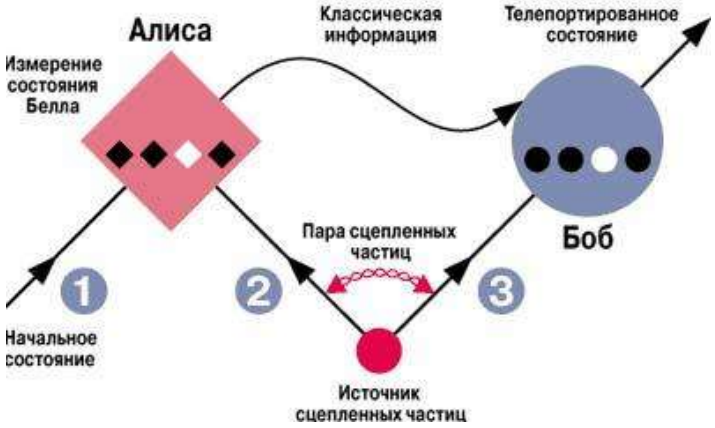
Миниатюризация аппаратуры КРК и массовое внедрение

>2024

Заглянем в будущее



Квантовая телепортация



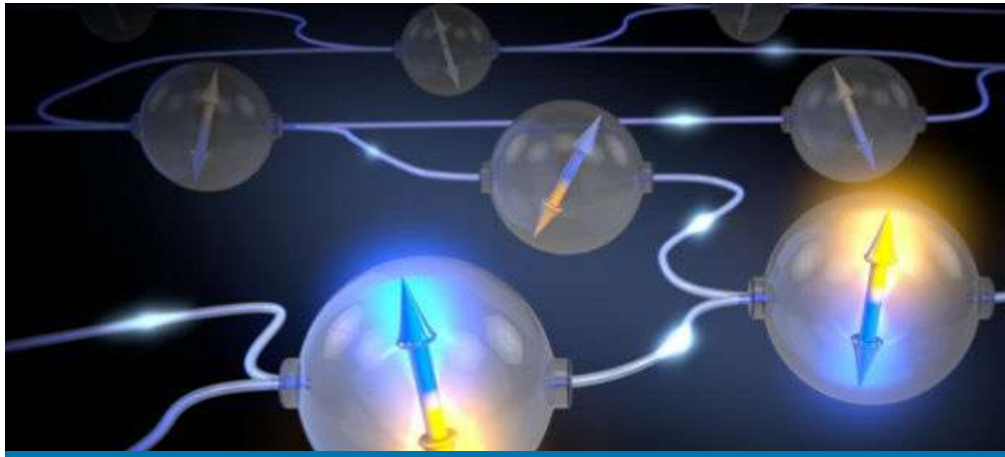
А может и не будущее...? ☺

Наша цель - построить оптически подключенную сеть из многих (малых) квантовых компьютеров. Такая сеть позволяет обмен квантовыми битами между любыми связанными квантовыми процессорами для решения проблем, которые трудноразрешимы классически.

Квантовая сеть, в которой процессоры расположены в разных географических точках, называется **квантовым Интернетом**. Наша цель - разработать технологию, позволяющую осуществлять квантовую связь между любыми двумя местами на Земле.

Одним из применений такого квантового Интернета является обеспечение принципиально безопасного способа общения, в котором конфиденциальность гарантируется законами физики. © QuTech

www.qutech.nl



Quantum Internet and Networked Computing

Ученые планируют реализовать такую сеть между несколькими квантовыми узлами… «В 2020 году мы хотим связать четыре города в Нидерландах посредством квантовой запутанности. Это будет самый первый квантовый интернет в мире»
Июнь 2018, Nature

infotecs®

СПАСИБО ЗА ВНИМАНИЕ