МОСКОВСКИЙ АКСЕЛЕРАТОР

Skolkovo

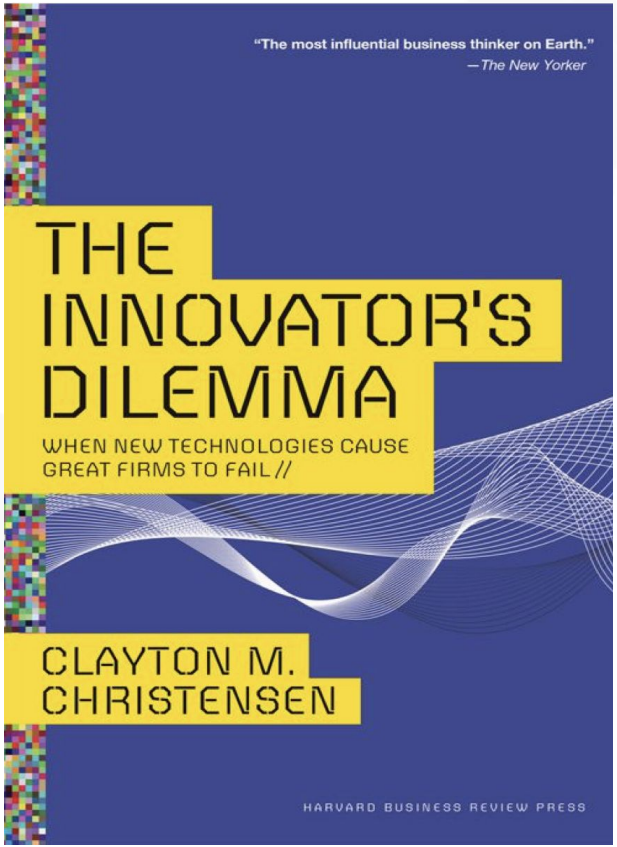
Сеть распределенной многофакторной идентификации

Сергей Вельц
Email: sales@cybertonica.ru

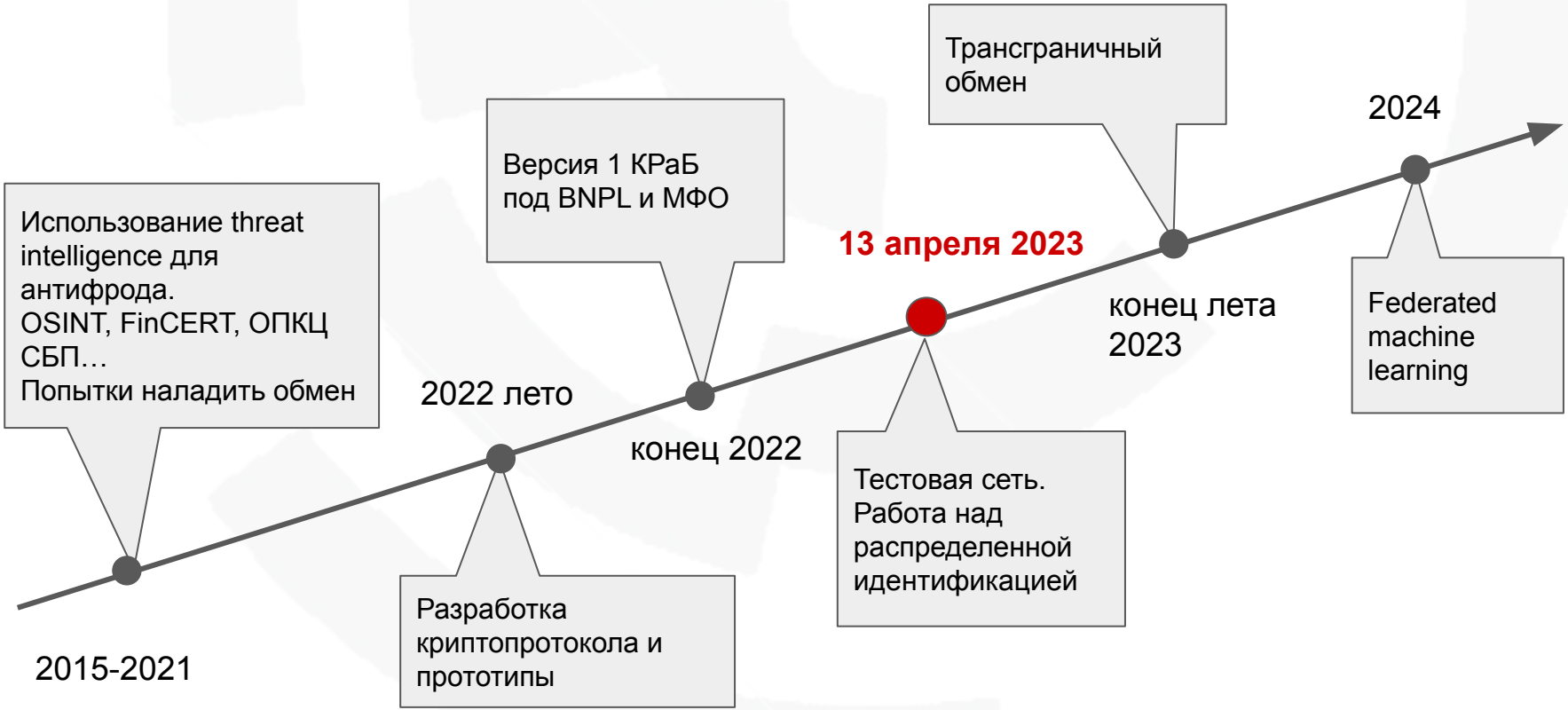
cybertonica

План доклада

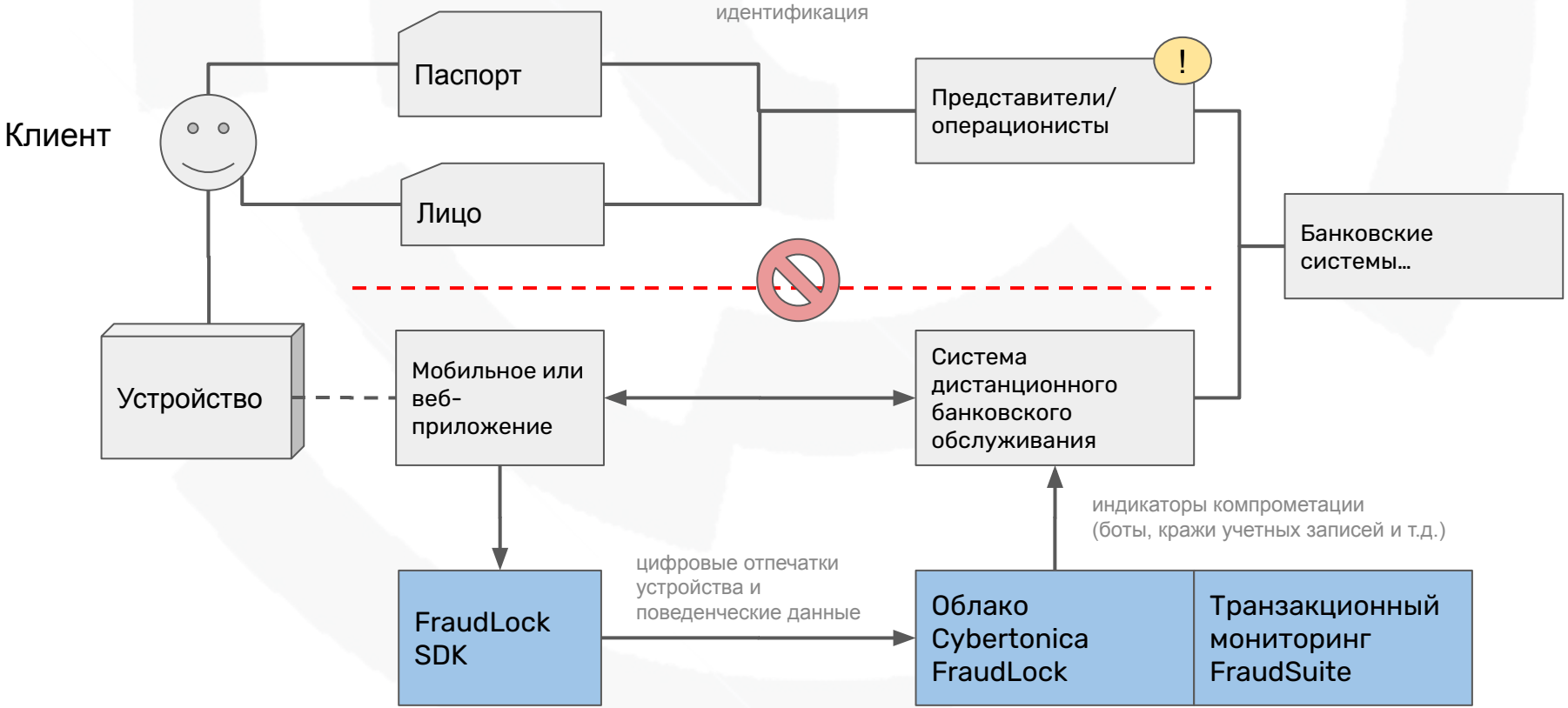
1. Сессионный мониторинг и аутентификация
2. Распределенное хранение данных на основе криптопротокола
3. 1-ое + 2-ое = Распределенная идентификация



Эволюция идеи



Сессионный мониторинг и аутентификация



Цели

1. Усилить общий уровень безопасности за счет коллективной работы 👬
2. Обеспечить механизм совместной работы конкурирующих между собой игроков на рынке. 🐁
3. Минимизировать работу с чувствительными данными (ПДн) 🔐

Схема решения КРаБ - Криптографическая Распределенная База

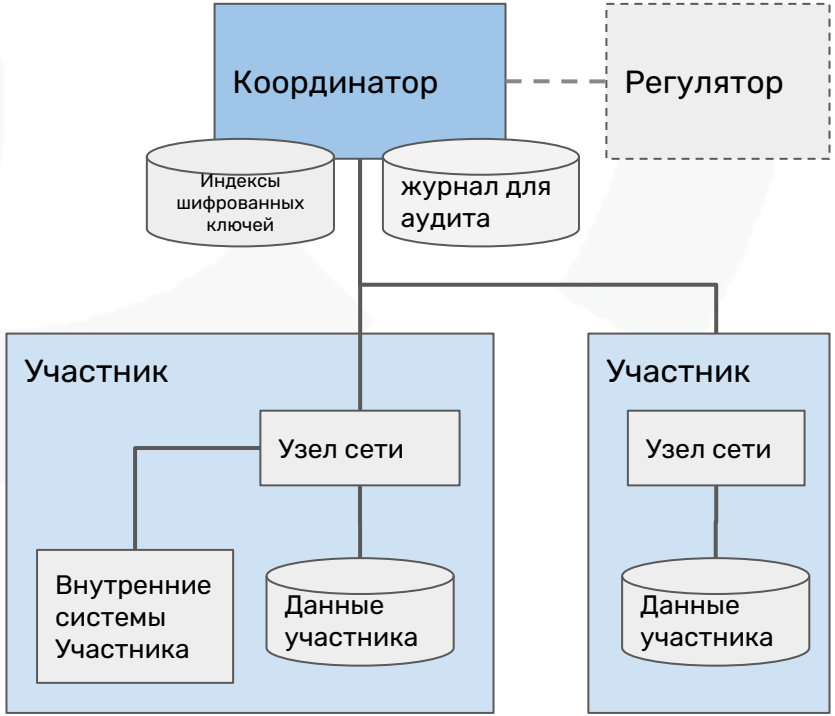
Закрытая распределенная двухранговая сеть.

Координатор аутентифицирует участников и обезличивает коммуникацию между ними, хранит журнал. Участники хранят свои данные.

Этап 1: Поиск данных на основе криптографического протокола private set membership test на базе криптографии на эллиптических кривых - запрашивающий не раскрывает по какому именно субъекту запрашивает данные.

Этап 2: Забывчивая передача (oblivious transfer) - Координатор запрашивает у участников данные, содержащие нужный ключ таким образом что при этом участники не узнают идентификатор субъекта и кто запрашивает данные.

Этап 3: Координатор проверяет целостность закупленных данных и соблюдение протокола, возвращает запрашивающей стороне наборы данных. Сделка фиксируется в журнале для возможность аудита со стороны регулятора для соблюдения регуляторных требований.



Гарантии безопасности КРаБ

1) **Децентрализация**. Каждый участник хранит и контролирует свои собственные данные, координатор ведет учет, но данные *не хранит*.
2) **Обезличенность**. Участники сети, за исключением запрашивающего, не могут однозначно идентифицировать субъекта по которому запрашивается информация, это предотвращает кражу лидов.
3) **Анонимность**. Участники сети не знают кто с кем обменивался информацией и кому принадлежат полученные записи.
4) **Журналирование**. Координатор записывает факты сделок, для возможности проводить аудит, и контролирует участников на предмет недобросовестного поведения (перебор, синтетические данные, и др.).

Каждый узел - независимая виртуальная машина, стоящая у участника. Развертывание занимает один день (не считая интеграции API).

Вместе с доступностью ≥ 99.9% Координатора это обеспечивает надежность сети.

Распределенная идентификация

Проблемы:

1. В онлайн:
   a. массовые выдачи
   b. сбор паспортных данных снижает конверсию
2. В оффлайн: недобросовестные операционисты/агенты (внутренний фрод)

Надо:

1. Сделать для мошенника создание синтетической личности дороже в 10 раз
2. Замедлить создание синтетической личности в 10 раз
3. Воспользоваться тем, что в ряде место сейчас идентификация уже есть.
4. Создать сетевой эффект между участниками для полноты анализа.

Решение:

Используется криптографически защищенное распределенное хранилище FraudHub.

Ключ: Номер телефона
Данные:

1. **Дата последней верификации паспорта**
2. **(опционально) Дата последнего входа в ДБО с проверкой биометрии**
3. **(опционально) FraudLock deviceID.**

Каждый раз когда выполняется идентификация - пишется (дата, телефон, успешная проверка, флаги)

В итоге: по номеру телефона можно узнать когда человек с данным телефоном появлялся и предъявлял паспорт.

Итого: мошенникам придется купить sim, телефон, паспорт, сходить в отделение, ждать 6 месяцев

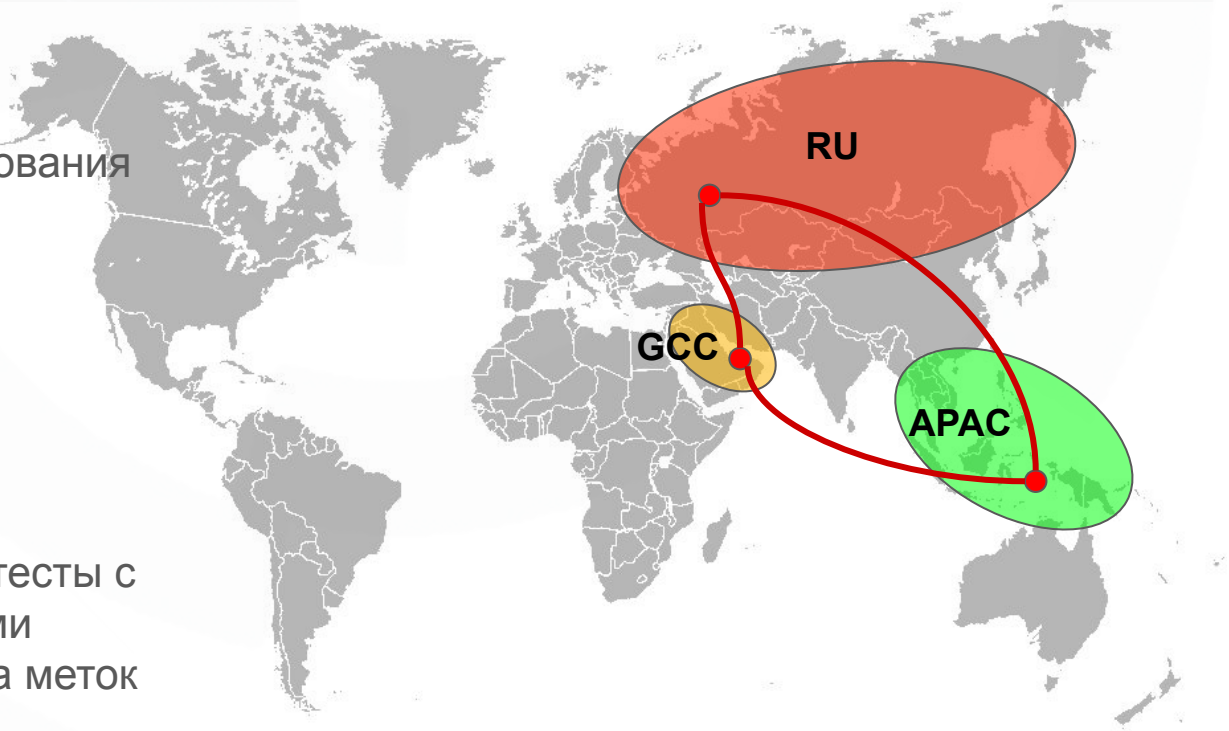
Трансграничная работа

На стадии CustDev, исследования рынка, переговоров

- Регион vs страна?
- Криптография?
- Юридическая часть
- Ищем партнеров

Техническая часть:

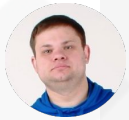
- сделали нагрузочные тесты с хорошими результатами
- реализация механизма меток безопасности / ACL.



О компании Cybertonica

- Технологическая компания в сфере финансовой безопасности основанная в 2015 выходцами из МГТУ им. Н. Э. Баумана, Сбербанка и платежной индустрии. Офисы в Москве и Дубае, резидент Сколково.
- Лауреат наград Sk Cybersecurity challenge, EPA Best data analysis, MPE backend innovation, EuroFintech Top100, победитель акселератора ВТБ & ФРИИ (2019), SAP & Минкомсвязь РФ (2020г)
- Продукты:
  - FraudSuite - мониторинг платежей
  - FraudLock - защита учетных записей
  - КРаБ[new] - конфиденциальный обмен данными
  - CbtProxy[new] - интеграция для подмены западных вендоров
- PCI DSS Level 1 (2017 - н.в.)
- Входим в Реестр отечественного ПО (2023г).
- Мониторинг более 150 млн платежей в месяц из 20 стран мира

Сергей Вельц
Технический директор и сооснователь
svelts@cybertonica.ru



Олег Кузнецов
Руководитель отдела по работе с заказчиками и партнерами
okuznetsov@cybertonica.ru

Евгений Шадрин
Операционный директор
eshadrin@cybertonica.ru