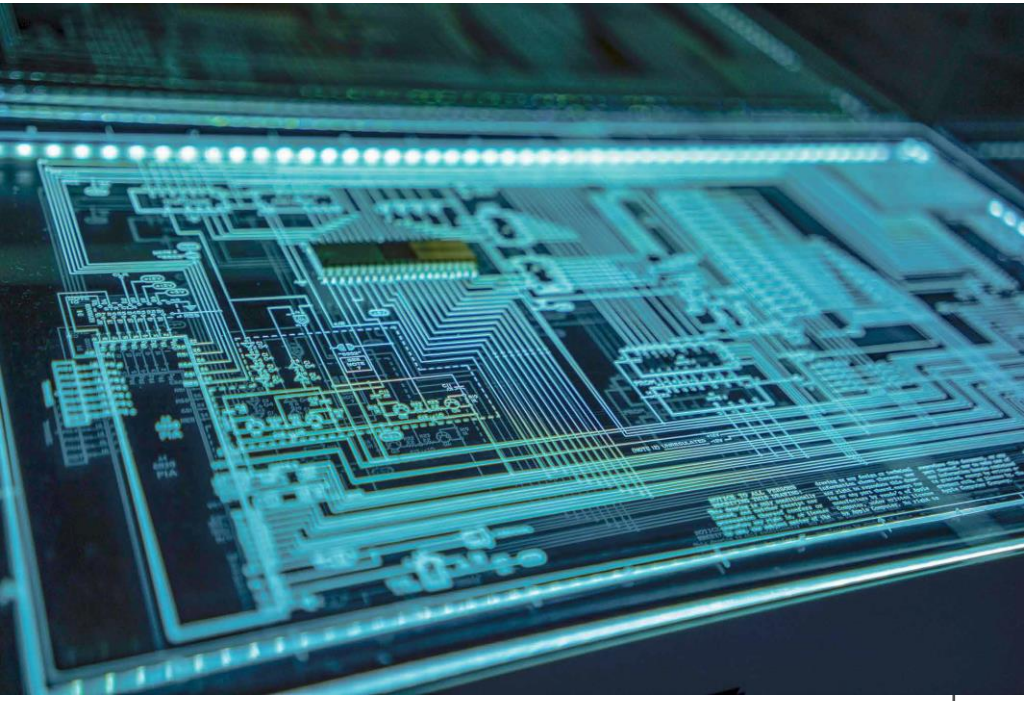
Smart Fraud Detection

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

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

Цели и задачи
борьбы с внутренним мошенничеством

Внутреннее мошенничество

Тип мошенничества	Тип риска
Внутреннее мошенничество	Проведение мошеннических операций со средствами клиентов
	Присвоение денежных средств с чужих счетов клиента/банка
	Кража персональных данных клиентов

Бизнес-кейсы для внутреннего мошенничества

- Для успешных противодействий мошенничеству со стороны сотрудников необходимо оперативно получать информацию о действиях пользователей
- Для выявления подозрительных действий Система должна уметь строить профиль Оператора и Клиента
- В случае аномального поведения Оператора или Клиента выдавать уведомления и создавать инциденты, например:
  - Увеличение продаж
  - Изменение времени продаж (например, после закрытия)
  - Продажи с разных IP адресов
  - Попытки подбора параметров для одобрения кредита

Бизнес-кейсы для внутреннего мошенничества

МОНИТОРИНГУ И АНАЛИЗУ ПОДВЕРГАЮТСЯ

- Финансовые операции по счетам клиента \ внутрибанковским счетам
- Просмотр \ поиск \ подбор персональных и финансовых данных клиента
- Изменение персональных и финансовых данных клиента
- Активности пропускной системы офис \ касса \ ячейки ...
- Информация по действиям на рабочей станции \ трафику
- 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
  - Работа в нетипичное время …

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

Адаптивная аутетификация 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

Новые требования к системам мониторинга

- Основная цель: уменьшить время обнаружения злоумышленника

Smart Fraud Detection
общие принципы работы

Почему решение Smart Fraud Detection?

Мониторингу и анализу подвергаются:

- Финансовые операции по счетам клиента/внутрибанковским счетам по всем направлениям обслуживания: кредитование, депозиты, банковские карты, рассчетно-кассовое обслуживание …
- Просмотр/поиск/подбор персональных и финансовых данных клиента
- Изменение персональных и финансовых данных клиента
- Активность пропускной системы: офис/касса, ячейки…
- Информация по действиям на рабочей станции/трафику

Отслеживание зависимости операций

- По различным бизнес направлениям
- В различных системах автоматизации ИТ-архитектуры

Адаптивная аутентификация по видео

ВИДЫ МОНИТОРИНГА – ФОТО И ВИДЕО ДАННЫЕ

Аутентификация сотрудника:

- Поиск лица сотрудника в общей базе, построение «отпечатка» лица на стороне клиента, поиск на стороне сервера

Анализ поведения сотрудника:

- Определение количества людей перед камерой
- Определение эмоционального состояния человека
- Определение позы сотрудника в целом и направления поворота головы в частности, определение направления взгляда
- Определение классов объектов в кадре
- Детектирование смартфона в кадре
- Манипуляции с камерой (закрывание камеры, изменение угла, подстановка фото

Адаптивная аутентификация по видео

ОБЩИЙ ПРИНЦИП РАБОТЫ – ФОТО И ВИДЕО ДАННЫЕ

- На стороне клиента для снижения объема трафика и нагрузки на серверную инфраструктуру используются оптимизированные свёрточные нейросети
- Использование локального хранилища для буферизации при отсутствии связи с сервером, отправка при восстановлении связи

- Варианты внедрения клиентского приложения:
  - Отдельное приложение
  - Пакет компонентов для существующего web-приложения

Результаты работы:

- Доступны в правилах операций сотрудника в виде параметров \ дополнительной оценке риска
- Атипичные события сохраняются в системе для возможности настройки правил \ расследования инцидентов

Схема обработки транзакций

Мобильные приложения

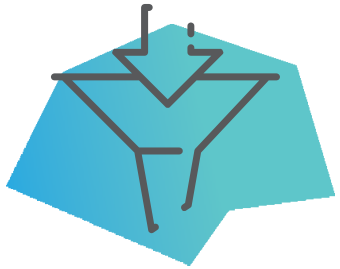
Интернет Банк

Контактный центр, Офис

Эмиссия, Эквайринг…

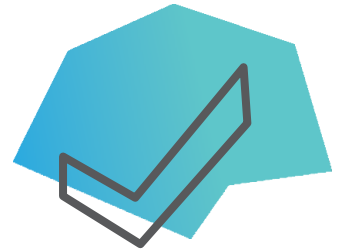
ПРИЛОЖЕНИЯ

Обработка транзакции

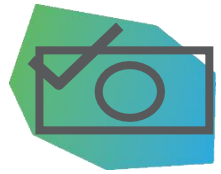


Оценка риска

Наборы правил

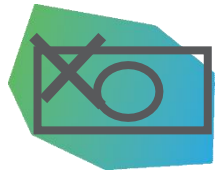


ПРОВЕРЕНО



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

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

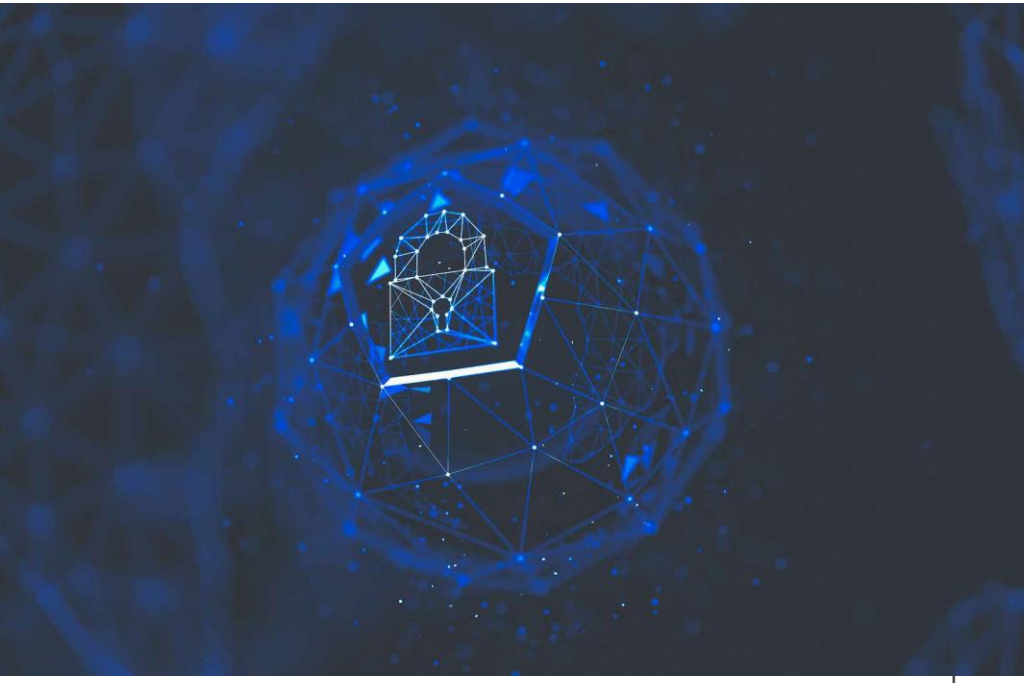
Управление доступом

Управление инцидентами

Отчет-ность

Планиров-щик

Фронт-офис: основные модули системы



Модуль обработки транзакций – выполняет следующие функции:

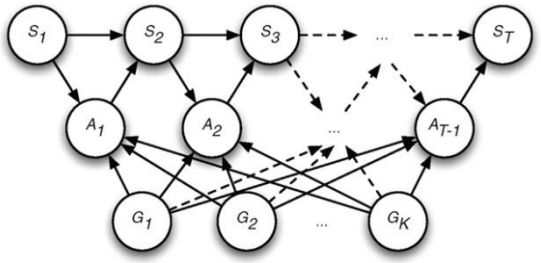
- Обработка \ преобразование входных данных: TCP (ISO 8583), HTTP/HTTPS (JSON)
- Обогащение транзакции справочными данными из внешних источников
- Формирование ответов с рекомендованным действием внешней системе в реальном времени

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

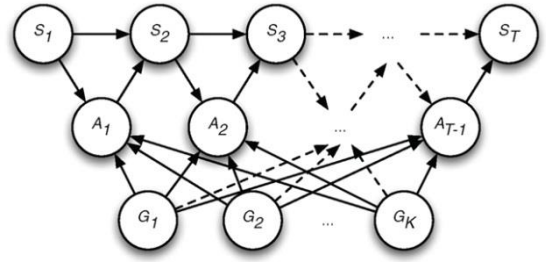


Модуль правил - модуль для построения собственной модели управления рисками:

- 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

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

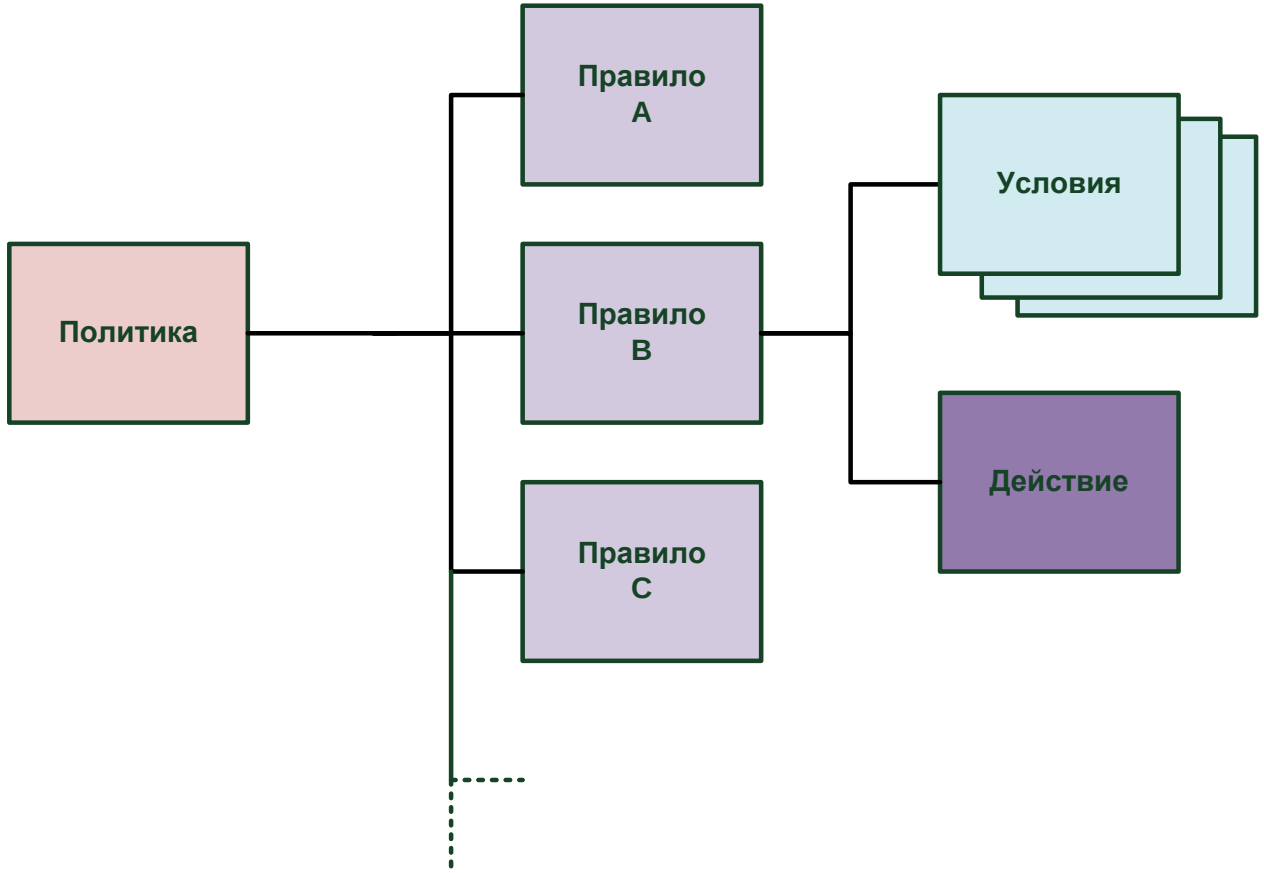
Substring –
получение подстроки (балансовый счет, БИН карты)

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

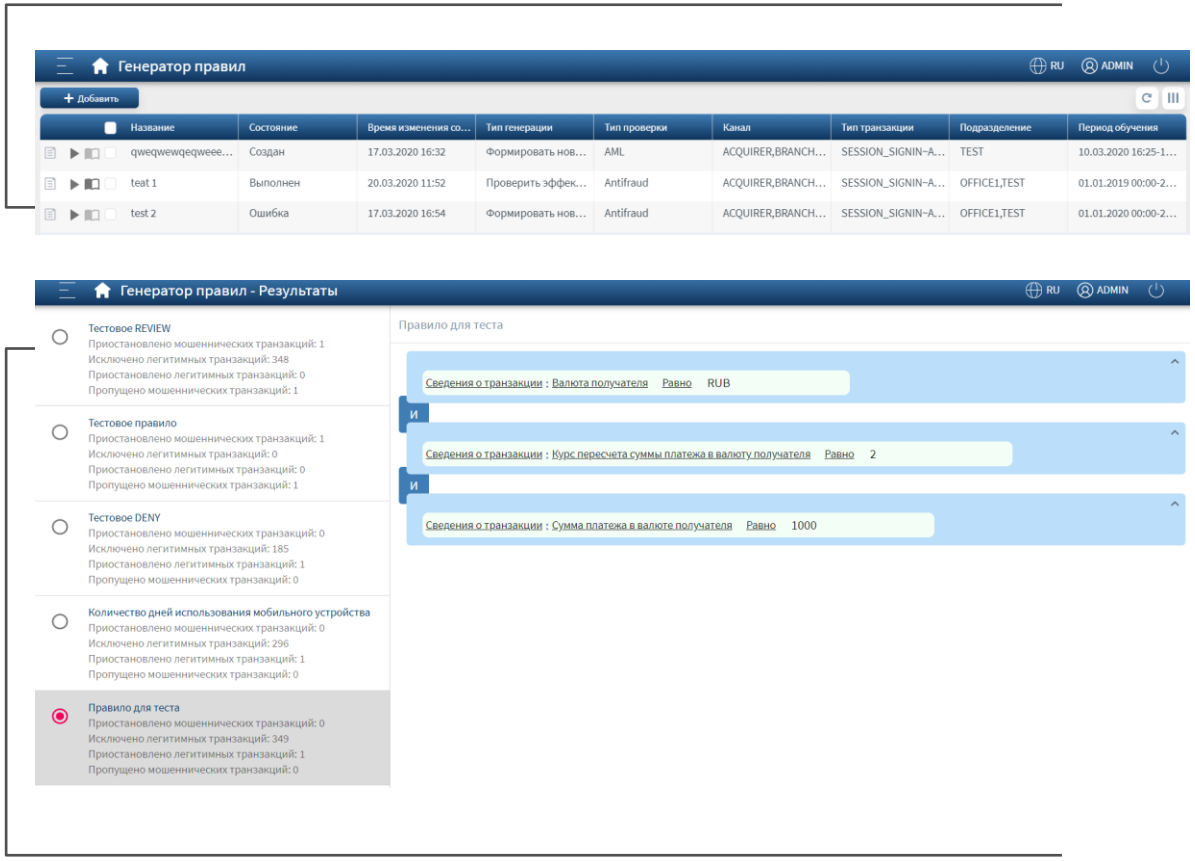
- Работа с правилами в режиме тестирования
- Хранение истории изменения состояния
- Бальная система подправил для формирования составного правила
- Генератор правил

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:

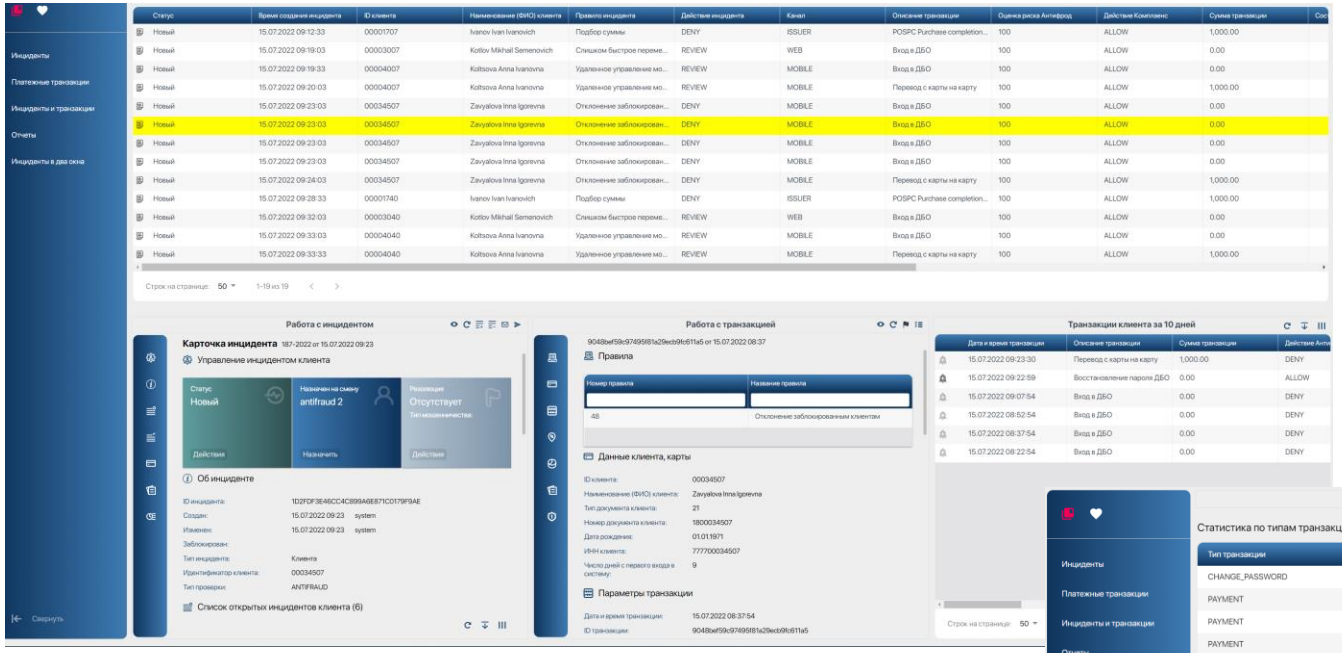
Управление правилами – интерфейсное решение для определения конкретных действий в зависимости от параметров и риска (настройка правил, настройка списков)

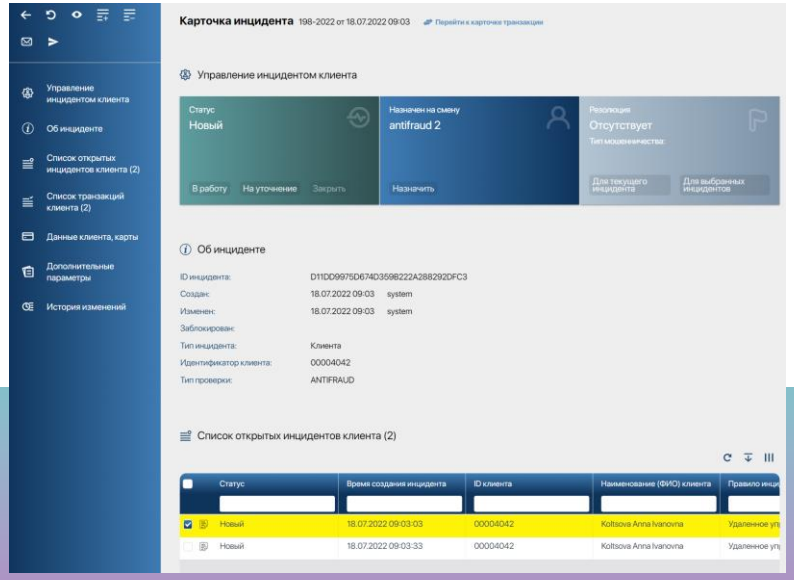
- Можно устанавливать любые правила обработки транзакций
- Большое количество готовых к использованию политик
- Работа с «черными» и «белыми» списками
- Генератор правил на исторических данных

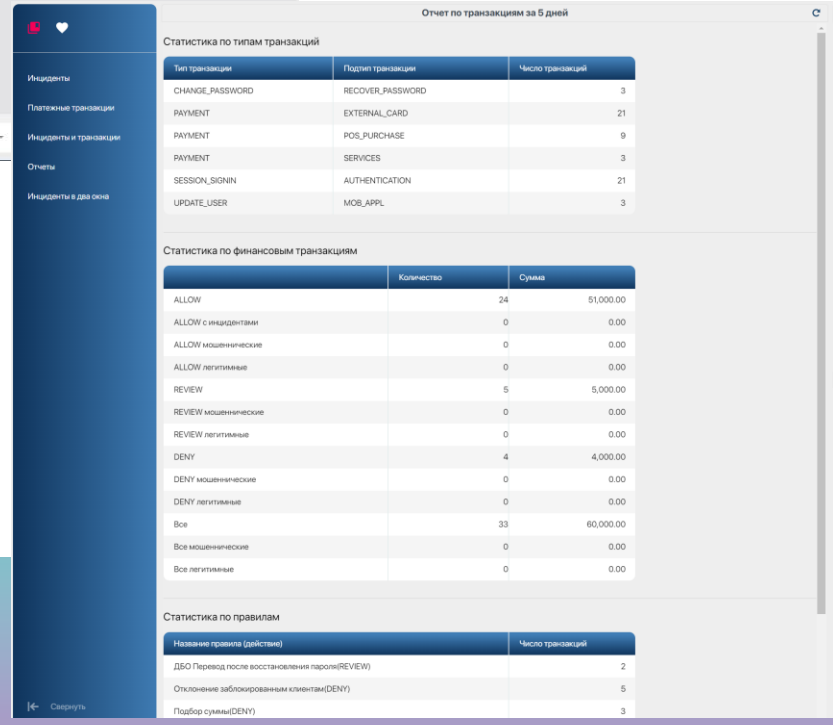
Расследование инцидентов – интерфейсное решение для расследования инцидентов и просмотра любых событий офицером безопасности

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

Бэк-офис: расследование инцидентов







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, Astra Linux, Alt Linux, RedOS)

Сервера приложений:

Фронт-офис: java приложения, в целях быстродействия

Бэк-офис: java приложения

Базы данных:

Oracle

PostgreSQL

Производительность

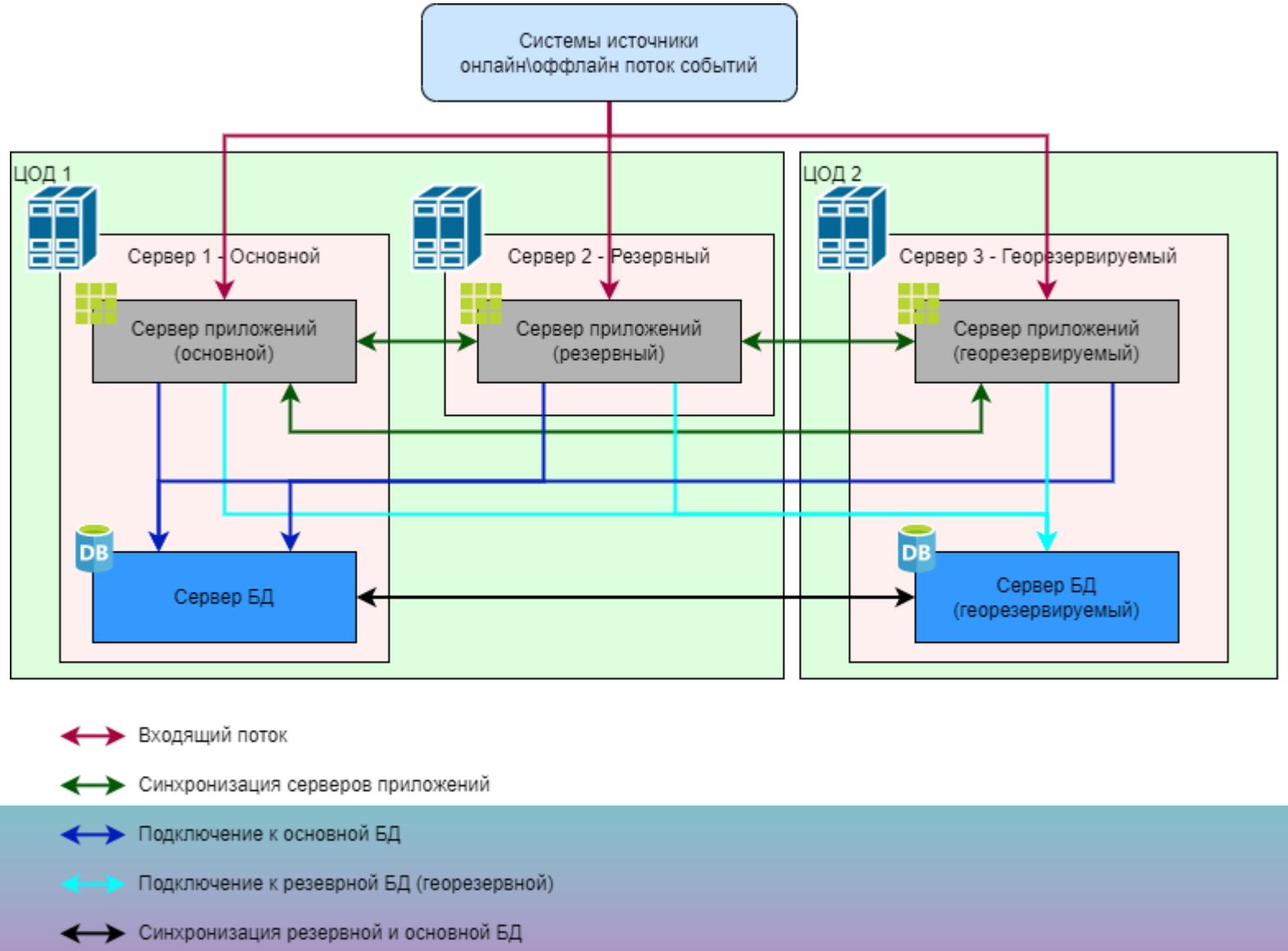
Параметры для расчета:

- 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

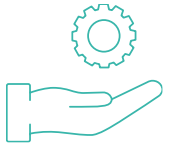


Преимущества системы

Виды мониторинга сотрудников подразделений: камера, микрофон

Кросс-канальный мониторинг действий сотрудников и финансовых операций

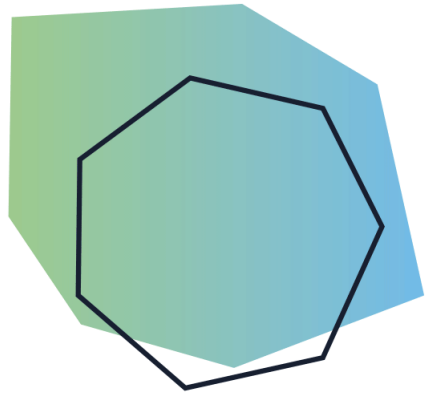
Самообучающийся модуль оценки поведения сотрудников



Вычисления на стороне клиента: большая приватность и не нужен широкий канал

Быстрая адаптация к новым аномалиям поведения

Мониторинг рабочего времени, контроль нарушений



FUZZY

СПАСИБО!