



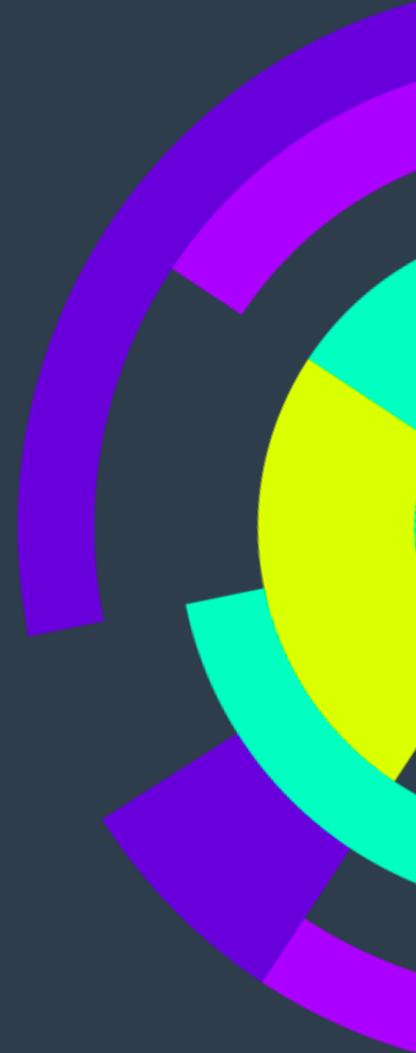
Мониторинг рисков в СБП

Пути решения

Евгений Шадрин

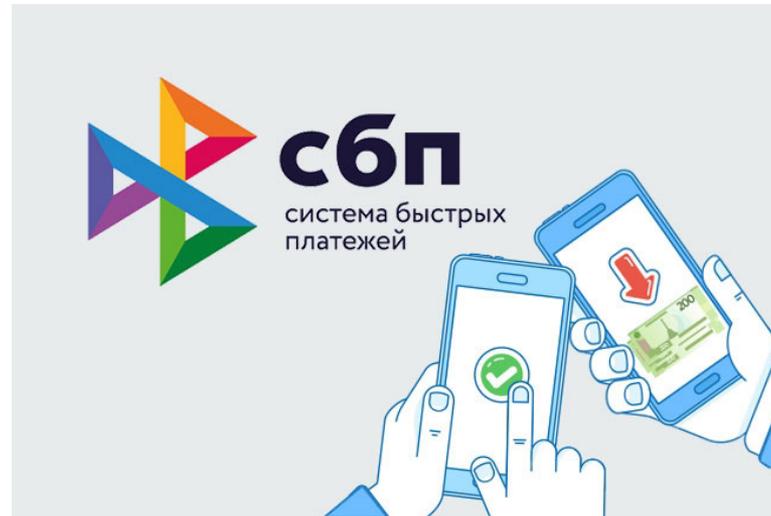
COO Cybertonica

eshadrin@cybertonica.com



План

- **Что мониторим**
- **Типы рисков**
- **Анализ рисков**
- **Проблемы**
- **Решения**



Что мониторим

- 30% рынка переводов
- 196 финансовых организаций
- 87 млн переводов
- 643 млрд рублей*

* По данным «Известия» на 3.12.20



* Статистика канала C2B за август 2020

Что мониторим

- Положение Банка России от 9 января 2019 г. № 672-П “О требованиях к защите информации в платежной системе Банка России”
- Стандарт ОПКЦ СБП. Порядок проведения мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента

Финансы, 11 ноя 2019, 11:17 | 34 453 | Поделиться

ЦБ предупредил о риске использования Системы быстрых платежей мошенниками

В разосланном банкам письме ЦБ предупредил о необходимости мониторинга вводимых в Систему быстрых платежей запросов. Ранее в ЦБ называли уровень риска в СБП нулевым

<https://www.rbc.ru/finances/11/11/2019/5dc90f969a79473ab9e5838a>

Система хитрых платежей

Мошенники нашли способ выводить деньги через СБП



Газета "Коммерсантъ" №151/П от 24.08.2020, стр. 1

<https://www.kommersant.ru/doc/4465889>

Риски

На стороне клиентов участников СБП:

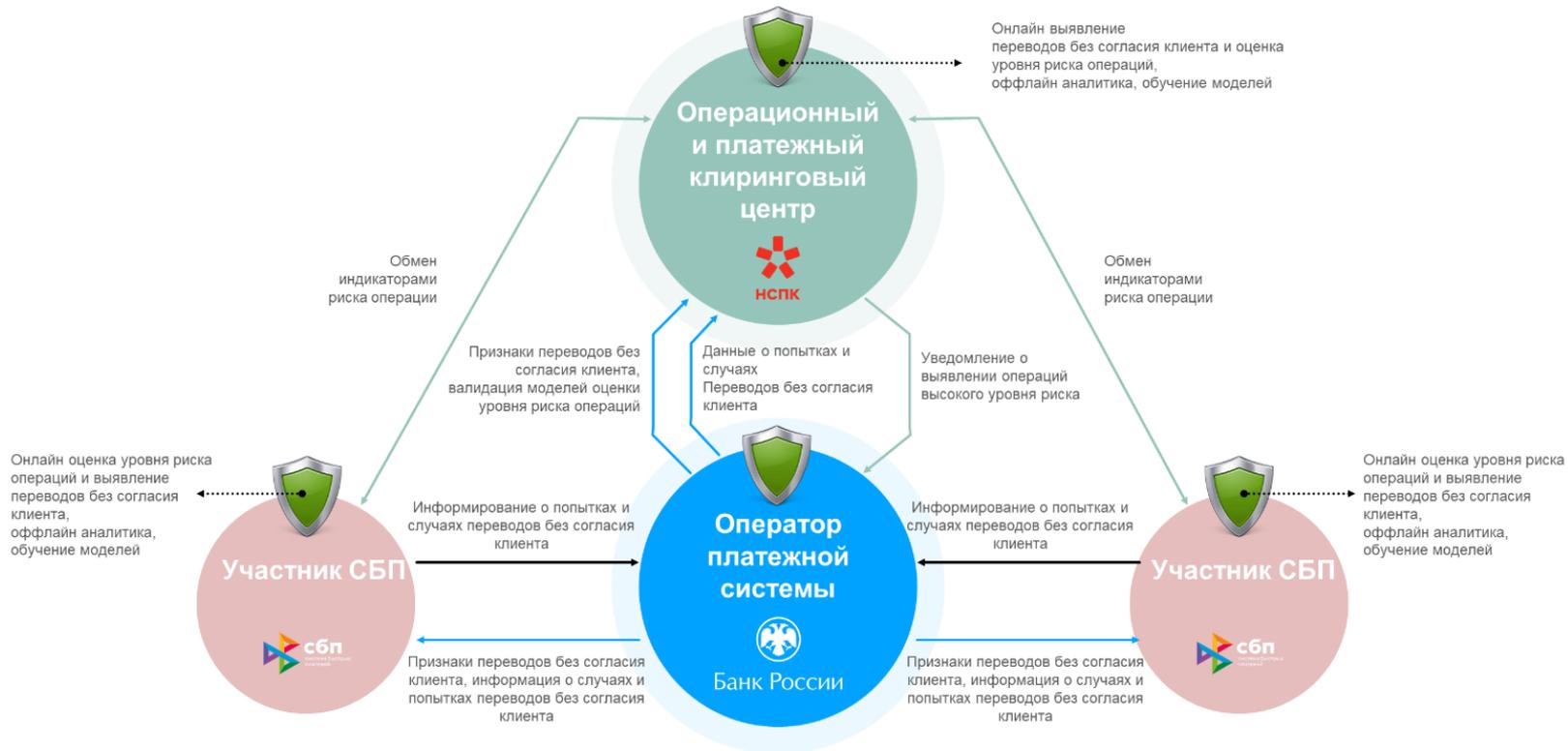
- риск перевода денежных средств без согласия клиента
- риск раскрытия сведений, в том числе персональных данных, а также сведений, составляющих банковскую тайну

На стороне участников СБП:

- риск уменьшения суммы денежных средств, используемых Участником СБП для осуществления переводов денежных средств с использованием СБП, вследствие осуществления множественных (массовых) переводов денежных средств без согласия клиента от имени одного либо нескольких Клиентов Участника СБП
- риск раскрытия сведений о клиентах Участника СБП, в том числе их персональных данных, а также сведений, составляющих банковскую тайну
- репутационные риски

Решение НСПК

Схема процессов



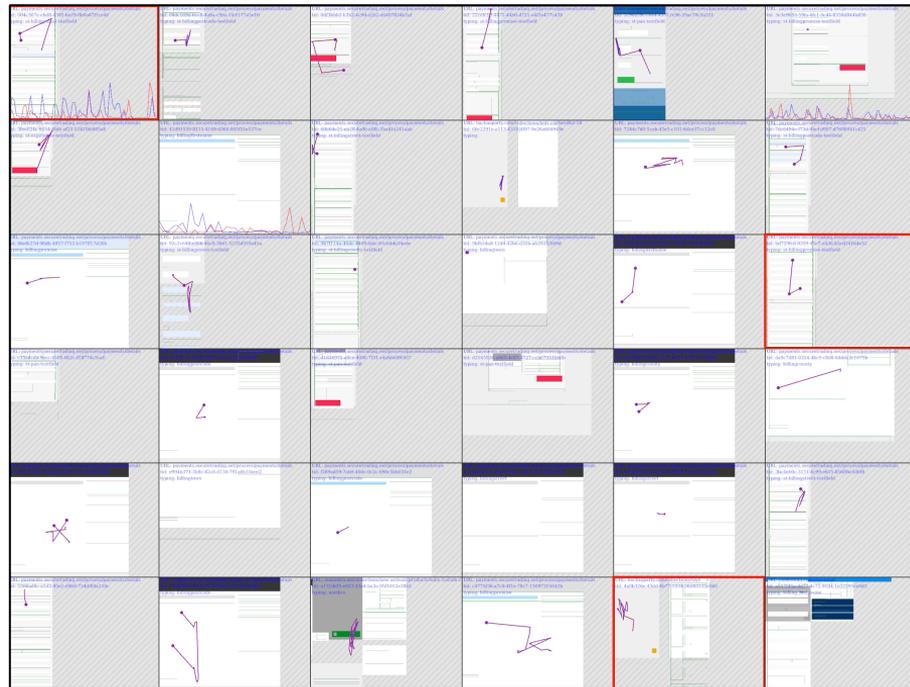
Анализ рисков

Сессия

- Поведенческая аналитика
- Цифровой профиль клиента
- Движение мыши, эллипс касания
- Паттерны клавиатуры, набора, нажатий

Локация

- IP
- Threat Intelligence
- geo (скорость перемещения)



Анализ рисков

Внесение изменений

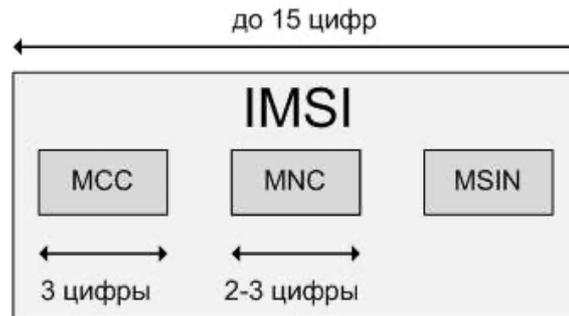
- IMSI/ICCID сим-карты
- IMEI устройства
- СМС/email информирование

Проблемы:

- Требуем интеграций с данными Телекома
- Интеграция с авторизацией
- Проблемы сбора данных – необходимы разрешения (не все версии android/ios поддерживают)

Решение:

- Комбинация с поведенческой аналитикой



- MCC (Mobile Country Code) – мобильный код страны (3 цифры)
- MNC (Mobile Network Code) – код сети сотовой связи, определяемый для каждого оператора в пределах страны (2-3 цифры)
- MSIN (Mobile Station Identification Number) – идентификационный номер абонента (он уникален в пределах одной страны и одного оператора)

Анализ рисков

Робот

- Боты
- Автоматизация

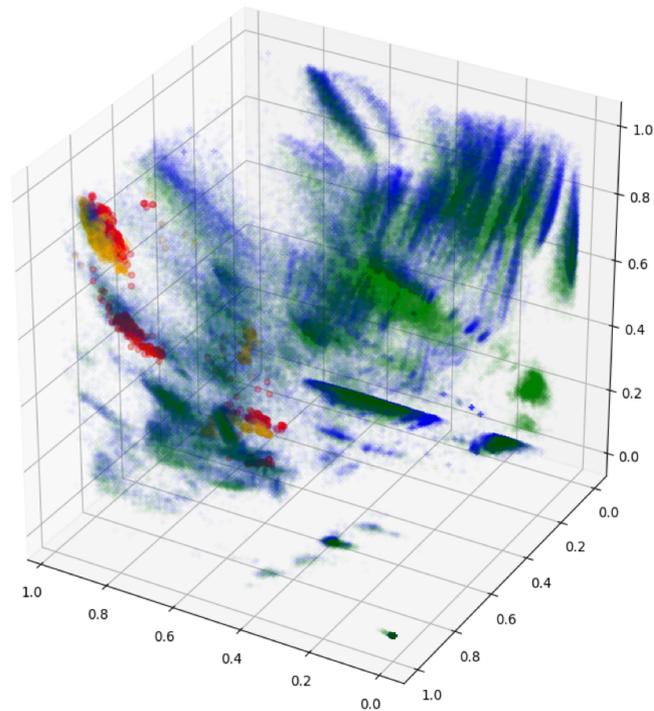
Аномальная транзакция

Аномальное поведение

Машинное обучение

Проблемы:

- Разметка
- Ресурсы



Кластеризация транзакций для выделения подозрительных групп

Что делать?

- Торопиться
- Реализовывать

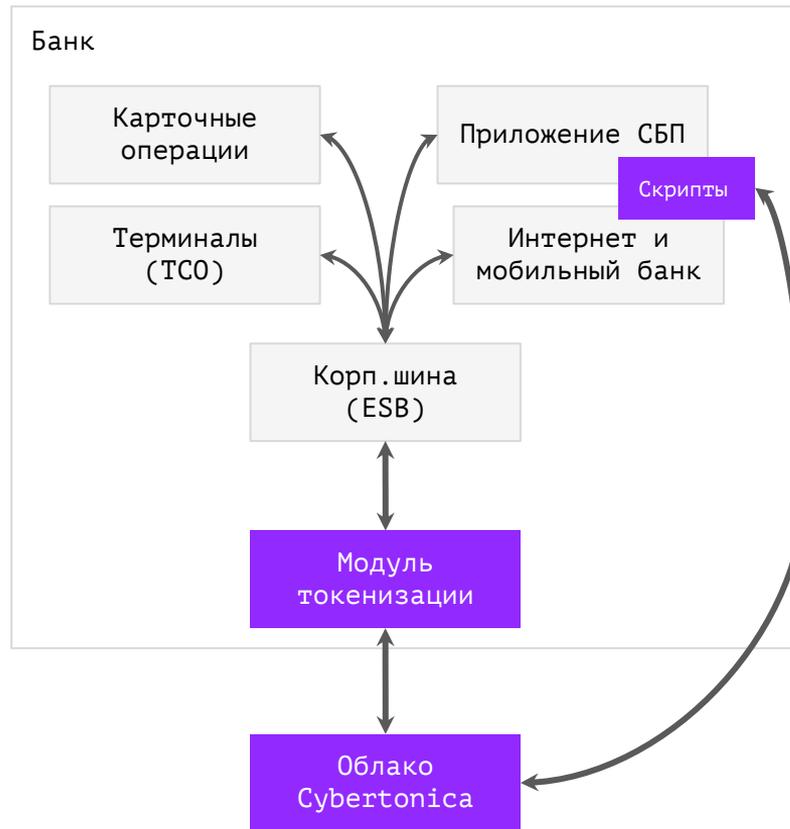
1) Собственная разработка

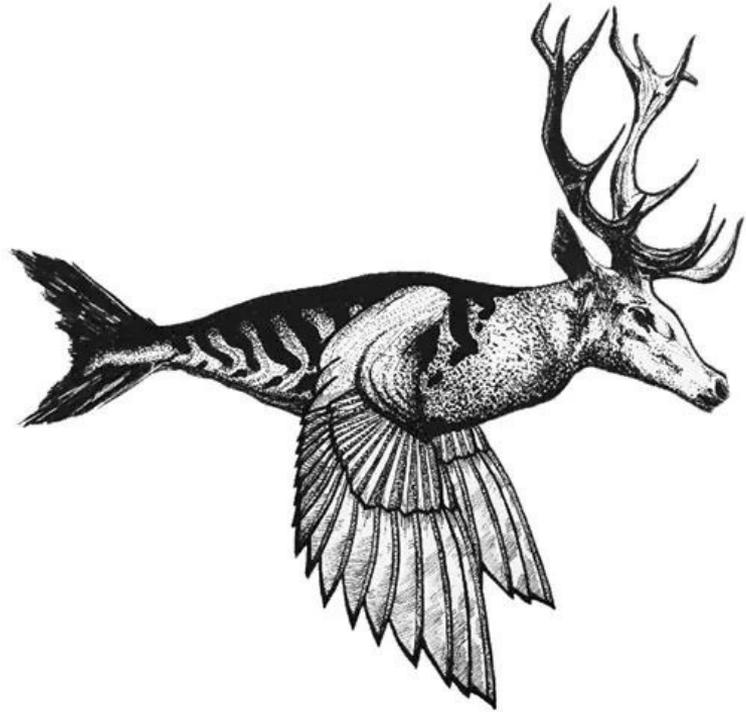
2) Внешнее решение

А) On-premise

Б) Сервис

С) Гибрид







Спасибо за внимание!
eshadrin@cybertonica.com



Евгений Шадрин
 Операционный директор



Сергей Вельц
 Технический директор и
 основатель



Олег Кузнецов
 Руководитель отдела по
 работе с заказчиками и
 партнерами

