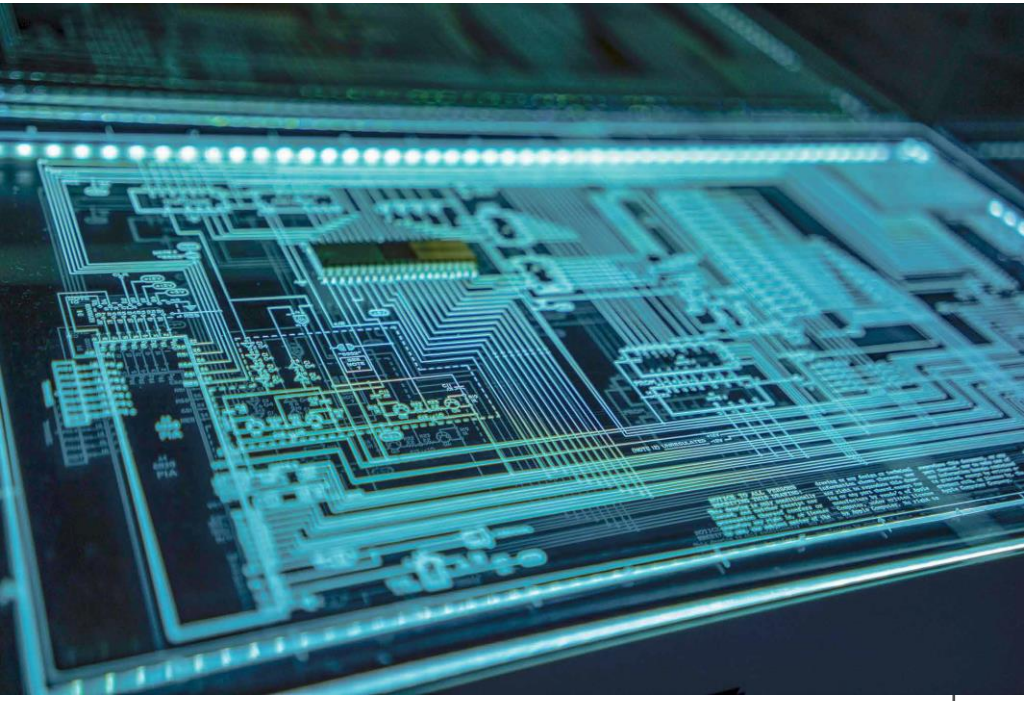
Smart Fraud Detection

Обнаружение и предотвращение мошеннических транзакций в каналах обслуживания клиентов

FUZZY LOGIC LABS

О компании



Компания «Фаззи Лоджик Лабс» уже несколько лет ведет разработку системы противодействия мошенничеству в реальном времени, основанной на:

- алгоритмах машинного обучения

(системы нечеткого вывода, вероятностные графические модели и другие);

- анализе данных и построении закономерностей

Smart Fraud Detection: назначение системы

Повышение устойчивости каналов обслуживания клиентов к хищению денежных средств

Задача №1:

- Сокращение убытков, связанных с мошенническими действиями от имени Клиентов;
  - Результат: Сокращение убытков

Задача №2:

- Сохранение репутации и снижение имиджевых рисков, укрепление позитивного восприятия каналов;
  - Результат: Сохранение и увеличение клиентской базы и объема операций

Задача №3:

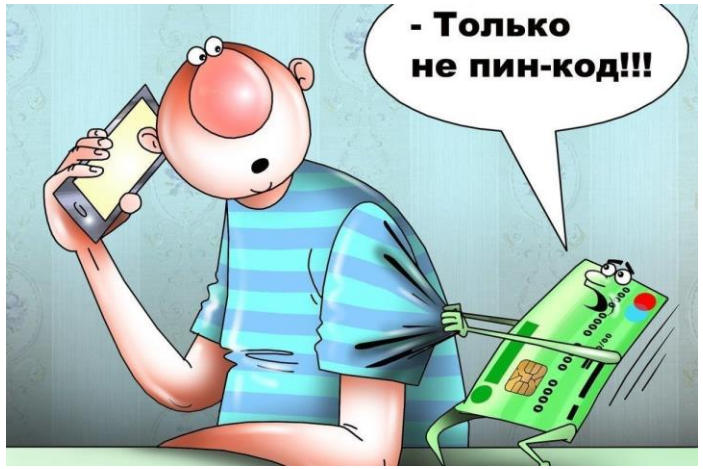
- Снижение расходов по предотвращению и расследованию мошеннических действий, за счет Эффективного выявления мошеннических платежей
  - Результат: Сокращение расходов

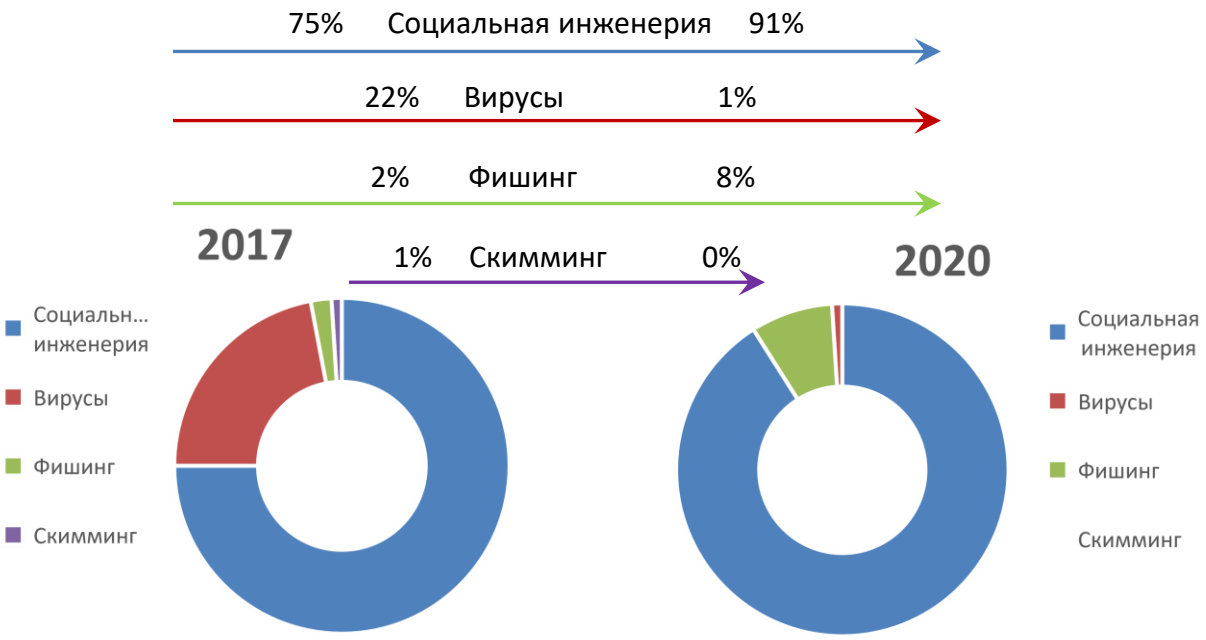
Задача №4:

- Выполнение требований регуляторов: противодействие переводов без согласия клиентов, расчет рисков;
  - Результат: Выполнение требований регуляторов

Тренды внешнего мошенничества

В цифровую эпоху происходит эволюция и совершенствование технологий как мошеннических инструментов, так и защитных систем, которые дают возможность их блокировать.





Структура социальной инженерии 2020

87%	Самопереводы
7%	Кража личности
6%	Обман на торговых площадках

Назначение системы

Smart Fraud Detection - комплексная система обнаружения мошенничества в реальном времени методом анализа поступающих транзакций в различных каналах обслуживания клиентов:

- Интернет-Банк, Банк-Клиент
- Мобильные приложения
- Эмиссия
- Эквайринг, Интернет-Эквайринг
- Платежные терминалы
- Операции в офисах, Кредитование
- Контактный центр \ IVR
- ‘Умные’ устройства, мессенджеры \ chatbot

<u>по направлениям:</u>

- Внутреннее мошенничество
- Внешнее мошенничество
- Комплаенс мониторинг.

Клиенты

СБЕР

ВТБ

ПСБ

ГАЗПРОМБАНК

ВОЗРОЖДЕНИЕ БАНК

АТБ Азиатско-Тихоокеанский Банк

сетелем

sravni.ru

РоссельхозБанк

KAZAKSTAN HALYK BANK
HALYK BANK
НАРОДНЫЙ БАНК КАЗАХСТАНА

Smart Fraud Detection
Соответствие требованиям потребителя

1. Хорошая интеграция с IT-системами банка +
2. Многоканальность +
3. Производительность +
4. Технологии проверки платежей («rule-based» + «model-based») +
5. Доступная цена, базовая комплектация, сервис +
6. Компетенции +
7. База знаний +

Фрод мониторинг 50% всех банковских транзакций в России

Схема обработки транзакций

Мобильные приложения

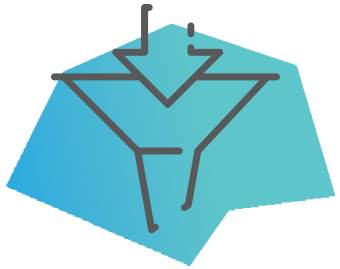
Интернет Банк

Контактный центр, Офис

Эмиссия, Эквайринг…

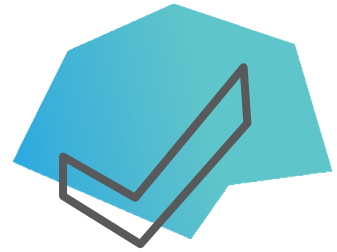
ПРИЛОЖЕНИЯ

Обработка транзакции

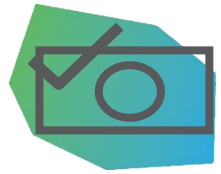


Оценка риска

Наборы правил

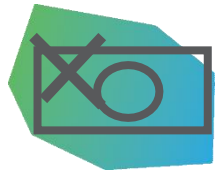


ПРОВЕРЕНО



Выполнить транзакцию

Приостановить транзакцию



Отклонить транзакцию

Управляющие воздействия:

1. Блокировки (карт,
2. аккаунтов)
3. Информирование SMS, E-Mail
4. Расследование инцидентов

SMART FRAUD DETECTION

FUZZY LOGIC LABS

Фронт-офис: сбор информации (мобильные приложения, интернет банк)

ИДЕНТИФИКАЦИЯ УСТРОЙСТВА, МОБИЛЬНОЕ ПРИЛОЖЕНИЕ

- Определение параметров устройства: модель устройства, версия системы, имя устройства, язык, wifiMac адрес, размер и разрешение экрана и т.п.
- Параметры: IMSI или MSISDN, номер телефона, IMEI для GSM \ MEID или ESN для CDMA, …
- Удаленное управление (TeamViewer …), Наличие активного звонка

СВЕДЕНИЯ ОБ УСТРОЙСТВЕ, ИНТЕРНЕТ БАНК

- Сведения заголовка HTTP
- IP адрес
- Профиль устройства («отпечаток устройства»)

Информация мобильного приложения (SDK)

ИДЕНТИФИКАЦИЯ УСТРОЙСТВА

- IMEI \ Device Vendor ID, IMSI, ID ОС, AppKey
- Модель устройства, MNC, MCC, версия ОС
- Wi-Fi MAC адрес, имя Wi-Fi сети
- Часовой пояс
- ID вышки
- Координаты ‘Широта, Долгота’
- IP адрес, геопозиция

СОСТОЯНИЕ УСТРОЙСТВА

- Проверка устройства на эмуляцию
- Проверка устройства на root \ jailbreak
- Наличие удаленного управления (RDP)
- Наличие активного звонка \ Направление звонка

	Название параметра	Описание
1	DeviceName	Имя устройства заданное пользователем.
2	HardwareID	IMEI
3	SIM_ID	IMSI
4	DeviceModel	Модель устройства.
5	WiFiNetworksData: BSSID	MAC адрес точки доступа.
6	WiFiNetworksData: SSID	Имя Wi-Fi сети.
7	WiFiNetworksData: SignalStrength	Уровень сила сигнала Wi- Fi роутера.
8	WiFiNetworksData: Channel	Канал Wi-Fi роутера
9	GeoLocationInfo: Latitude	Широта
10	GeoLocationInfo: Longitude	Долгота
11	GeoLocationInfo: Altitude	Высота над уровнем моря.
12	GeoLocationInfo: HorizontalAccuracy	Точность долготы и широты.
13	GeoLocationInfo: AltitudeAccuracy	Точность высоты над уровнем моря.
14	GeoLocationInfo: Timestamp	Время получения геоданных.
15	GeoLocationInfo: Status	Статус данных по геолокации (success=0, deny=1, notAvailable=2).
16	MNC	Mobile country code
17	MCC	Mobile carrier code
18	WiFiMacAddress	Wi-Fi MAC адрес мобильного устройства.
19	CellTowerId	ID обслуживающей вышки.
20	LocationAreaCode	Код зоны расположения.
21	DeviceSystemVersion	Версия ОС.
22	MultitaskingSupported	Проверка на мультизадачн ость.
23	TIMESTAMP	Время получения данных.
24	DeviceSystemName	Название ОС.
25	ScreenSize	Размер экрана.
26	Languages	Язык устройства.
27	SDK_VERSION	Версия SDK.
28	OS_ID	Android_ID
29	AppKey	Ключ приложения. Генерируется новый при переустановке приложения.
30	TimeZone	Часовой пояс.
31	Emulator	Проверяет устройство на эмуляцию.
32	MultitaskingSupported	Проверка на мультизадачность.
33	Compromised	Проверять устройство на root.
34	RdpConnection	Определение, что устройство находится под управлением RDP (Remote Desktop Protocol)
35	Displays	Информация о экранах телефона, включая виртуальные
36	HoursSinceZoomInstall	Показывает сколько часов прошло с момента установки приложения Zoom. Вернет -1 если Zoom не установлен на устройстве
37	HoursSinceAnyDeskInstall	Показывает сколько часов прошло с момента установки приложения AnyDesc. Вернет -1 если AnyDesc не установлен на устройстве
38	HoursSinceQSInstall	Показывает сколько часов прошло с момента установки приложения QuickSupport. Вернет -1 если QuickSupport не установлен на устройстве
39	InstallationSource	Возвращает строку с названием магазина из которого приложение было установленно. Возможные значения: Название магазина; Пустое значение, если установить источник невозможно; или источник АДБ
40	GooglePlayProtect	Показывает активирован ли на устройстве сервис Google Play Protect. 1 - Сервис активен. 0 - Не активен. -1 - поле не проинициализировалось (при первом запуске оно только запускает инициализацию и всегда будет -1)
41	UnknownSources	Показывает включена ли настройках «Установка из неизвестных источников” на устройстве. 1 - включены 0 - выключены. -1 - поле не поддерживается (для Android 8 и выше)
42	DeveloperTools	Показывает включены ли инструменты разработчика настройках устройства 1 - включены, 0 - выключены
43	PhoneCallState	Наличие активного звонка 1 - есть активный звонок, 0 - нет звонка

Адаптивная аутентификация пользователя по видео

АДАПТИВНАЯ АУТЕНТИФИКАЦИЯ – ОБЩИЙ ПРИНЦИП РАБОТЫ

- Используются нейросетевые вычисления на стороне клиента для снижения объема трафика и нагрузки на серверную инфраструктуру
- Распознавание лица:
  - поиск лица сотрудника в общей базе (если доступно): построение
    - «отпечатка» лица на стороне клиента, поиск на стороне сервера
  - реидентификация лица сотрудника: сопоставление с предыдущим аутентифицированным изображением
- Детектирование аномалий в позе и движениях:
  - детектирование позы и выражения лица на каждом изображении
  - ансамбль алгоритмов для выявления различных видов аномалий

Компонентный состав системы

Фронт-офис

Источники транзакций

JSON
TCP (ISO 8583)

Модуль обработки транзакций

Модуль оценки риска

Модуль правил

Бэк-офис

Базы данных

Бизнес приложения

Oracle
PostgreSQL

Управление правилами Справочники

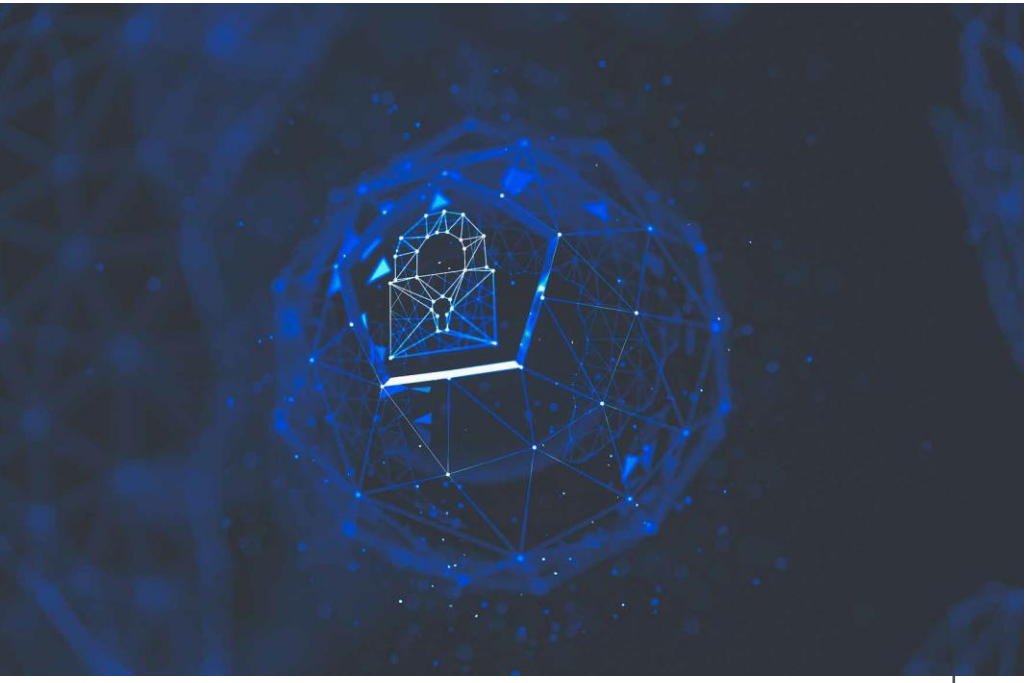
Управление доступом

Управление инцидентами

Отчет-ность

Планиров-щик

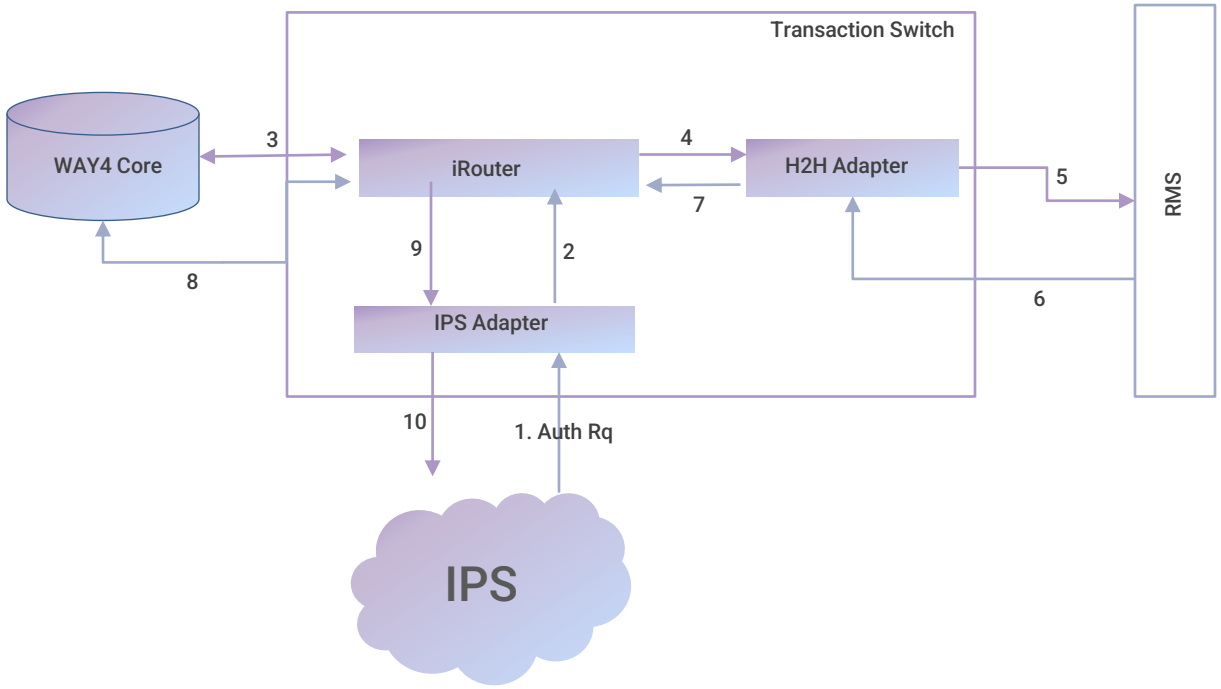
Фронт-офис: основные модули системы



Модуль обработки транзакций – выполняет следующие функции:

- Обработка \ преобразование входных данных: TCP (ISO 8583), HTTP/HTTPS (JSON)
- Обогащение транзакции справочными данными из внешних источников
- Формирование ответов с рекомендованным действием внешней системе в реальном времени

Пример онлайн взаимодействия с ПЦ по TCP (ISO 8583)



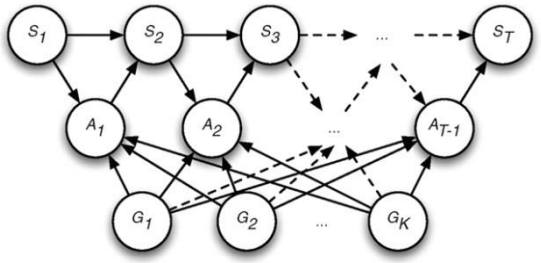
Базовый сценарий (транзакция принимается всеми участниками):
1 - Запрос от IPS
2 - Перевод во внутренний формат и отправка на iRouter (адаптер с подключением к WAY4Core)
3 – Проверка запроса в WAY4 Core
4 – Отправка на адаптер к RMS (если система не доступна, то шаг пропускается)
5 – Отправка в RMS (Request)
6 – Ответ от RMS (Response)
7 - Отправка Response Code, полученного от RMS на iRouter
8 – Сохранение ответа от RMS в WAY4
9, 10 – Отправка ответа в IPS

Эффективный мониторинг: комбинация «model-based» и «rule-based» подходов

Фронт-офис: основные модули системы

Модуль оценки рисков - динамическая самообучаемая модель оценки риска, аккумулирующая схемы поведения клиентов, обладающая следующими преимуществами:

- Модульная организация модели – дает возможность дополнять модель при изменении структуры данных
- Online оценка подозрительности события – система формирует балл оценки риска 0 до 1000
- Оперативная реакция на изменения схемы поведения клиента

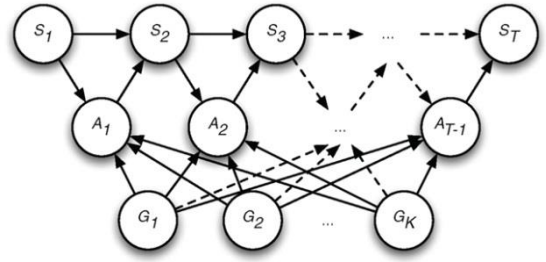


Модуль правил - модуль для построения собственной модели управления рисками:

- Расчет параметров in memory
- Набора правил и списков проверки транзакции

Фронт-офис: основные модули системы

- **Модуль оценки рисков** использует механизмы вероятностных моделей: байесовских сетей, набор из нескольких нейросетей и деревьев с градиентным бустингом



- Результаты анализа и входные данные используются для ежедневного обучения. Цель: адаптация к новым угрозам

- Оценка риска — аналитический механизм, что дает следующие :
  - быстродействие на порядки выше;
  - требования к аппаратным ресурсам существенно ниже;

	Positives	Negatives
Predicted Positives	True Positives	False Positives
Predicted Negatives	False Negatives	True Negatives

Фронт-офис: нормализованная оценка риска

Нижний диапазон	Верхний диапазон	Процент	Суммарный процент
900	1000	0.25%	0.25%
800	900	0.25%	0.50%
700	800	0.50%	1.00%
600	700	2.00%	3.00%
500	600	2.00%	5.00%
400	500	5.00%	10.00%
300	400	10.00%	20.00%
200	300	10.00%	30.00%
100	200	20.00%	50.00%
0	100	50.00%	100.00%

Фронт-офис: расчет параметров in memory по внутрисистемным объектам

Расчет параметров транзакции по истории:

Event Number –
количество транзакций за период

Transaction Amount –
сумма транзакций за период

Event Interval –
время с момента ближайшей транзакции

New Device Interval –
время с момента нового устройства

Условия / параметры фильтрации для функций расчета:

Event type –
с фильтрацией по типам событий

Amount –
с условиями по сумме

Currency –
с условиями по валюте

Card Number List –
с ограничением по списку карт получателей

IP list –
с ограничением по списку IP

Преобразование параметров транзакции, включая рассчитанные on-line:

Ratio –
отношение (деление) двух параметров

Sum –
сумма параметров

Multiple –
кратность параметров

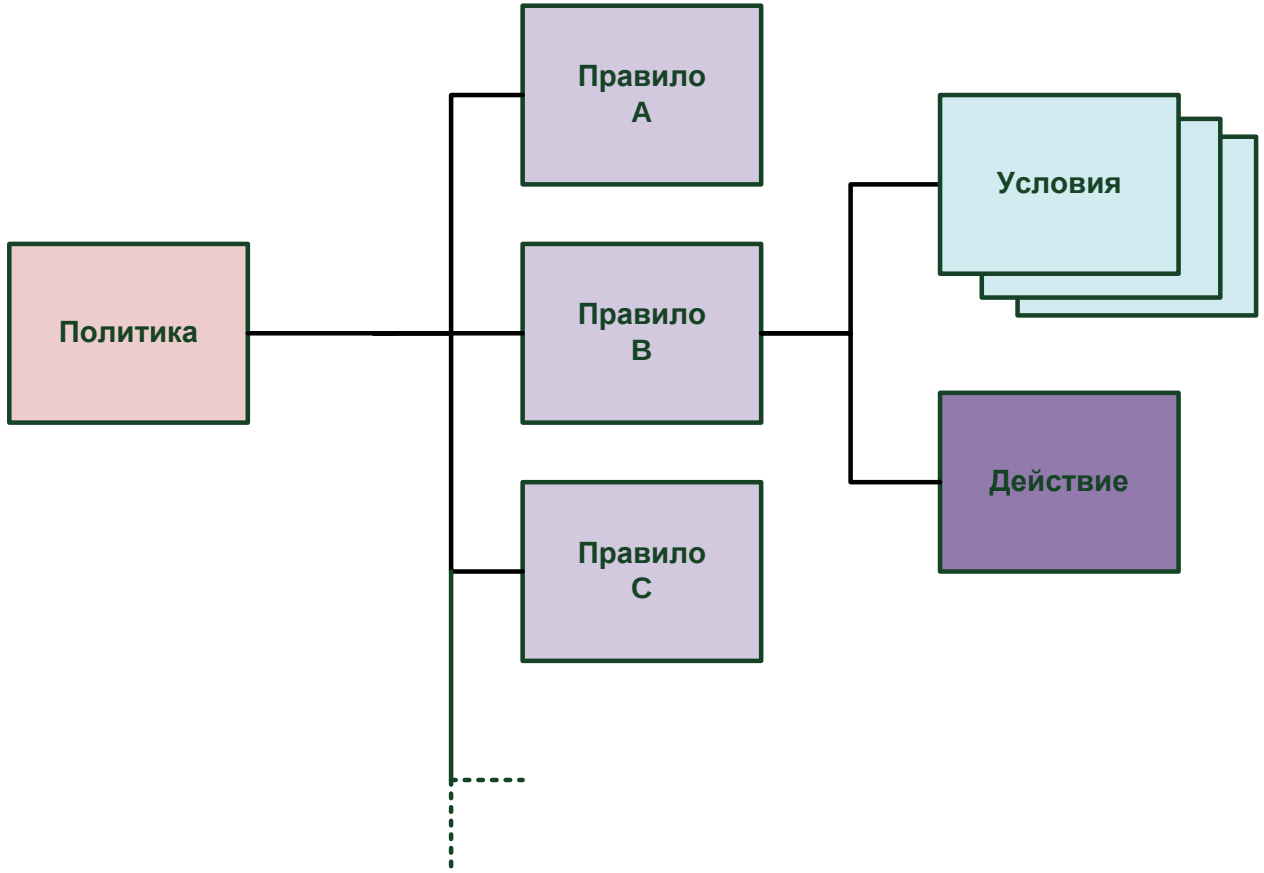
Substring –
получение подстроки (балансовый счет, БИН карты)

Фронт-офис: динамические объекты расчета

Динамические объекты расчета – собственные настраиваемые объекты хранения:

- Объект – ключ:
  - Простой ключ – один атрибут транзакции (клиент, получатель, терминал, филиал, телефон, сумма транзакции, тип карты, БИК получателя …)
  - Составной ключ – несколько ‘склеенных’ атрибутов транзакции («карта + терминал», «сумма + БИК», «город + получатель» …)
- Элементы объекта:
  - Виды элементов: элемент (first, last, sum, min, max, count, unique), массив (sum, min, max, count, unique)
  - Неограниченное количество элементов объекта, массив с заданной глубиной \ максимальным количеством записей
- Добавление \ обновление \ наполнение объектов выполняется в on-line ‘in memory’
- Расчет параметров транзакции по динамическим объектам ‘in memory’ (получить значения, математические действия, уникальны элементы …)

Фронт-офис: управление правилами



Работа с правилами:

- Статусы
  - Рабочее
  - Тестовое
  - Настройка

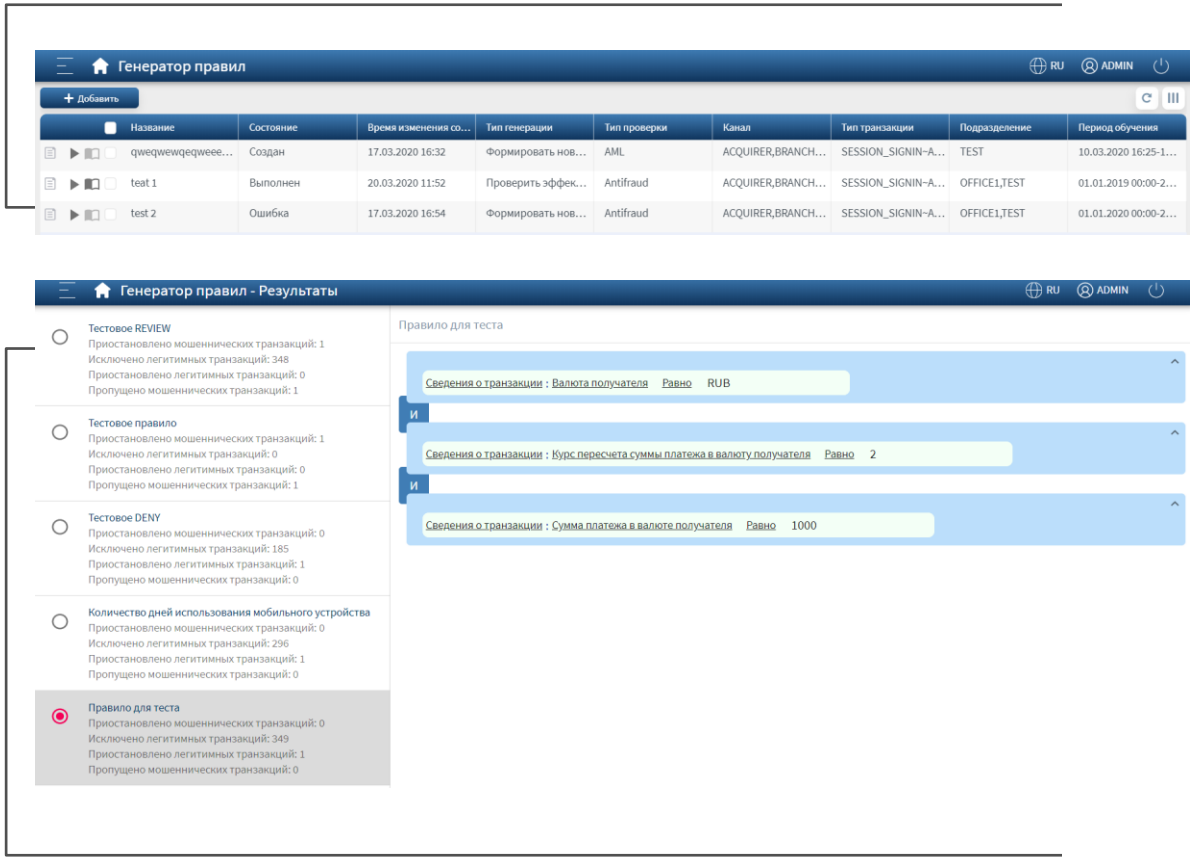
- Работа с правилами в режиме тестирования
- Хранение истории изменения состояния
- Бальная система подправил для формирования составного правила
- Генератор правил

Бэк-офис: генератор правил

Генератор правил формирует правила-гипотезы в формате конструктора правил на исторических данных

Генератор правил:

- формирует новый комплект правил
- оптимизирует правила-гипотезы экспертов
- проверяет эффективность правил по истории



Генератор правил основан на алгоритме эволюции грамматических структур, описанных в нормальной форме Бэкуса—Наура

Генератор правил:

масштабируем - распараллеливается

FUZZY LOGIC LABS

Бэк-офис: основные модули системы

Бизнес приложения:

Управление правилами – интерфейсное решение для определения конкретных действий в зависимости от параметров и риска (настройка правил, настройка списков)

- Рассчитываемые параметры на системных и собственных объектах
- Можно устанавливать любые правила обработки транзакций
- Большое количество готовых к использованию политик
- Работа с «черными» и «белыми» списками
- Генератор правил на исторических данных

Управление инцидентами – интерфейсное решение для расследования инцидентов и просмотра любых событий офицером безопасности

Отчетность - формирование оперативных отчетов , генератор отчетных форм, формирование отчетных форм по расписанию

Бэк-офис: основные модули системы

Модули администрирования:

Управление доступом - модуль для автоматизации рабочего места администратора системы (настройка рабочих мест пользователей, ролей и доступов)

Планировщик - планирование и администрирование задач с помощью единой консоли.

- Внутрисистемные процедуры;
- Коммуникации с внешними системами: управляющие воздействия, обновление списков и другое…

Поддерживаемые платформы

Операционные системы:

Unix системы (Debian, RHEL, CentOS, Solaris, AIX)

Сервера приложений:

Фронт-офис: java приложения, в целях быстродействия
Бэк-офис: java приложения

Базы данных:

Oracle
PostgreSQL

Производительность 1\2

Показатели проведенных испытаний:

- Количество транзакций в секунду – 5’000 tps
- Время ответа для 90% транзакций не превышает - 40 мс
- Максимальное время ответа не превышает – 100 мс
- Глубина хранения данных – 1 месяц (150 млн транзакций в день)

Сервера приложений Фронт-офис	
Количество ядер процессоров на все сервера приложений	128
Частота процессора	3Ghz+
Оперативная память на все сервера приложений	5 TB
Жесткий диск на все сервера приложений	10 TB

Производительность 2\2

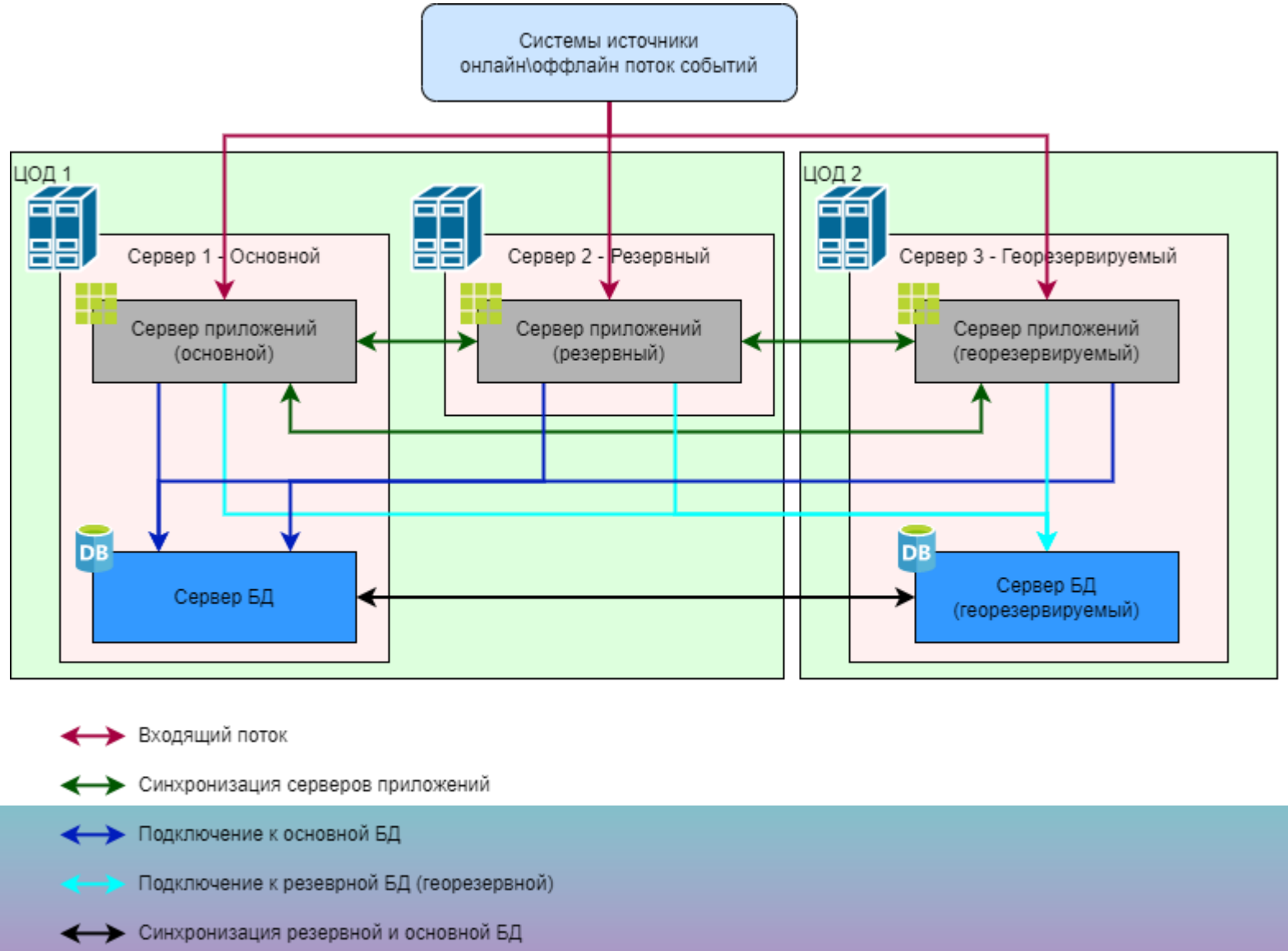
Параметры для расчета:

- Общее количество активных клиентов – до 1’000’000
- Пиковое количество транзакций в секунду – 100
- Общее количество транзакций в день – 500’000
- Время ответа на транзакцию – 200 мс
- Глубина хранения данных – 180 дней

Сервер приложений	
Количество ядер процессора	8 2Ghz+
Оперативная память	128 GB
Жесткий диск	500 GB

Сервер БД	
Количество ядер процессора	8 2Ghz+
Оперативная память	32 GB
СХД	4 TB

Пример. Отказоустойчивая \ катастрофоустойчивая конфигурация



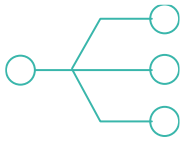
Smart Fraud Detection
Соответствие требованиям потребителя

1. Хорошая интеграция с IT-системами банка +
2. Многоканальность +
3. Производительность +
4. Технологии проверки платежей («rule-based» + «model-based») +
5. Доступная цена, базовая комплектация, сервис +
6. Компетенции +
7. База знаний +

Фрод мониторинг 50% всех банковских транзакций в России

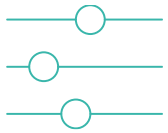
FUZZY LOGIC LABS

Преимущества системы



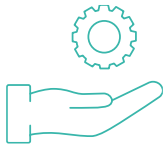
Самообучающийся модуль оценки риска

Кросс-канальный мониторинг транзакций клиентов (интернет банк, мобильный банк, эмиссия и т.п.)



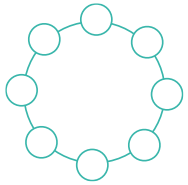
Быстрая адаптация к новым типам атак

Компоненты модели обновляются в процессе работы (квазирилтайм)



Минимизация «ручного» вмешательства

Четкое прогнозирование нагрузки на службу контроля финансовых операций в зависимости от принимаемого Банком уровня риска



Единая модель для разных категорий клиентов

Детерминированное время обработки каждой транзакции (не более 0.1 с)

FUZZY LOGIC LABS

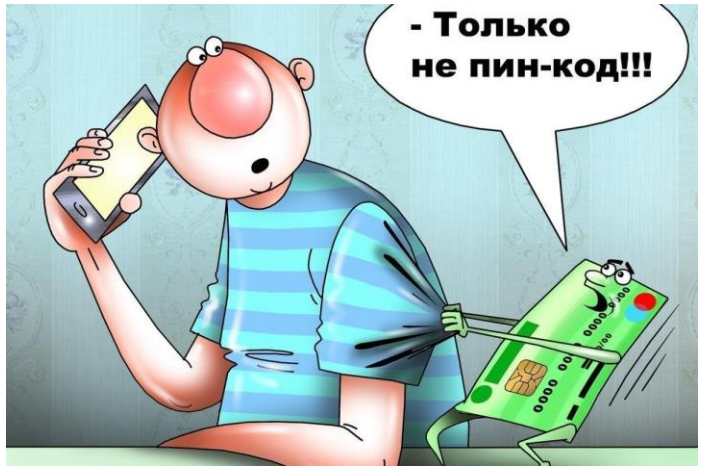
От чего защищать?

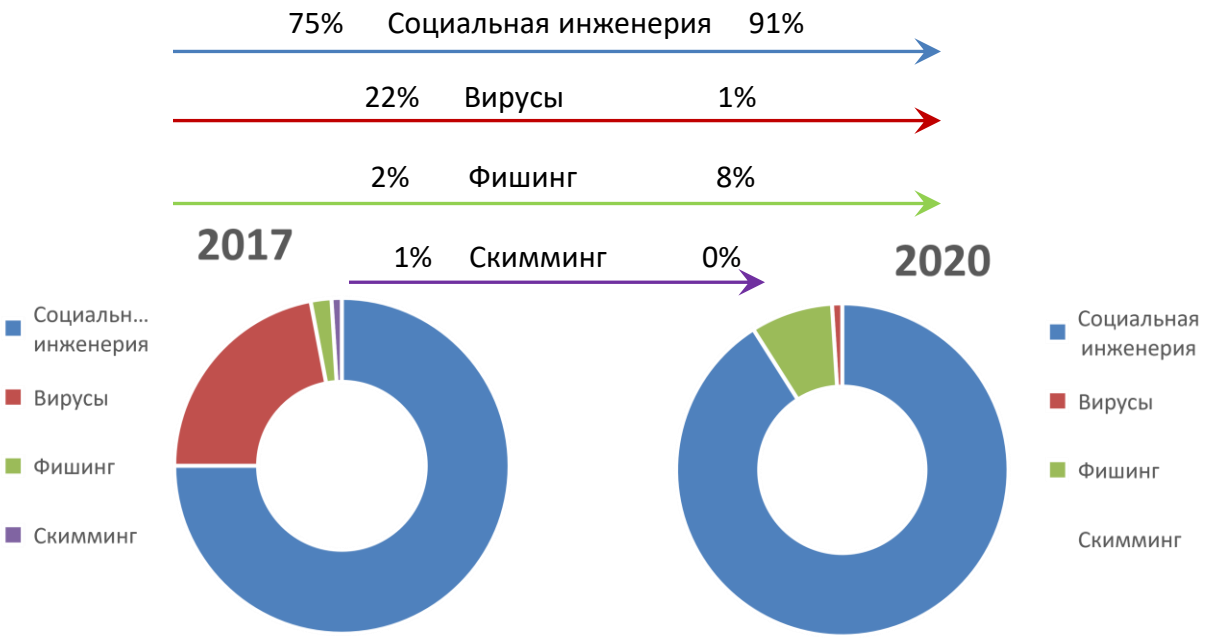
Типы мошенничества

Тип мошенничества	Тип риска
Внешнее мошенничество	Предоставление поддельных и мошеннически измененных электронных платежей
	Мошеннические операции с использованием банковских платежных карт Банка
	Несанкционированные действия со счетами и средствами внутри банковской сети информационных систем
Внутреннее мошенничество	Проведение мошеннических операций со средствами клиентов
	Присвоение денежных средств с чужих счетов

Тренды внешнего мошенничества

В цифровую эпоху происходит эволюция и совершенствование технологий как мошеннических инструментов, так и защитных систем, которые дают возможность их блокировать.





Структура социальной инженерии 2020

87%	Самопереводы
7%	Кража личности
6%	Обман на торговых площадках

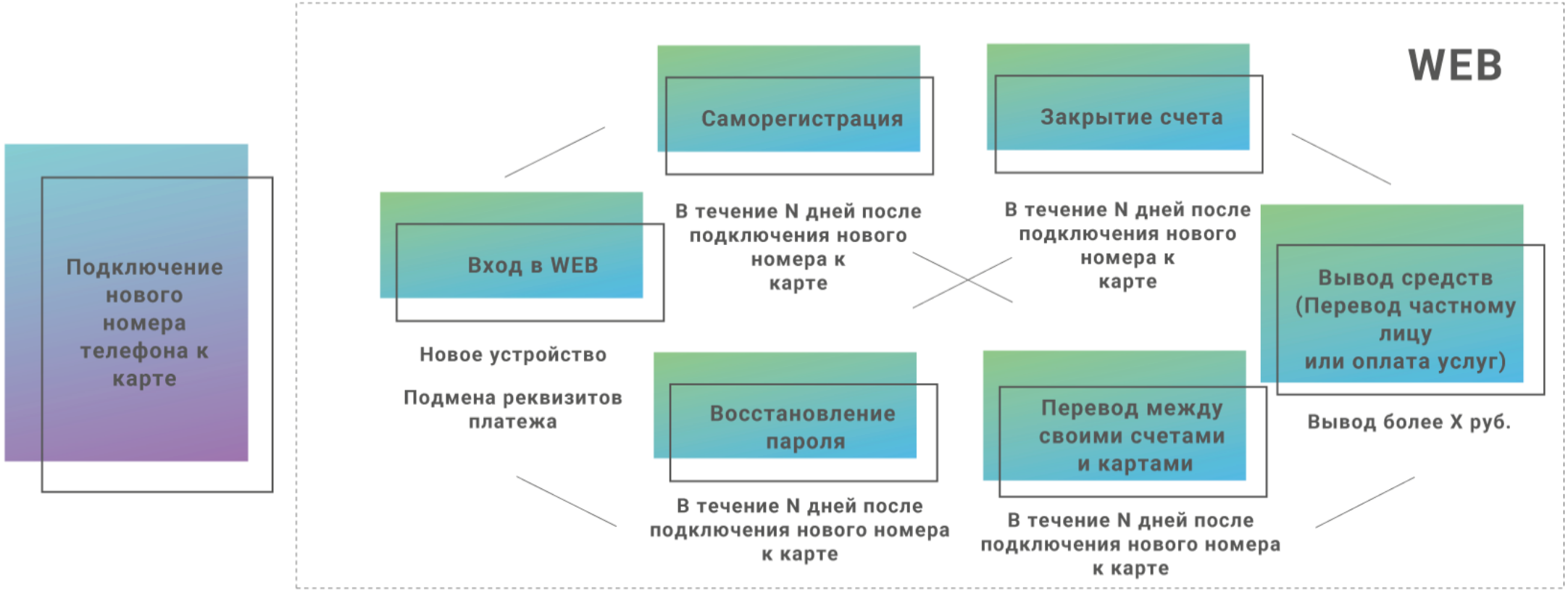
Интернет Банк и Мобильные приложения. Примеры атак

Нарушитель	Угроза	Метод атаки
Мошенник		
	Несанкционированные операции в ДБО с рабочих станций клиентов	
	Троян-заражение Клиента	Подмена реквизитов платежа
		Удаленное управление компьютером Клиента
		Автоматизированный процесс формирования и отправки незаконных платежей
	Кража учетных данных пользователей ДБО	
	Фишинг (поддельный сайт) + СПАМ («Социальная инженерия»)	Хищение учетных данных клиентов: логинов / паролей Перехват одноразовых паролей

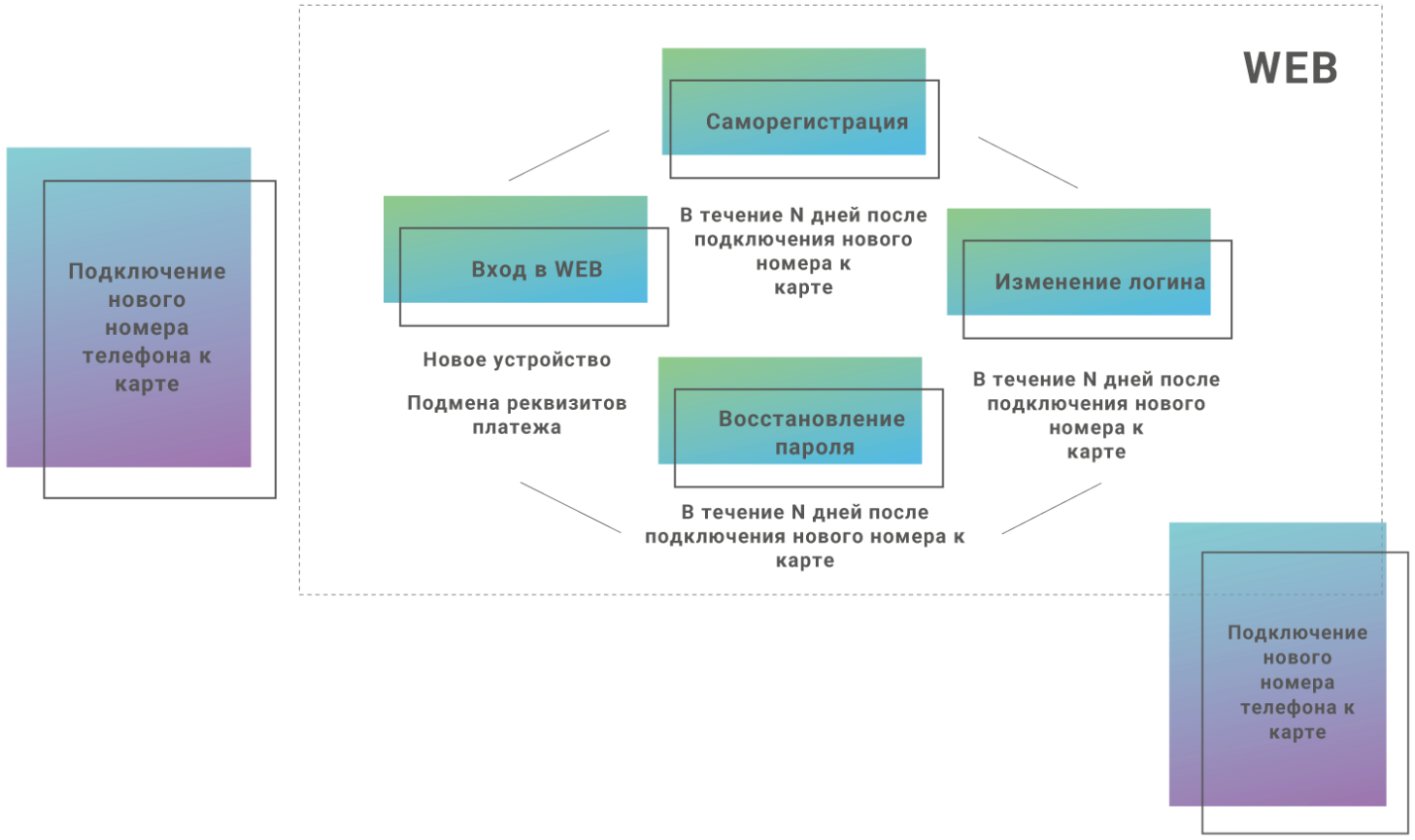
Интернет Банк и Мобильные приложения. Примеры атак

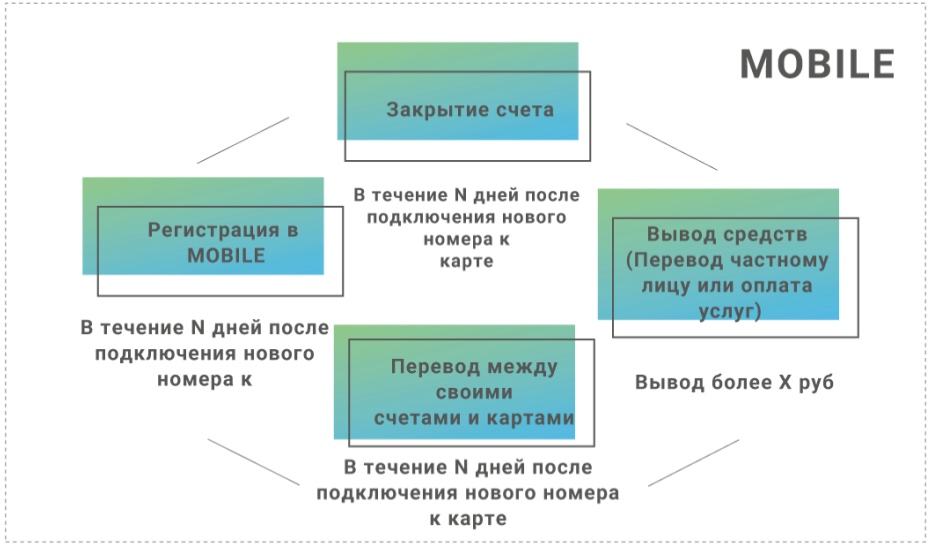
Нарушитель	Угроза	Метод атаки
Мошенник		
	Атака на инфраструктуру ДБО	
	Троян-заражение в инфраструктуре Банка	Хищение учетных данных клиентов: логинов / паролей …
		Распространение вредоносного кода - Заражение рабочих станций клиентов
		Формирование и отправка незаконного платежа
Недобросовестный Клиент	Злоупотребление полномочиями	Формирование и отправка незаконного платежа
Недобросовестный сотрудник Банка	Злоупотребление полномочиями	Формирование и отправка незаконного платежа

Социальная инженерия. Схема – пример 1



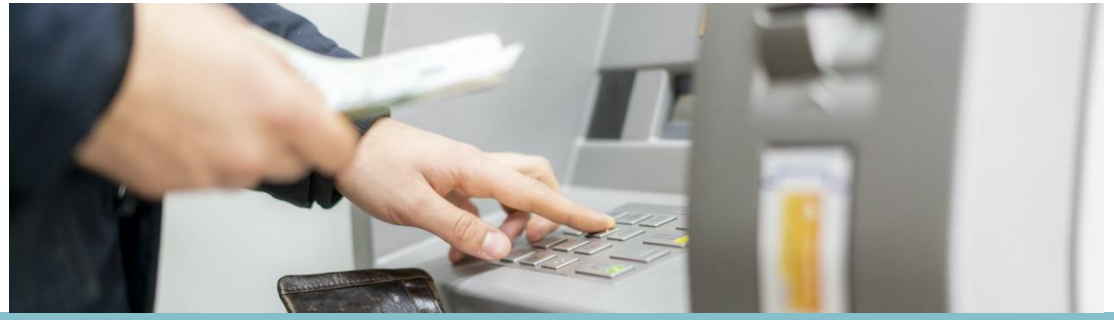
Социальная инженерия. Схема – пример 2





Операции по картам, примеры атак

- **Скимминг** (считывание данных), изготовление дубликатов
- **Скимминг** (считывание данных), выполнение платежей “Card Not Present” (покупки через Интернет)
- **Фишинг** (поддельный сайт) при покупках через Интернет
- **Мошенническая точка продаж**: с POS терминалом или виртуальная – Интернет магазин
- Кража подлинной карты, использование в мошеннических целях



Примеры атак с картами лояльности, Внутреннее и внешнее мошенничество

- Кража данных по карте с бонусами:
  - Доступ к личному кабинету с бонусами или регистрация личного кабинета на карту другого человека
  - Использование бонусов при оплате покупок
- Массовое начисление бонусов на ‘свои карты’
  - Начисление бонусов операторами на карту по операциям клиентов и покупка товара накопленными бонусами
- Покупка и возврат товара
  - Покупка товара с начислением бонусов, использование бонусов в сети магазинов и возвратом исходного товара
- Обналичивание баллов кассиром
  - Технические махинации на кассе при покупке товара (ложные зависания кассы и т.п.)
  - В результате выполняется полная оплата покупки и списание баллов по карте лояльности клиента, вырученная разница остается кассиру

Расширение протокола 3-D Secure версии 2.x

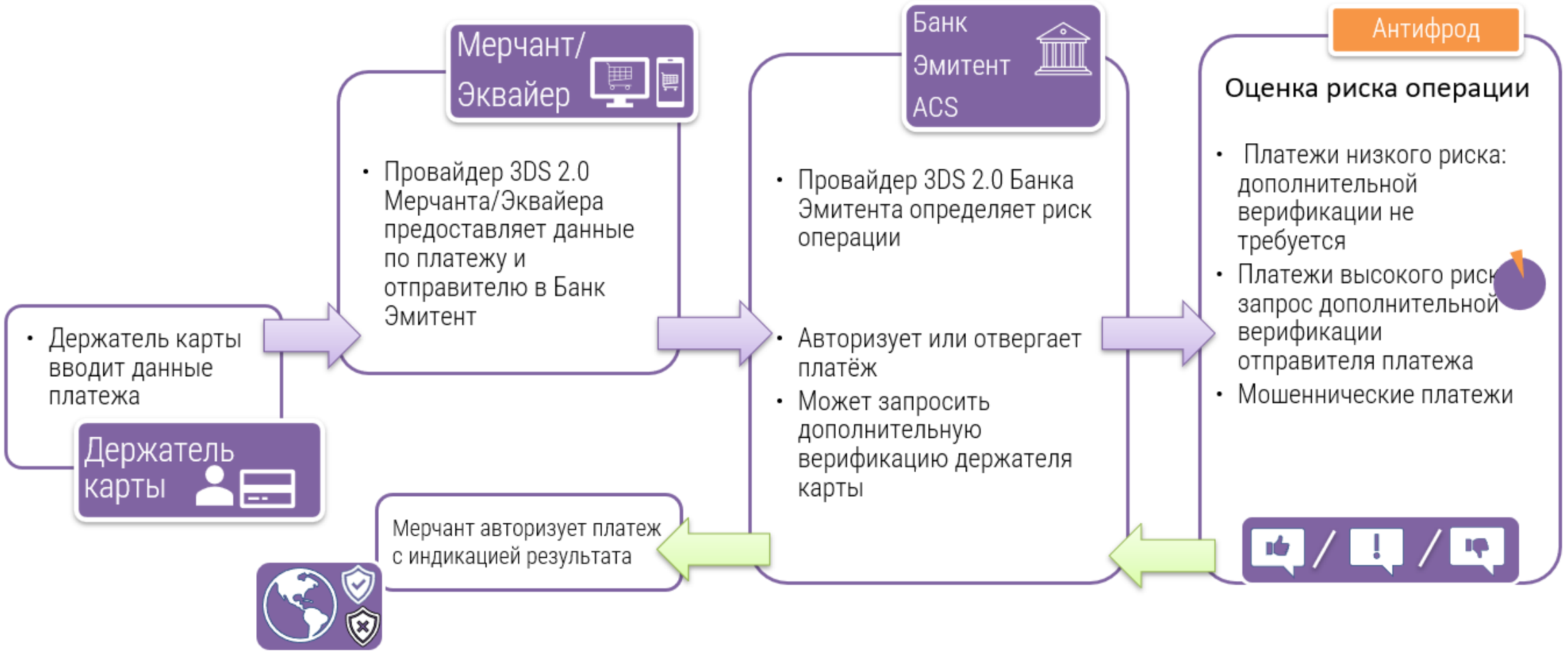
Повышение качество оценки легитимности транзакции и необходимости аутентификации

	3D Secure 1.0	3D Secure 2.0
Аутентификация	Статичный пароль	Динамические пароли и биометрия
Требуется верификация транзакций	100% транзакций	5% транзакций
Интерфейс	Браузер	Браузер и приложения
Параметры для анализа	15 элементов	Более 150
Область покрытия	Страна	Страна и мир

FUZZY LOGIC LABS

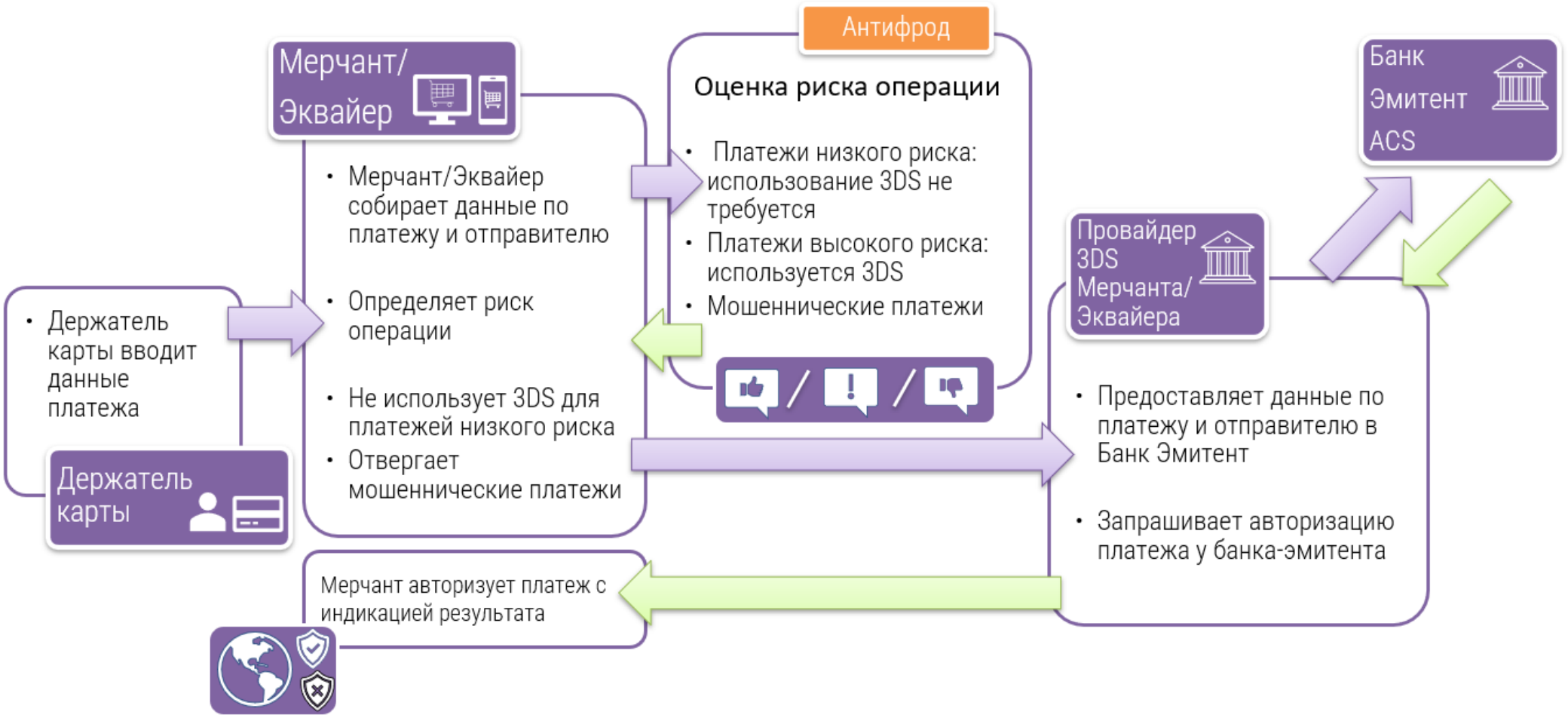
Верификация интернет-покупки

Принятие решения на стороне Банка Эмитента



Верификация интернет-покупки

Принятие решения на стороне Мерчанта / Эквайера



Общий принцип,
Карты лояльности и бонусные системы

- Для успешных противодействий мошенничеству необходимо оперативно получать информацию о действиях клиентов \ операторов в различных каналах, включая:

  - Начисления, покупки, возвраты\ отмены транзакций, акции
  - Информацию об устройствах и геопозиции выполнения операции
  - Информация по клиенту, оператору, офису \ точке продаж, партнеру

- В случае аномального поведения Оператора или Клиента выдавать уведомления и создавать инциденты, например:

  ✓ Аномальные действия с бонусами (зачисление и использование) клиентами, операторами, партнерами

  ✓ Несанкционированный вывод бонусов

  ✓ Хищение учетных данных клиентов для использования бонусов

  ✓ Возврат товара с ранее начисленными и использованными бонусами

ЦБ Признаки осуществелния операций без согласия Клиента

- Реквизиты платежа в базе дропперов
- Для операции используются скомпрометированные устройства (например, фиды от ФинЦЕРТ)
- Несовпадение характера и параметров операции типичным для клиента:
  - Время, Место, Устройство
  - Сумма, Частота, Получатель
- Платежи СБП, Индикаторы риска

НСПК, Операции СБП, Вариативность операций

Вид операции	Операции СБП	
C2C	■ Банк Плательщик: переводы ФЛ – ФЛ (списание)	■ Банк Получатель: переводы ФЛ – ФЛ (зачисление)
ME2ME	■ Банк Плательщик: списание (с подтверждением и без) ■ Банк Плательщик: согласие клиента на автоматическое списание	■ Банк Получатель: зачисление
C2B	■ Банк Плательщик: списание с ФЛ (с подтверждением и без) ■ Банк Плательщик: привязка к ТСП (согласие на автоматическое списание)	■ Банк Получатель: зачисление на ЮЛ
B2C	■ Банк Плательщик: списание с ЮЛ (возвраты,…)	■ Банк Получатель: зачисление на ФЛ

НСПК, Операции СБП, Индикаторы Подозрительной Операции

Вид операции

C2C

ME2ME

C2B

B2C

Индикаторы Подозрительной Операции

ИПО, Плательщик, C2C C2B

ЭБД {107}	
Поз.	**Описание**
1	Сессия
2	Локация
3	Устройство
4	Внесение изменений
5	Время работы
6	Робот
7	Аномальная транзакция
8	Аномальное поведение
9	Серый Получатель
10	Машинное обучение
11	Подтверждение Плательщика
12 — 16	Зарезервировано

ИПО, Получатель, C2C B2C

ЭБД {108}	
Поз.	**Описание**
1	Аномальная транзакция
2	Счет Получателя
3	Управление счетом
4	Белый Получатель
5	Машинное обучение
6 — 16	Зарезервировано

ИПО, Агент ТСП, C2B

Параметр «fraudscore» – Индикатор Подозрительной Операции Агента ТСП (ИПО АТ)	
Поз.	**Описание**
1	Аномальная транзакция (C2B)
2	Аномальное поведение (C2B)
3	Продолжительность работы
4	Деятельность
5	Оценка операции на предмет признаков 115-ФЗ

ИПО, Плательщик, B2C

ЭБД {107}	
Поз.	**Описание**
1	Наличие прямой операции
2	Аномальная транзакция (B2C)
3	Аномальное поведение (B2C)
4	Продолжительность работы
5	Деятельность
6	Оценка операции на предмет признаков 115-ФЗ

ЦБ Признаки осуществелния операций без согласия Клиента

- Реквизиты платежа в базе дропперов
- Для операции используются скомпрометированные устройства (например, фиды от ФинЦЕРТ)
- Несовпадение характера и параметров операции типичным для клиента:
  - Время, Место, Устройство
  - Сумма, Частота, Получатель
- Платежи СБП, Индикаторы риска

Бизнес-кейсы внутреннего мошенничества

- Мониторингу и анализу подвергаются:
  - Финансовые операции
  - Просмотр персональных и финансовых данных клиента
  - Изменение персональных и финансовых данных клиента
  - Модель поведения сотрудника Банка в системах автоматизации банковской деятельности, например:

•Работа с нетипичными клиентами (например, VIP)
•Выполнение нетипичных действий и операций,
•Массовый просмотр данных без выполнения транзакции
•Увеличение продаж
•Попытка подбора параметров для одобрения кредитов
•Работа в нетипичное время

Адаптивная аутентификация пользователя по видео

Тип атаки	Вид решения
Первое противоправное действие сотрудника	Динамика эмоций, динамика взгляда
Работа с неадекватным / подставным клиентом	Постоянная аутентификация лица клиента, динамика эмоций
Работа с физически отсутствующим клиентом	Постоянная аутентификация лица клиента
Фотографирование экрана	Детектирование телефона/фотоаппарата, динамика позы
Переписывание с экрана	Динамика взгляда, динамика позы
Подмена клиента	Постоянная аутентификация лица клиента, наличие прочих лиц
Чтение вслух с экрана	Динамика эмоций
Принуждение третьими лицами	Динамика эмоций, наличие прочих лиц, динамика взгляда
Доступ к незаблокированному устройству	Наличие прочих лиц, постоянна аутентификация лица сотрудника
Использование нелегитимных документов	Динамика позы, динамика эмоций
Поиск по экрану при таргетированном пробиве	Динамика взгляда

Внутреннее мошенничество. Фронт. Защита от атак

Примеры атак кражи средств и данных

- Сотрудник в провинции списывает небольшие суммы у слабодееспособных клиентов
- Сотрудник списывает средства со спящих счетов, получатель платежа \ отправитель платежа – спящий клиент
- Сотрудник выводи средства клинета дробя на непрерывную последовательность одинаковых платежей
- Сотрудник изменяет информацию о клиентах с целью кражи аккаунта
- Сотрудник переводит средства клиентов на один счет, возможно связанный с сотрудником
- Получатель мошеннических платежей обслуживался только у одного сотрудника
- Сотрудник выполняет сразу несколько мошеннических операций от имени клиента

- При совершении мошеннических действий сотрудник открывает две и более сессии с клиентом в день
- Клиентский сотрудник выполняет операции во время, когда клиентов нет
- Пострадавший клиент обслуживался только у одного сотрудника
- Сотрудник списывает маленькие суммы со счетов клиентов
- Сотрудник списывает суммы со счетов умерших клиентов
- Личная информация клиента была изменена незадолго до платежей
- Сотрудник закрывает вклад клиента сразу после открытия \ незадолго до закрытия
- На один спящий счет приходят много почти одновременных переводов

Внутреннее мошенничество. Фронт. Защита от атак

Примеры атак кражи средств и данных

- Сотрудник банка совершает перевод бонусов на свою карту
- Сотрудник оформляет кредитный продукт в отсутствии клиента только по скану его паспорта
- Сотрудник вводит неправильные данные клиента для улучшения условий кредита
- Работники одной компании (возможно зарплатные клиенты) офомляют кредиты на себя и потом передают их руководителю
- Вирус на личном компьютере сотрудника совершает действия от его имени
- Сотрудник (возможно в сговоре с сообщниками) кликает на опасную ссылку в почте, инфицирует виртуальное рабочее место

- Сотрудник входит в систему, но ничего не делает
- Сотрудник выполняет заведомо подозрительные поиски клиентов
- Сотрудник изменяет график погашения задолженности юзера
- Сотрудник откатывает операции без ведома клиента
- Сотрудники банка используют поддельные/краденные паспорта от имени клиентов
- Банковский пробив - сотрудник таргетированно или массово ищет иформацию по клиентам за вознаграждение
- Третьи лица принуждают сотрудника к операции
- Сотрудник впервые совершает кражу
- Сотрудник подумывает о краже данных клиентов, исследует варианты

Внутреннее мошенничество. Бэк. Защита от атак

Примеры атак кражи средств и данных по операциям бэкофисных систем

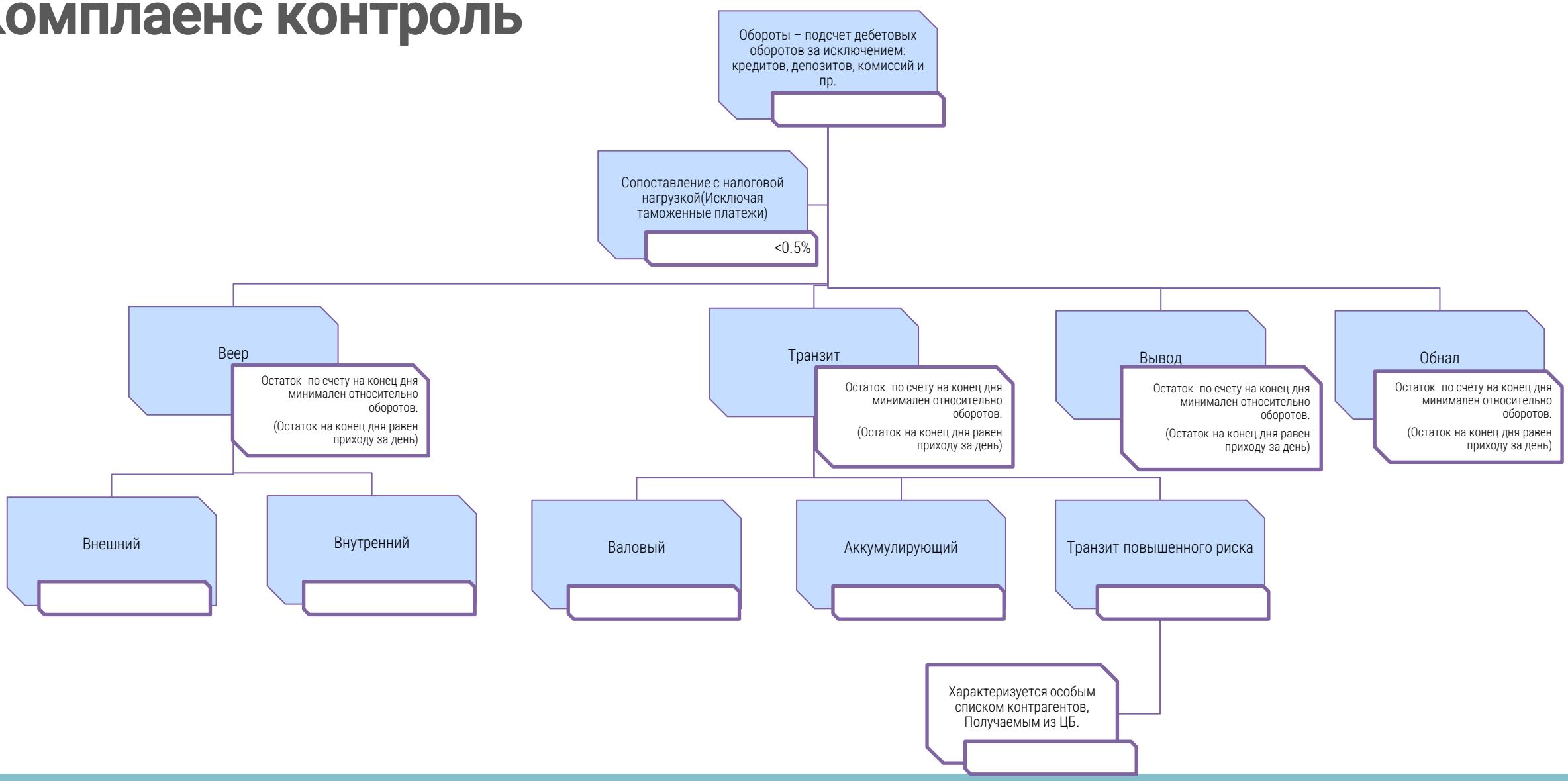
- Вирус на личном компьютере сотрудника совершает действия от его имени
- Сотрудник (возможно в сговоре с сообщниками) кликает на опасную ссылку в почте, инфицирует виртуальное рабочее место
- Сотрудник входит в систему, но ничего не делает
- Сотрудник выполняет заведомо подозрительные поиски клиентов
- Банковский пробив - сотрудник таргетированно или массово ищет иформацию по клиентам за вознаграждение
- Сотрудник подумывает о краже данных клиентов, исследует варианты или крадет данные о других сотрудниках
- Сотрудник крадет суммы на страхование (insurance premiums)
- Сотрудник крадет конфеденциальную информацию, не относящуюся непосредственно к клиентам
- Сотрудник крадет данные о физическом перемещении ценностей (инкассаторов и т.п.)
- Сотрудник крадет кэш из банкомата или кассы, имущество из банковских ячеек, прочее имущество банка
- Отмыв/уход от налогов с использованием ресурсов банка

- Сотрудник массово крадет PAN/PIN
- Сотрудник отключает/нарушает работу внутреннюю систему кибербезопасности или физической безопасности
- Манипуляция с банковскиими коммиссиями, с данными цен на валюту/ценные бумаги
- Инсайдерская торговля, Подставные торги, Откаты по торгам
- Фронтраннинг
- Сотрудник намеренно нарушает работу IT-систем банка, не относящихся к безопасности
- Выдача платежного терминала неавторизованным лицам
- Мошенненничество с ключами платежного терминала
- Мошенничество с зарплатными проектами
- Переоформление залоговых документов
- Сотрудник получает откат от страховщиков за навязывание страховки клиентам
- Хищения со счетов касс, контрагентов, отделений и других технических счетов
- Фиктивные сотрудники, Поддельные больничные, Завышение показателей

Триггеры комплаенс онлайн контроля ЦБ

- **ТИП 1** «Веерное распределение ЮЛ денежных средств по счетам ФЛ, с последующим их обналичиванием»
- **ТИП 2** «Веерное распределение ЮЛ денежных средств по счетам ИП, с последующим их обналичиванием»
- **ТИП 3** «Смена назначения платежа, сопровождаемая «ломкой» НДС»
- **ТИП 4** «Смена назначения платежа, направленная на покупку наличной торговой выручки у оптово-розничных предприятий»

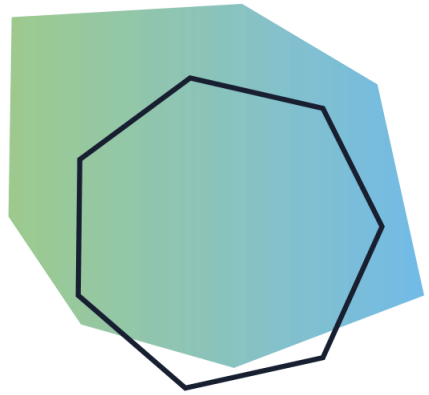
Комплаенс контроль



Санкционный контроль

- Контроль реквизитов входящих и исходящих документов по спискам:
  - OFAC SDN List
  - Объекты международных санкций
  - Список банком с иностранным капиталом и т.п.

- Алгоритм поиска элементов списка по неточному совпадению в реквизитах документа
- Работа с белыми списками исключения
- Расследование инцидентов - выявленных соответствий реквизитов документа с элементами списков



FUZZY

СПАСИБО!