КриптоПро

Российская криптография и технологическая независимость

Смышляев Станислав Витальевич,
д.ф.-м.н., генеральный директор, КриптоПро

Суровая правда в области внедрения средств [криптографической] защиты

Реальность

1. Заказчики не восхищаются достижениями криптографии, а ищут решения для выполнения требований НПА.
2. Регуляторы, опираясь на состояние курируемых отраслей, вводят или ужесточают требования и выпускают новые НПА.
3. Разработчики дорабатывают свои решения.

Появление новых областей

1. Создаются прорывные решения.
2. Заказчики-новаторы их внедряют.
3. Регуляторы очерчивают границы, содействуя [обычно] развитию конкуренции.

В криптографии: обязанность применять российские решения разработки лицензиатов ФСБ России.

Причины для широкого внедрения российских криптосредств

1. Требования по импортозамещению.
2. Трудности с закупкой иностранных средств из-за санкций.
3. Требования регуляторов в сфере ИБ по применению российских криптосредств.

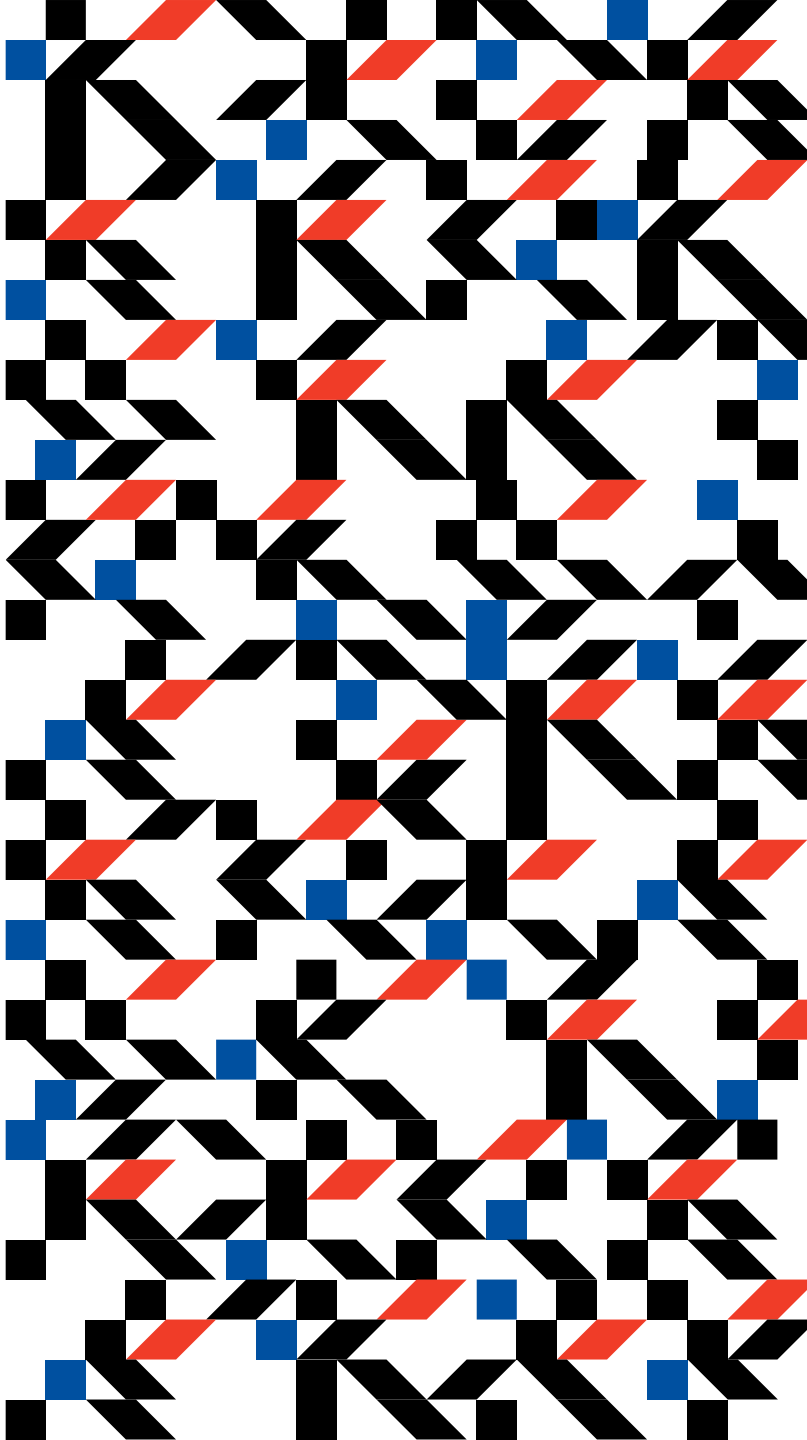
Важнейшие импульсы, но бесполезные без качественных передовых СКЗИ.

Для истинной независимости:

Достижения, ценные не только самодостаточностью и выполнением требований регуляторов, но и своими техническими характеристиками и научной базой.

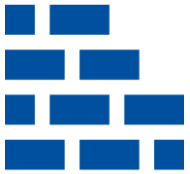
И в российской криптографии их немало.

Передовые наработки криптографической школы



Передовые наработки криптографической школы

Ключевое преимущество – **наработки криптографической школы.**



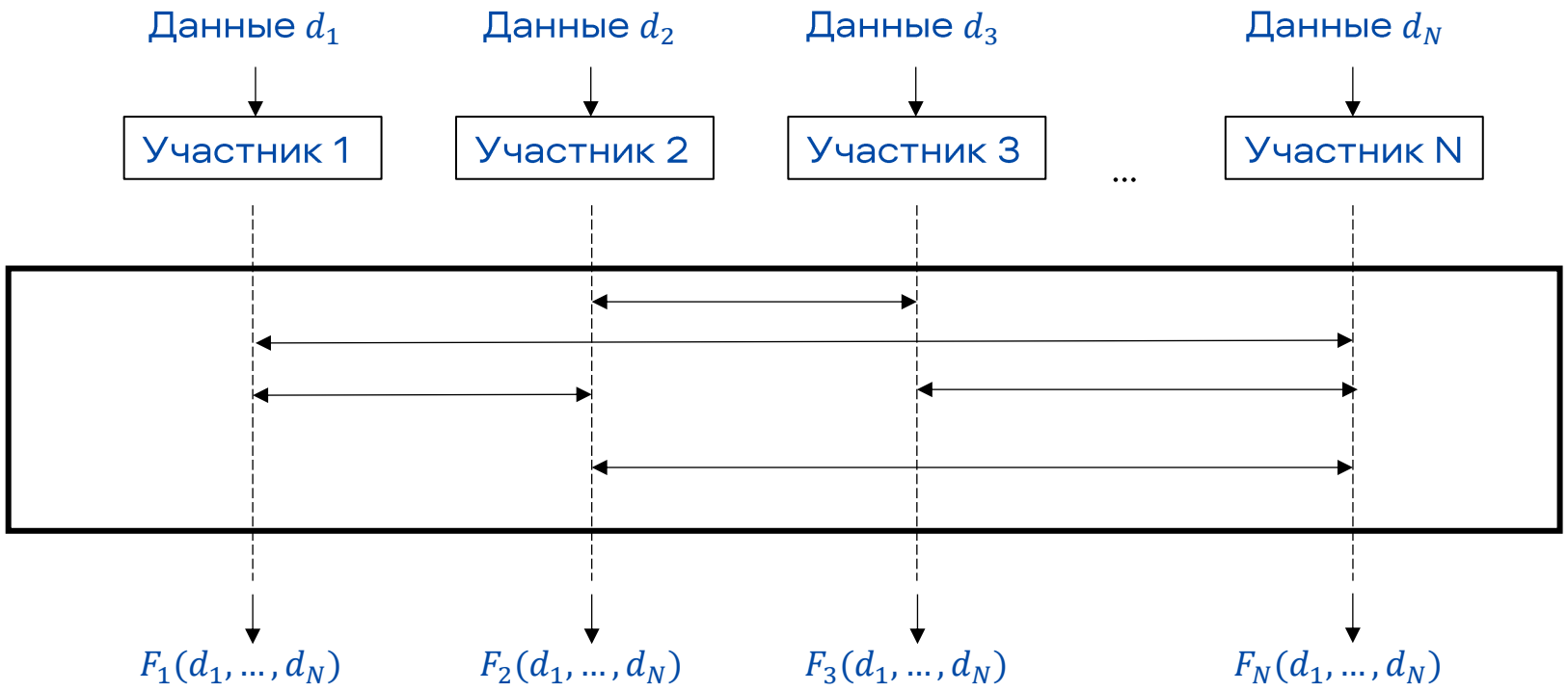
Базовые алгоритмы – необходимый фундамент,
без которого нельзя говорить о суверенитете.

Опережение дают не сами базовые алгоритмы, а их применение в протоколах:

- Применение в мобильных устройствах, с компенсацией угроз слабодоверенного окружения.
- Распределенные реализации ЭП.
- Защита соединений на основе пароля, SESPAKE, безопасный доступ к ключам.
- Протоколы систем дистанционного электронного голосования.
- Конфиденциальные вычисления.

Конфиденциальные вычисления

Задача: вычислить значение **функции** с использованием **данных нескольких участников**, обеспечивая при этом **необходимый уровень конфиденциальности** входных и выходных данных, вычисляемой функции и промежуточных значений.



Задачи конфиденциальных вычислений

Дистанционное электронное голосование

Банковский скоринг

Мобильная ЭП для применения на массовых устройствах

Распознавание человеческой активности

Выявление фактов мошенничества в финансовом секторе экономики

Вычисление среднего рейтинга пользователя сервисом

Генетические и медицинские исследования

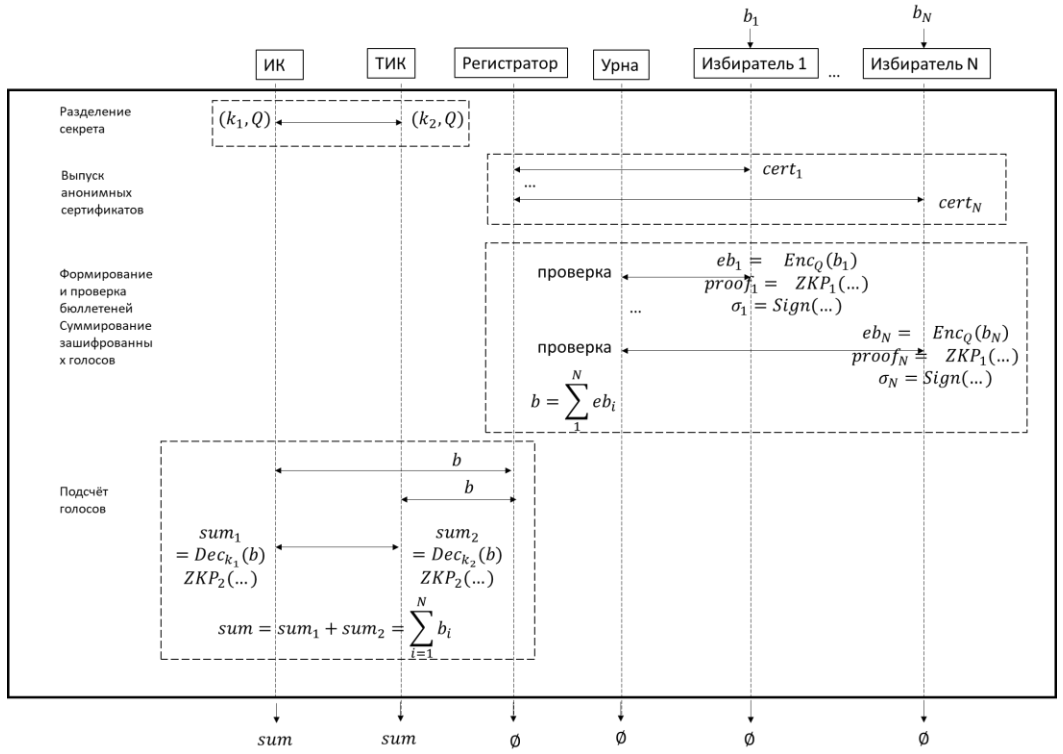
Определение перспективной категории малого бизнеса

Оценка эффективности рекламной кампании

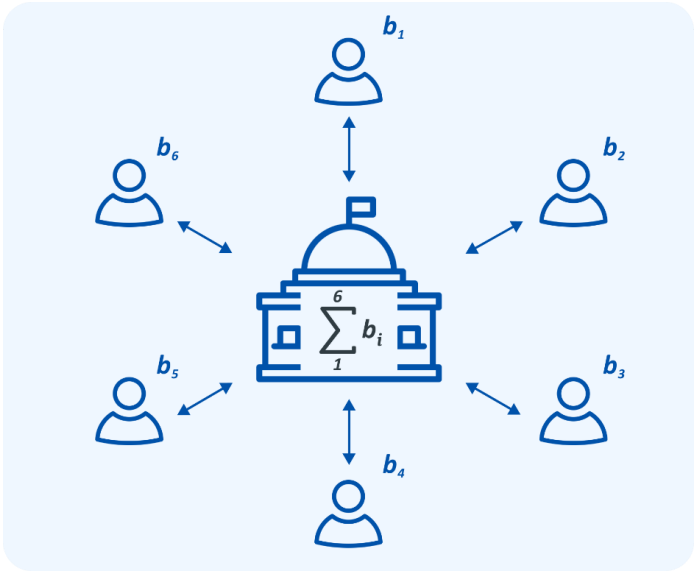
...

Дистанционное электронное голосование

Задача: посчитать сумму голосов, обеспечив сохранение тайны голосования



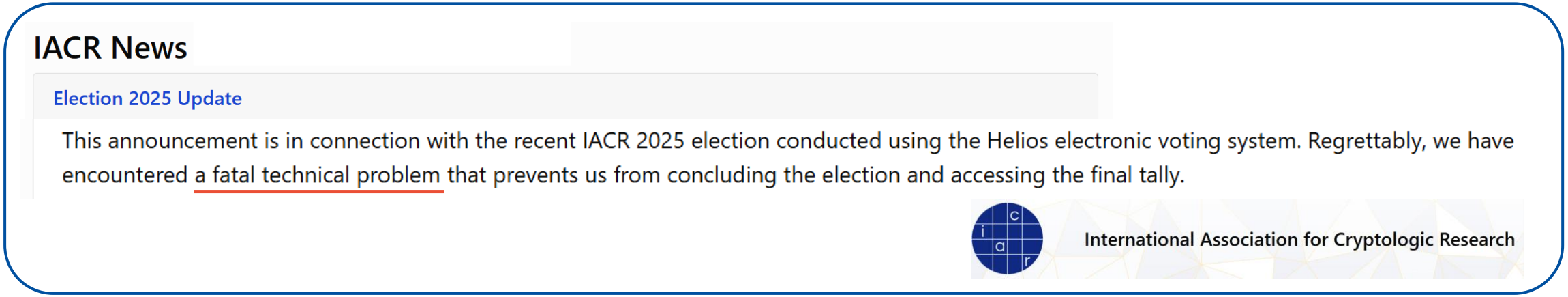
- Схема подписи вслепую.
- Схема подписи ГОСТ 34.10-2018.
- Схема разделения секрета.
- Два протокола доказательств с нулевым разглашением (ZKP).
- Схема гомоморфного шифрования.



Мировые аналоги

Мировой опыт:

Системы за рубежом в основном проработаны на уровне красивой теории без учета суровой реальности, либо имеют слабые гарантии безопасности в актуальных для ДЭГ моделях.



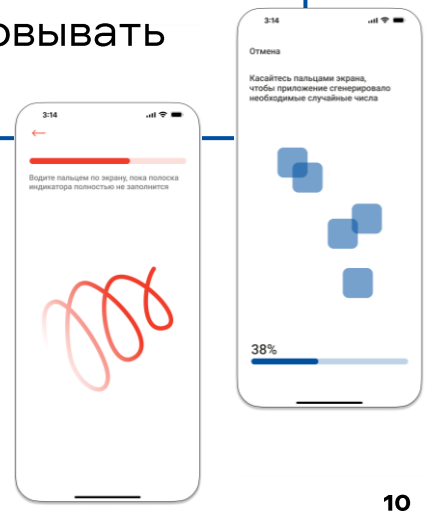
Ключевые требования к отечественному ДЭГ:

- Устойчивость к реальным кибератакам.
- Работа под сильнейшим давлением, в том числе исходящим от недружественных государств.
- Обоснование каждого решения.

Массовая мобильная ЭП

Необходимость работы в слабодоверенном окружении:

1. Безопасное хранение ключевой информации в ОЗУ (маскирование, смена ключа, CTR-ACPKM), снижение риска утечки из-за уязвимостей.
2. Протоколы двусторонней электронной подписи.
3. Знания CryptoAPI и интеграции в ОС: Cloud CSP, нет аналогов в мире.
4. БиоДСЧ: уровень безопасности всегда требовался не ниже того, который разработчики кошельков для криптовалют начали реализовывать в 2020-х годах.



Подробнее: секция «Мобильные решения и криптография»

Массовая мобильная ЭП

Госключ

КриптоКлюч

PayControl ГОСТ

КриптоПро Ключ

Альтернатива:

Мобильная электронная подпись вместо ПЭП и подтверждения по СМС.

Уникальный пример повышения безопасности:

Требования Банка России (851-П).

Преимущество не из области ИБ:

Экономия денег на СМС.

Подробнее: секция «Мобильные решения и криптография»

Платежные HSM

Сбербанк: самый нагруженный эквайринг мира полностью на **отечественных HSM**

Финансы · 17 октября 2025, 16:04

Сбербанк обогнал JPMorgan и впервые возглавил рейтинг мировых эквайеров

В прошлом году Сбербанк занимал в рейтинге второе место, а теперь смог сместить с этой позиции JPMorgan. В число 150 крупнейших эквайеров вошли еще шесть российских банков

14 августа 2025 года:

В Музее криптографии прошло мероприятие «Импортозамещение платёжных криптографических HSM-модулей: теория, практика, обмен опытом».

Результат: возможность реагировать на специфичные запросы (доработки, специфичные для конкретной системы ошибки).

Крупнейшие российские банки успешно применяют российские платежные HSM-модули в большом количестве.

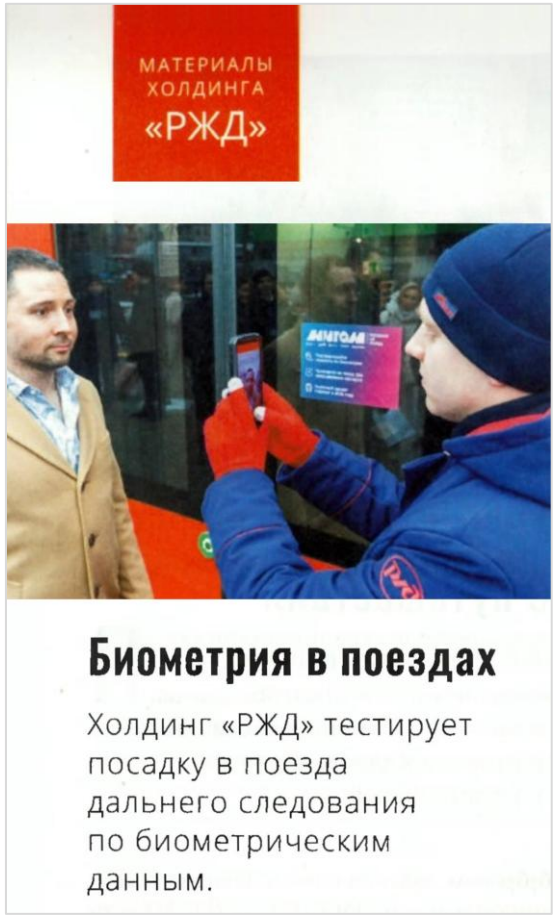
Благодаря совместной работе НСПК, ЦБ и разработчиков СКЗИ российские платежные HSM-модули первыми среди аналогичных решений получили поддержку современных криптографических алгоритмов, в том числе алгоритма Шнорра, опередив международного лидера Thales.

№1

Биометрические системы и криптография в России: безопасность и массовость

Российский опыт:

- ЕБС и КБС: надежная защита на всех уровнях позволяет развиваться сервисам.
- Единые жесткие требования по криптографической защите – работающий механизм, а не формальность.
- Реальная борьба с риском утечек (обратный пример: Индия, утечки Aadhaar).
- Интерес к российскому опыту из-за рубежа из дружественных стран.
- Безопасность не мешает массовости:
  - сервис «Оплата улыбкой»;
  - сервис «Мигом» – посадка на поезд и на самолёт по биометрии.



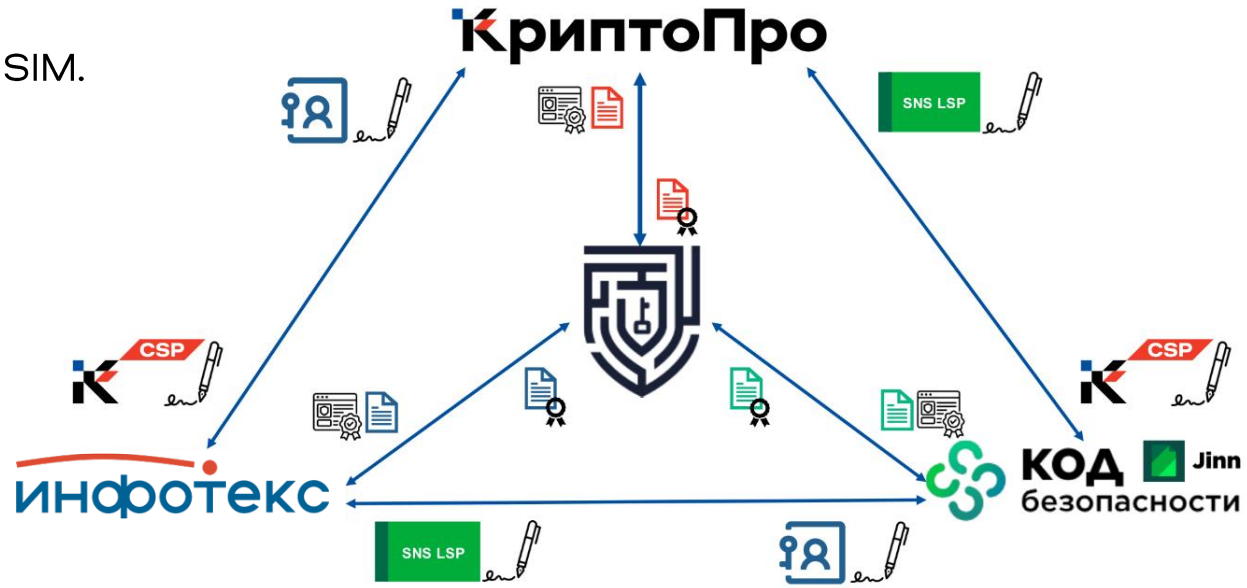
Обеспечение доверия к российскому ПО

Объективные трудности в области корня доверия:

- Нет своих TPM в устройствах пользователей для корня защиты.
- Нет массового распространения своих чипов.
- Только ведутся работы в части чипов и в части SIM.

Что уже есть:

- Суверенные системы обеспечения доверия к ПО для сред российских ОС (Astra Linux, Аврора).
- Десятки лет наработок по развитию систем доверенной доставки криптосредств у разработчиков СКЗИ.
- Рабочая группа по развитию системы применения меток доверенного кода.



Подробнее: секция «РБПО и подпись ПО, построение единого пространства доверия к российскому программному обеспечению»

HSM как ядро защиты системы

Опора на HSM для обеспечения корней доверия в информационных системах (в условиях отсутствия массового TPM)

Применение HSM в ЦФА

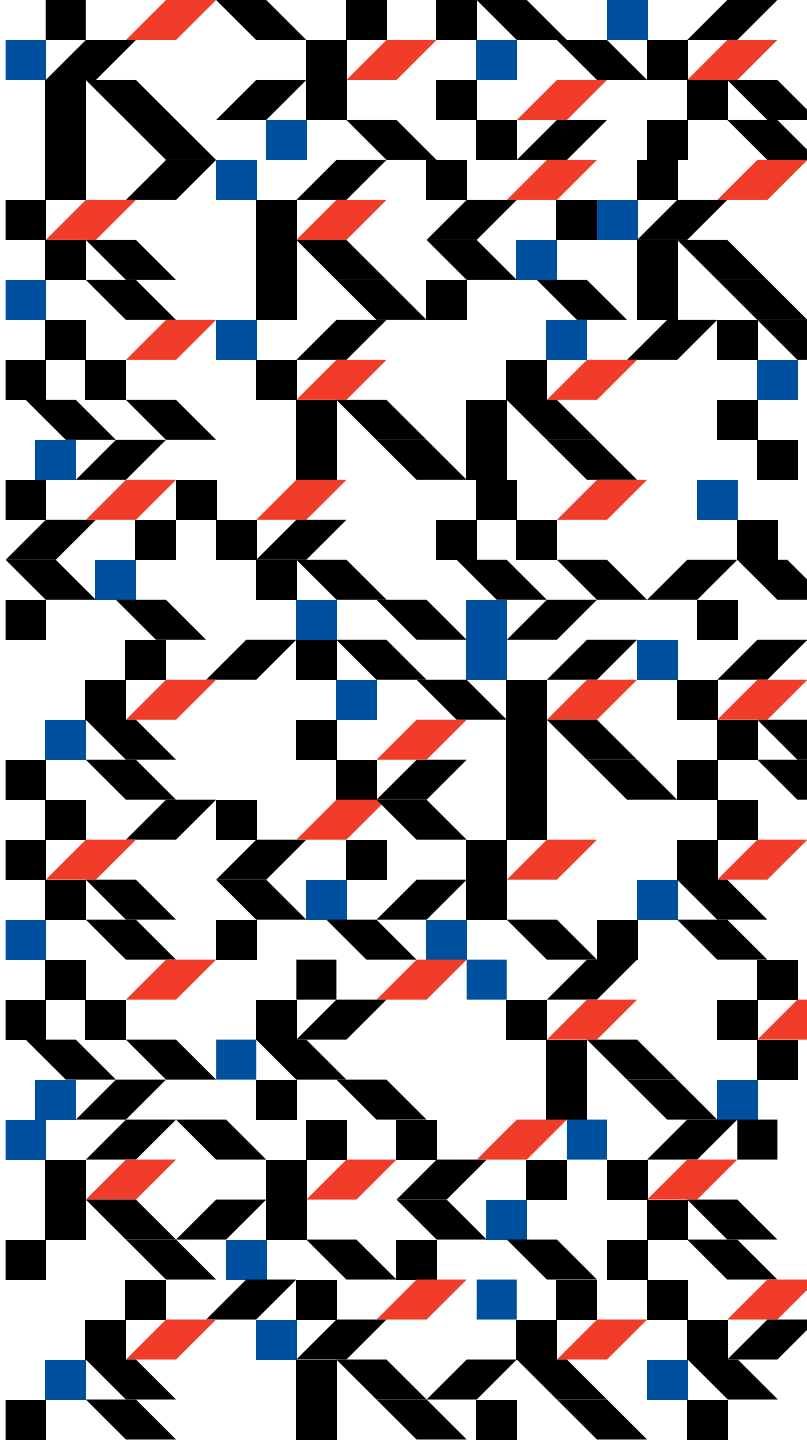
Конфиденциальные вычисления

Доверие к источникам случайности и защита данных в docker-образах, виртуальных машинах

Опыт с многочисленными УЦ, мобильной ЭП и внедрением HSM для ЭП → Эффективное и успешное внедрение Цифрового рубля

Подробнее: секция «Информационная безопасность и криптография кредитно-финансовой сферы»

Успехи промышленности



Успехи промышленности

1 **Близость к заказчикам:** понимание потребностей заказчиков, быстрая реакция.

2 **Защита источников случайности:** собственная разработка с нуля (не было возможности опереться на встроенную).

3 **Разработки и защита** в условиях слабодоверенного окружения.

VPN-решения

Работа через протокол TLS: хуже работает на плохих каналах (TCP over TCP), но единственная возможность работы из WiFi-сетей (например, в гостиницах), где открыты только порты 80 и 443.

Преимущества:

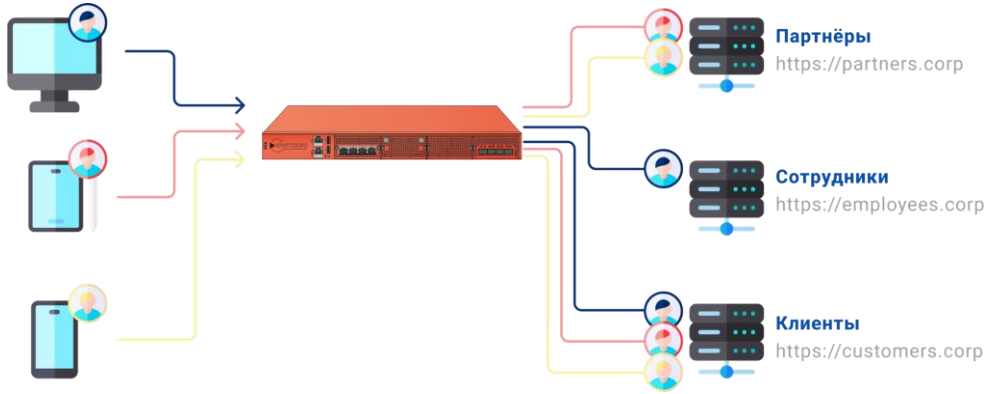
1. Высочайшая производительность без аппаратных ускорителей и расширений процессора.

2. Обширный перечень поддерживаемых платформ/операционных систем.

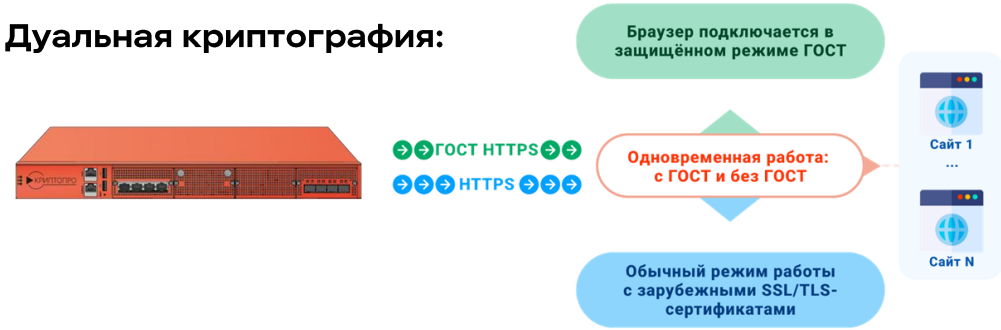
3. Универсальность:

- На одной инсталляции несколько логически изолированных сущностей для разных целевых групп/ролей.
- Поддержка двух криптографических фундаментов (ГОСТ/RSA) из коробки.

Разные целевые группы:



Дуальная криптография:



Российская криптография и аппаратные решения

1) Безопасные и быстрые решения на стандартной, не предназначенной специально для криптографических средств элементной базе:

- Оптимизированные криптографические библиотеки для микроконтроллеров.
- Быстрая криптография без криптографических сопроцессоров.
- Отсутствие заимствований: работают только свои написанные с нуля библиотеки (с учетом всех известных ошибок зарубежных разработчиков).
- Единая кодовая база для разных аппаратных платформ и микропроцессорных архитектур.
- Уникальные подходы для защиты от инвазивных и неинвазивных атак.

2) Максимальный контроль стека технологий для большей защищенности:

- Собственные bootloader-ы.
- Избегание любого стороннего кода внутри микропрограмм.

3) Процессы разработки и производства, архитектура, позволяющие быстро адаптироваться и незаметно для потребителя менять элементную базу аппаратных решений.

4) Развитие в рамках единых подходов, обеспечение совместимости со всеми российскими решениями, быстрое внедрение для новых применений в создаваемых информационных системах.

Криптографические решения для промышленных систем и IoT/IIoT

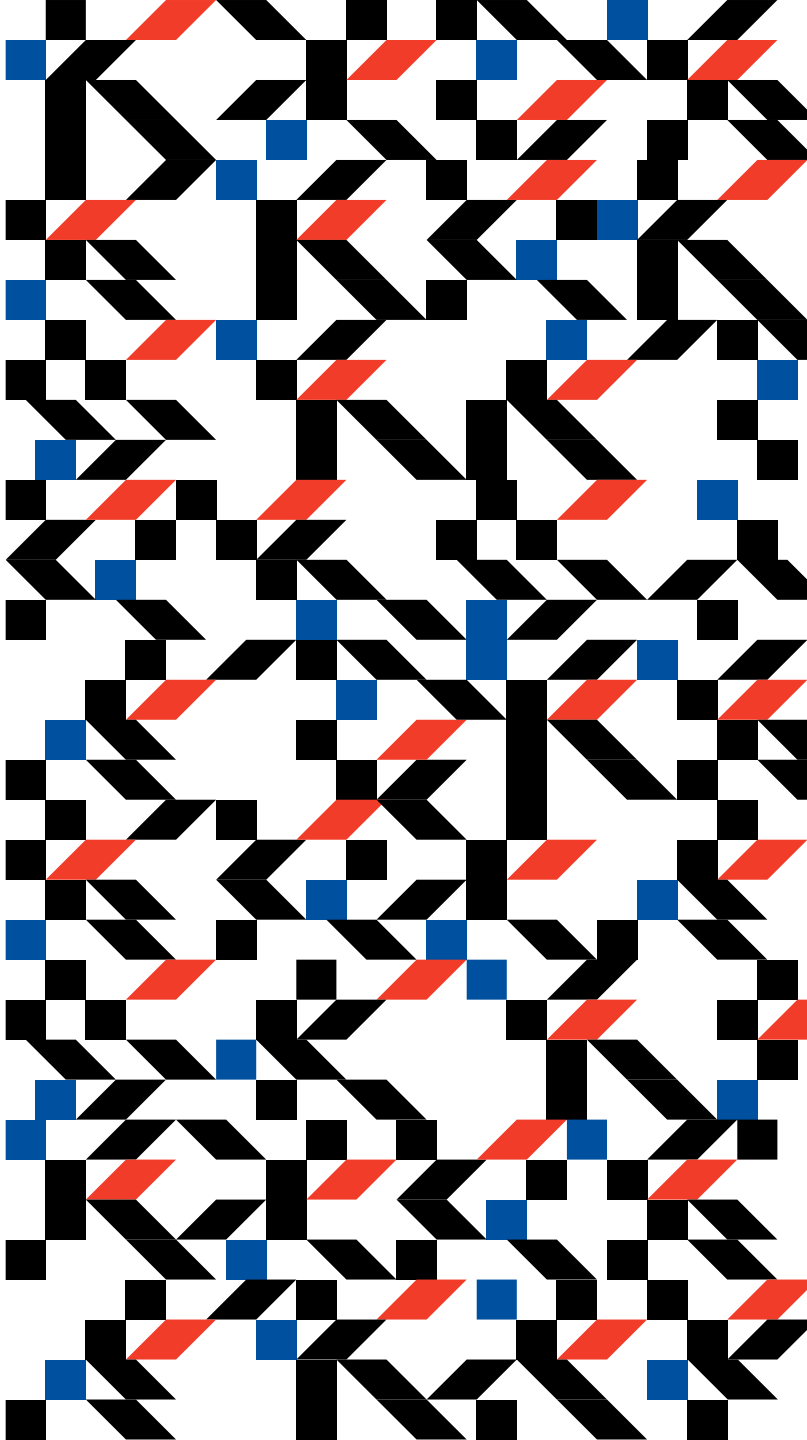
Зарубежные решения строятся на протоколах IPsec/TLS:

- Требуются существенные вычислительные возможности от конечных вычислительный устройств (в т.ч. с ГОСТ).
- Ненадёжность работы на нестабильных каналах.
- Требуется оптимизация PKI и поддержка специальных форматов сертификатов безопасности.

Отечественные разработки:

- В российских криптонаборах TLS внесены меры защиты, позволяющие эффективно и безопасно использовать их в промышленных системах и IoT.
- В России разработан и стандартизован ТК 26 специализированный протокол **CRISP (ГОСТ Р 71252–2024)** для криптографической защиты данных в промышленных системах, использующий симметричную криптографию ГОСТ, с минимальными накладными расходами на защищаемые данные – зарубежных аналогов этого протокола не известно.
- Разработаны и сертифицированы российские СКЗИ для промышленных систем, допускающие необслуживаемые режимы работы сроком до 16 лет, и уже начались массовые внедрения продуктов и решений на базе российских протоколов, в частности в энергетике.

Ближайшее будущее



Разумное применение постквантовой криптографии

1) Квантовое распределение ключей и постквантовая криптография: разумное внедрение.
2) Отсутствует давление для необдуманно быстрого перехода.
3) Переход через гибридные KEMы.
   - Внедрение постквантовых механизмов в протокол TLS.
   - Внедрение постквантовых механизмов в CMS.
   - Внедрение постквантовых механизмов в PKI.
4) Перспективные версии массовых СКЗИ.

Массовая постквантовая криптография: план действий

1) Работать, не дожидаясь стандартизации базовых механизмов в ТК 26.

- Механизмы: синтез, анализ.
- Сопутствующие алгоритмы и процедуры: синтез, анализ.
- Протоколы: выбор решений по доработке протоколов.
- Документы: перечень требуемых стандартов/рекомендаций и НПА (форматы сертификатов, электронных документов и т.п.).
- Макетирование и испытания: проверка функциональных свойств.
- Реализации: доработка СКЗИ (пока в экспериментальном режиме).
- Методики: исследования СКЗИ, встраивание в ИС, оценка влияния.

2) Учитывать зарубежный опыт и подходы (например, draft-ietf-pquip-pqc-engineers).

3) Реалистичная цель: в течение 5 лет после стандартизации механизмов перейти в средствах массовой криптографии на поддержку гибридных схем.

- ТК 26, НТЦ ЦК, разработчики СКЗИ и лаборатории
- Поиск и обсуждение решений на секциях CTCrypt и РусКрипто.

Платежные HSM: что дальше?

1 **Новые алгоритмы для 2031 года**

Устранение ряда родовых травм криптографии в стандартах PCI.

2 **Требования ФСБ России**

Ограничения, которые дают возможность творчества.

Выводы

1

Честное
осознание трудностей.

2

Важность осознания
реальных преимуществ
российских криптосредств.

3

Продолжение
развития сильных сторон.

4

Учет
замечаний заказчиков.

5

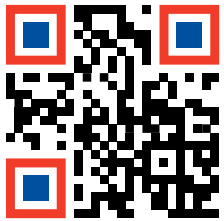
Уважение к зарубежному
опыту, взаимодействие в
рабочих группах.

6

Развитие уважительной
и честной конкуренции внутри
страны, содействие развитию
в условиях соперничества.

Настоящая независимость и свобода: не только замена, а перенятие лучшего и создание превосходящего с учетом пожеланий потребителей, соотечественников.

Спасибо
за внимание



svs@cryptopro.ru
www.cryptopro.ru