Jet Detective
Описание решения

Оглавление

1 Заявление о конфиденциальности

Данный документ содержит конфиденциальную информацию, принадлежащую АО «Инфосистемы Джет».

Заказчик обязуется не разглашать, не копировать, не распространять данный документ и не раскрывать его содержание среди юридических и/или физических лиц, не связанных непосредственно с принятием решения по использованию описанного продукта без предварительного согласования с Исполнителем.

Указанные ограничения не распространяются на информацию, которая включена в данный документ, но была известна Заказчику до получения данного документа от Исполнителя, на информацию, известную из общедоступных источников, или на информацию, полученную Заказчиком из сторонних источников, относительно которых Заказчик не несет каких-либо обязательств по сохранению конфиденциальности полученной информации.

2 Общее описание Jet Detective

Система обеспечит получение, хранение, обработку, анализ данных и визуализацию его результатов, а также передачу информации во внешние системы в автоматическом режиме. Подобное решение позволяет обеспечить своевременное реагирование на мошеннические действия и защитить Банк и его клиентов.

Решение Jet Detective имеет микросервисную архитектуру: единое приложение строится как набор небольших сервисов, каждый из которых отвечает за свои функции. Такой подход дает два преимущества:

- Система легко масштабируется за счет четких границ, разделяющих компоненты;
- Для изменения одного компонента, не требуется внесения изменений в остальные.

Особенность решения состоит в том, что для использования Jet Detective не требуются навыки программирования, и вся рутинная работа по поддержке Системы, настройке правил и политик обработки операций осуществляется через ее интерфейс.

2.1 Описание функции противодействия мошенничеству

Для анализа событий в автоматическом режиме используются методы обработки данных, позволяющие рассчитать количественный показатель риска совершения мошеннической операции. Система реализует два базовых метода оценки риска:

Rule-based подход, Профилирование.

Помимо отклонений от профиля клиента, Система способна выявлять мошеннические операции, вызванные в том числе компрометацией учетных данных клиента.

Анализ операции и оценка ее риска представляет собой комплекс действий:

- формирование и перерасчет оценки объектов модели данных, в том числе параметров профилирования, агрегатов (статистических данных) и пр., которые будут использованы в правилах анализа;
- работа аналитических алгоритмов и т.д., результатом которых является формирование оповещения в интерфейсе (инцидент) и рекомендация Системы по дальнейшей обработке события: разрешить проведение операции, запретить или приостановить ее для обработки вручную (то есть решение о типе операции будет принимать аналитик Системы).

Выявление рисков мошенничества обеспечивается за счет двух ключевых особенностей Системы:

- управляемые правила и политики оценки операций;

- аналитическими модели выявления мошенничества: обработка инцидентов аналитиком позволяет адаптировать модель выявления мошенничества по проверенным транзакциям или на базе задаваемых обучаемых выборок.

3 Функциональное описание Jet Detective

3.1 Общая функциональная схема

Ниже приведено описание функциональной схема Jet Detective. Отдельные сервисы решения здесь объединены в логические блоки на основании выполняемых функций.

Модуль интеграции обеспечивает информационный обмен между системами заказчиков и системой Jet Detective. JD может взаимодействовать со всеми распространенными системами и легко настраивается под атрибутивный состав и формат данных целевых систем.

Модуль управления данными позволяет создавать через вэб-интерфейс описание таблиц-приемников для данных, получаемых из модуля интеграции. Также он отвечает за сохранение данных в СУБД и последующее отображения в интерфейсе и использование для расчета статистики на базе истории.

Модуль бизнес-логики отвечает за настройку и запуск правил и сценариев, формирование результатов работы стратегий.

Модуль визуализации и анализа позволяет проводить точечный анализ данных, формировать отчетность в ручном и автоматическом режимах, формировать графики и диаграммы и проводить анализ эффективности стратегий. Модуль визуализации

3.2 Описание модуля визуализации

Деятельность сотрудников Заказчика, связанная с анализом подозрительных операций, принятием решений по результатам анализа, настройкой объектов хранения данных и настройкой правил выявления осуществляется в вэб-интерфейсе Системы.

Верхнеуровневое описание основных форм интерфейса приведено далее.

Доступ к областям интерфейса зависит от прав пользователя, заданным ролевой моделью.

Обработка сформированных системой инцидентов осуществляется в инструменте расследования, сконструированном на основании принципа одного окна: вся информация, необходимая для проведения анализа и принятия решения по операции собрана на одном экране.

Пример экрана анализа приведен на Рисунке 1.

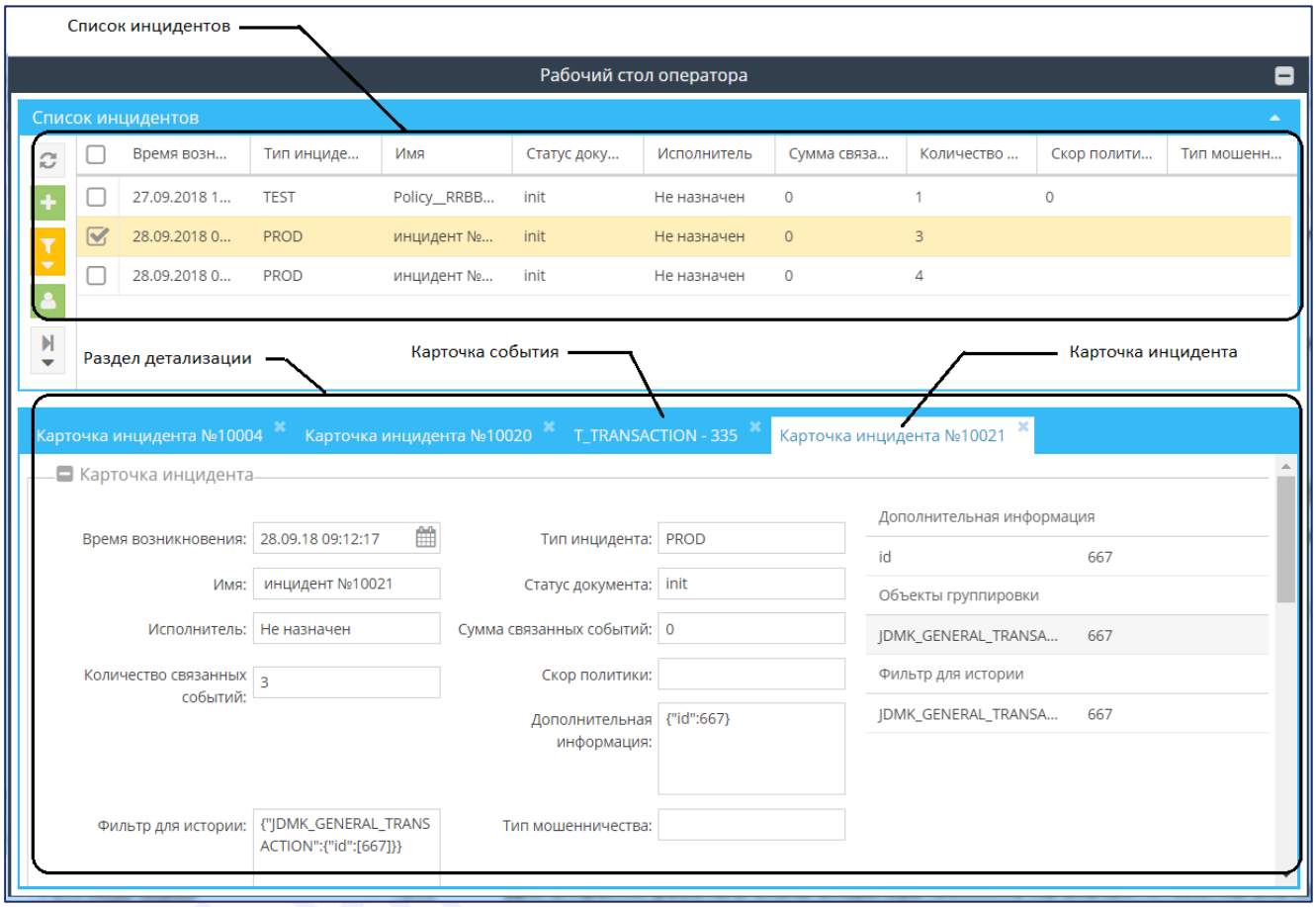

Рисунок 1 – Общий вид интерфейса расследования решения Jet Detective

При разработке интерфейса Системы учитывалась необходимость проведения кросс-канального анализа операций, т.е. контроля действий в информационных системах массового обслуживания клиентов, имеющих различные каналы и инструменты взаимодействия клиента с ресурсами Заказчика.

Для анализа связей событий используется форма кросс-канального расследования, показанная на Рисунке 2. Она состоит из трех частей:

- Диаграмма, где точками отмечены события, распределенные во времени (горизонтальная ось) и по каналам (вертикальная ось). На рисунке событие, связанное с расследуемым инцидентом, отмечено вертикальной линией.
- Форма события (справа) для отображения деталей.

- Список событий, попавших в окно диаграммы (внизу).

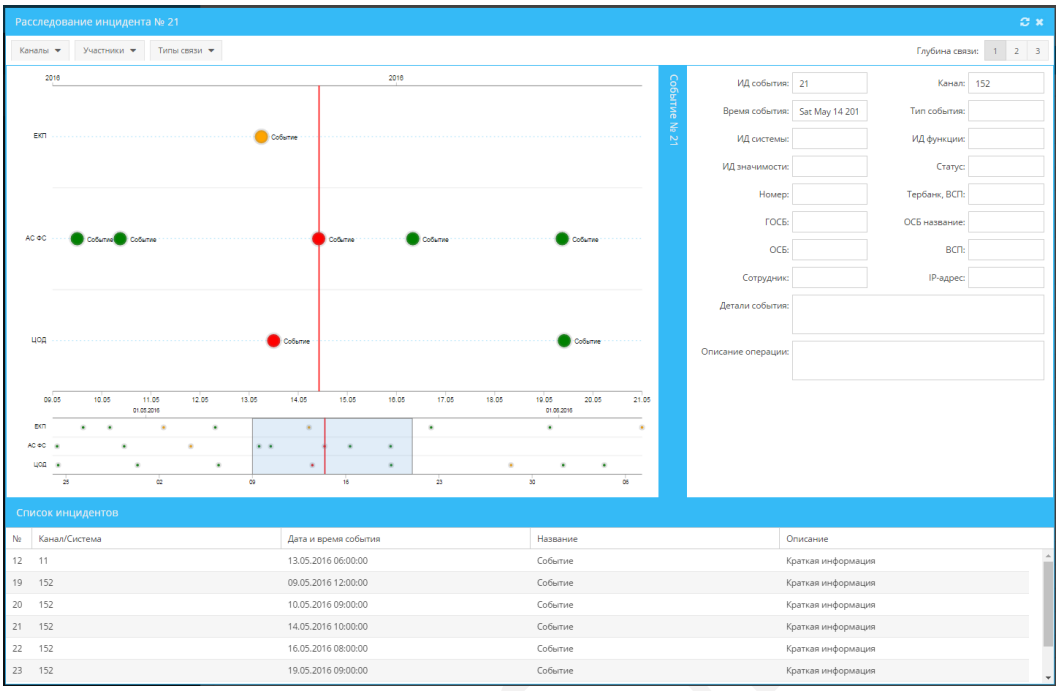

Рисунок 2 – Форма кросс-канального расследования

Система предлагает возможности настройке графиков для визуализации бизнес-показателей и бизнес-данных. В том числе, графическое или табличное представление основных показателей эффективности работы системы фрод-мониторинга, таких как процент ложно-положительных и ложно-отрицательных срабатываний правил (на основании размеченных пользователем операций).

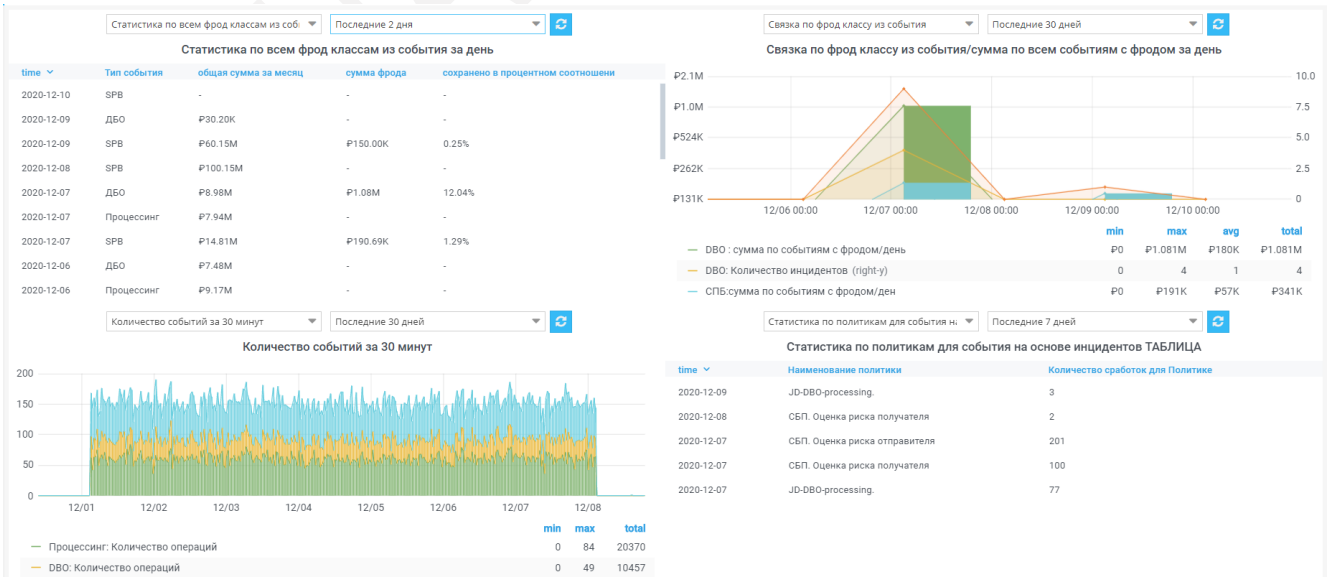

Рисунок 3 – Пример графиков

3.3 Описание модуля бизнес-логики

Создание и настройка правил и политик обработки операций осуществляется в интерфейсе Системы администраторами или аналитиками в зависимости от ролевой модели.

Для создания/изменения правил выявления мошенничества в системе используется конструктор правил.

Система позволяют использовать для анализа:

- атрибуты (поля) операции, переданной в обработку
- данные из связанных с операцией справочников
- данные из хранящихся в системе списков
- значения, рассчитанные на основании исторических данных за определенный период времени.

Каждому правилу можно присвоить скоринговый бал при использовании в качестве основной модели анализа – скоринговой модели.

На Рисунке 4 приведено окно настройки правил.

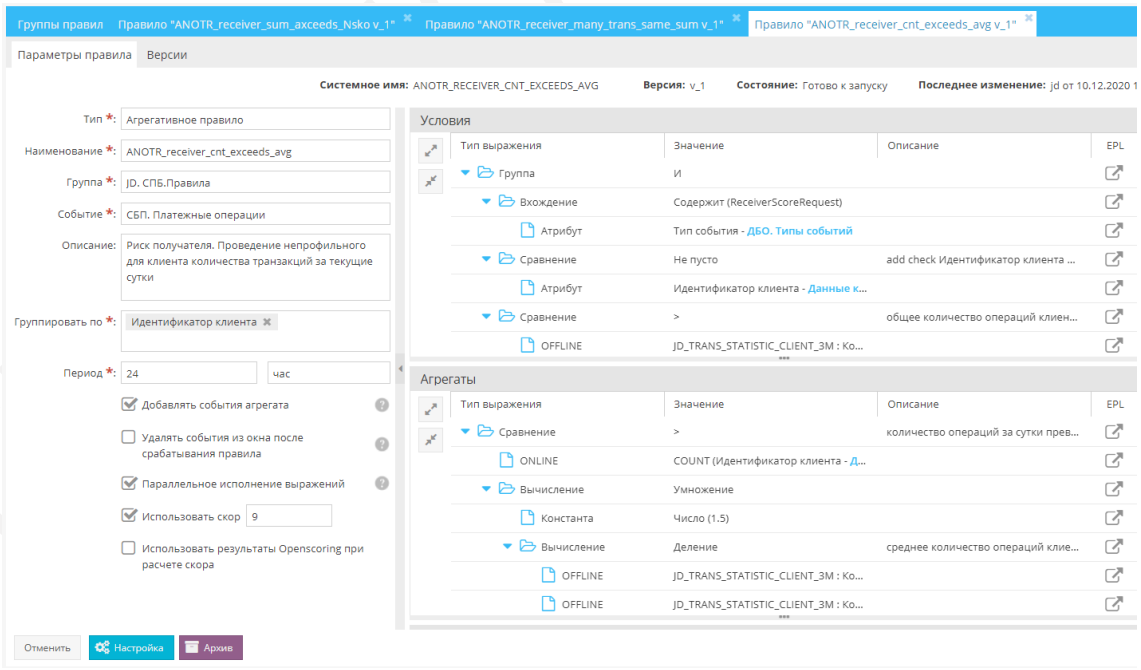

Рисунок 4 – Окно настройки правил

Управление использованием правил осуществляется через общую сущность – политику. Через нее определяется, в частности:

- набор действий, которые должны быть выполнены по результатам срабатывания сценариев (в том числе, формирование ответов во внешнюю систему, создание инцидентов, отправка уведомлений на почту, заполнение списков, формирование индикатора уровня риска)
- настройка модели сценария (скоринговая, с учетом или без учета последовательности срабатывания правил за период)
- режим запуска (тестовый или продуктивный)
- настройка кросс-канальных сценариев.

Пример окон настройки политики приведен на Рисунках 5 и 6.

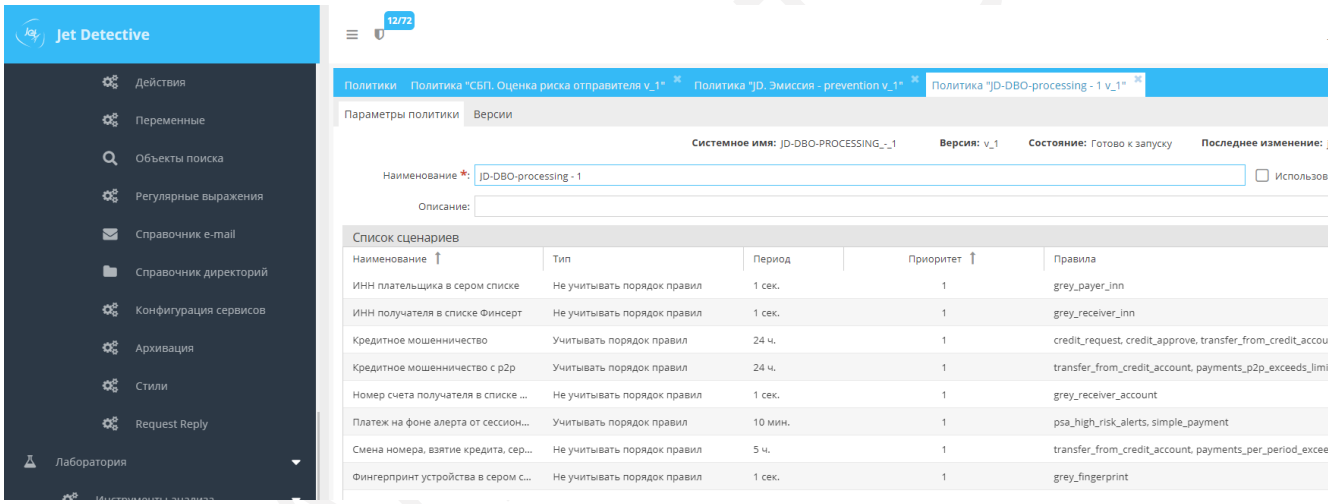

Рисунок 5 – Окно настройки политик

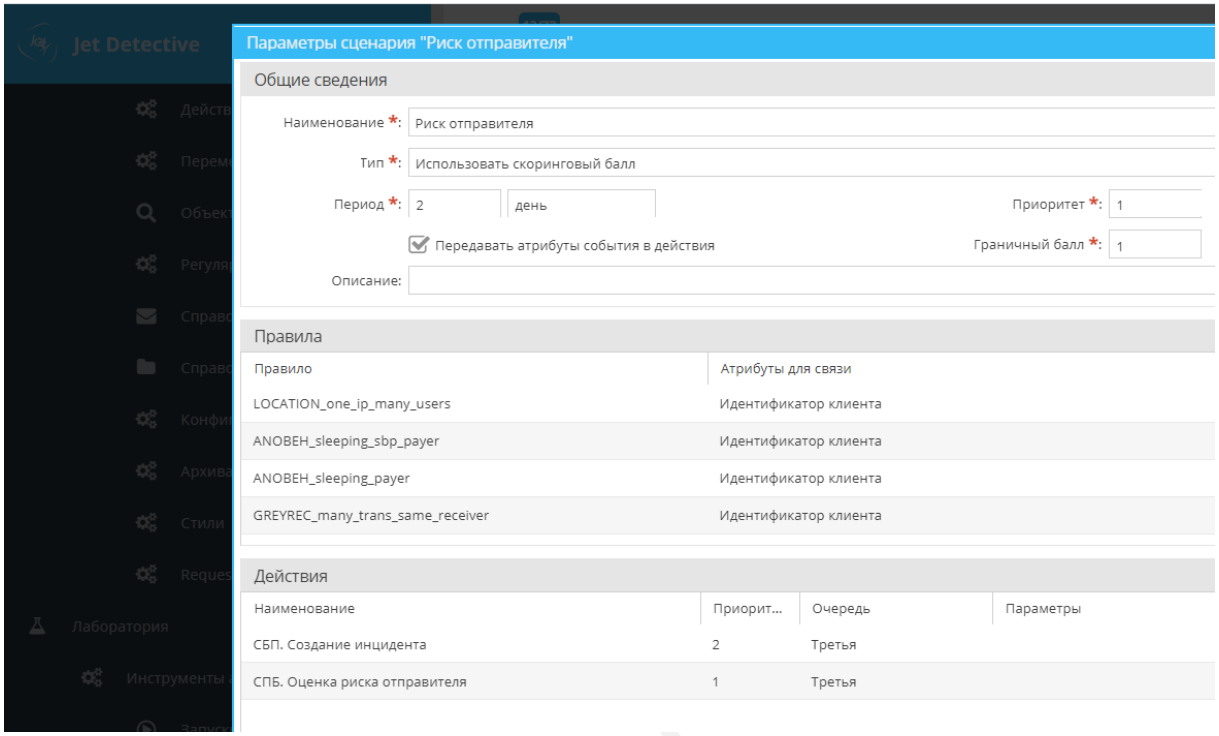

Рисунок 6 – Сценарии срабатывания

3.4 Описание модуля управления данными

Предложенное решение по противодействию мошенничеству построено на принципе свободного управления данными, поступающими как извне, так и циркулирующими внутри Системы. Ядром Системы является Модуль Business Object Model (BOM), позволяющий создавать внутренние бизнес объекты (транзакции, счета, карточки клиентов, филиалы, сотрудники и т.д.) и online или offline наполнять их данными при использовании ETL-процедур.

Такие действия клиентов как вход в личный кабинет, совершение платежа, начисление или списание бонусных балов, регистрация новых продуктов и услуг регистрируются системой ДБО и передаются в систему противодействия мошенничеству. Полученной информацией она наполняет существующие бизнес-объекты в соответствии со схемой их формирования, хранения и расчета. Это позволяет отслеживать отклонения от профилей объектов, обеспечивает контроль связей между ними, характер изменения их бизнес-показателей (статусов, уровней аккаунтов и пр.). Пример объектной модели приведен на рисунке 7.

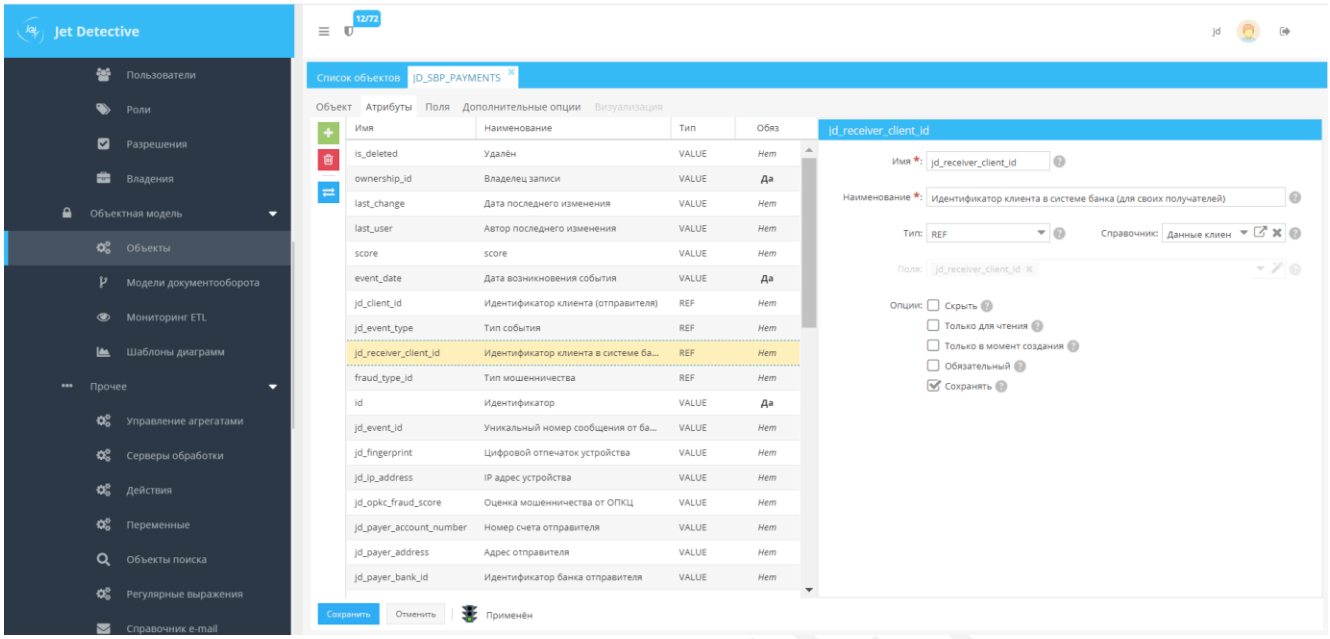

Рисунок 7 Объектная модель данных

3.5 Описание интеграционного слоя

В упрощенном виде процесс онлайн-обработки операции изображен на схеме:

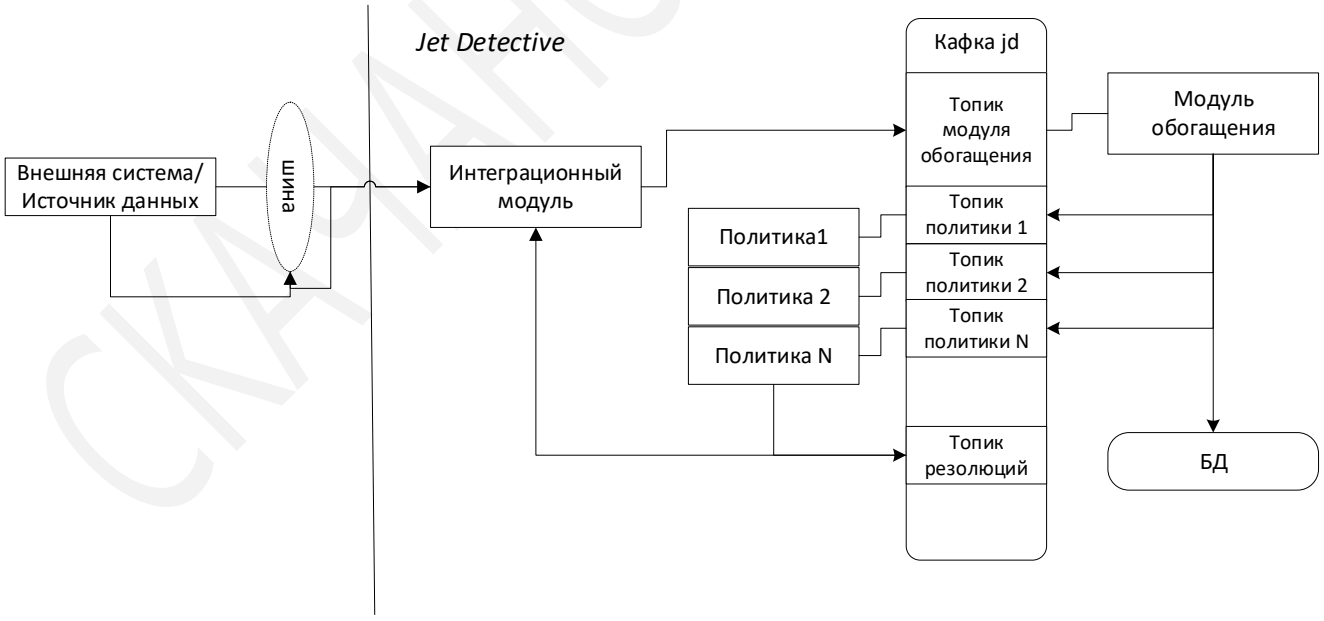

Схема 1 Обработка операции в JD

Взаимодействие с внешней системой может происходить, как напрямую, так и через промежуточную шину данных.

С точки зрения назначения данных, получаемых из источника, их можно разделить на два вида:

- Данные для списков/справочников, используемые для анализа или процесса разбора инцидентов и сохраняемые напрямую в БД.

  В режиме полной перезаписи или обновления. Способы обновления списков и справочников:

  - Вручную
  - Автоматически с использованием ETL
  - Автоматически с использованием скрипты при срабатывании триггера в JD
- Данные для обработки правилами.

3.6 Типы взаимодействий с внешним источником

Некоторые варианты интеграций с внешней системой / источником данных:

- Файловая интеграция. Файлы загружаются на сервер на регулярной основе с заданной периодичностью.
- Интеграция с базой данных. Данные загружаются из определенной таблицы/представления БД. Способ получения данных зависит от базы и требований к интеграции.
- Интеграция с системой, имеющей rest-api для взаимодействия. Настройка взаимодействия в соответствии с описанием.
- Интеграция через очередь сообщений. Большая часть интеграций на данный момент строится на базе взаимодействия через очередь сообщений (kafka, rabbit mq, ibm mq, active mq и т.д.). Формат сообщений json или xml.

4 Описание модулей Jet Detective

Решение имеет сервисориентированную архитектуру с межмодульным взаимодействием через REST. Каждый сервис представляет собой самодостаточное приложение, управляемое на уровне OS через systemd.

В таблице приведен перечень сервисов с кратким описанием их функционала.

Сервис / модуль	Описание
jd-bom	Модуль предназначен: ▪ для настройки бизнес-модели объектов (Business Object Model), с которыми будет работать Система. ▪ загружаемых из внешних источников (баз данных, файлов различных типов, файлов протоколов серверов, интеграционных компонентов смежных систем и прочих. ▪ для настройки логики загрузки и преобразований данных для объектов, трансформация данных: очистка, обогащение, агрегация, связывание данных. ▪ для настройки системы хранения для объекта. ▪ для отображения загруженных объектов в интерфейсе. ▪ создание массивов данных для обучения моделей выявления.
jd-enrichment	Модуль обогащения данных предназначен для: ▪ Обогащения данных объекта за счет поиска и добавления атрибутов связанных с ним объектов. ▪ Формирования сущности объектов для анализа. ▪ Сохранение поступивших в систему данных в базе данных. Участвует в потоке online и offline анализа событий.
jd-cep-coordinator	Модуль отвечает за маршрутизацию анализируемых событий внутри Системы и выполняет следующий функционал: ▪ Настройка статических правил выявления. ▪ Настройка правил для моделей выявления. ▪ Настройка и тестирование политик выявления: хранение параметров выполнения политик, сбор данных из jd-bom за промежуток времени. ▪ Связывание событий с результатами проверки по правилам. ▪ Выполнение действий после применения правила: o пометка события или группы событий суммарным значением скоринговых баллов правил, значением истина\ложь или другими показателями работы правил выявления;

	○ внутренние действия: создание инцидента, запуск нотификации, добавление в черный список, пересчет атрибутов профиля; ○ внешние действия: запуск нотификации, загрузка данных из системы-источника, выгрузка данных в систему-потребитель, формирование ответа на запрос внешней системы, выполнение функции внешнего программного интерфейса, выполнение программного сценария. Модуль участвует в потоке online и offline анализа событий.
jd-cep-engine модуль анализа событий	Модуль предназначен для обработки входящих потоков данных и реализует следующие функции: ▪ Применение правил и политик выявления к событиям. ▪ Вызов внешних сервисов для оценки события. ▪ Оценка события. Участвует в потоке online и offline анализа событий.
jd-auth	Сервис аутентификации предназначен для организации доступа пользователей к функциям и данным Jet Detective и реализует следующие функции: ▪ настройка справочников доступа: учётные записи и роли пользователей. ▪ аутентификация и авторизация пользователя. ▪ настройка прав доступа к действиям пользователей.
jd-afs-workflow	Сервис отвечает за создание, настройку и хранение моделей документооборота, которой будут подчиняться выбранные объекты Jet Detective. Модуль реализует следующие функции: ▪ настройка модели смены статуса, действий при переходах и логики определения ответственного для события в соответствии с выполняемым переходом; ▪ связь модели с объектами; ▪ перевод объекта по статусам; ▪ инициация действий при переходе;
jd-aggregate	Сервис отвечает за: ▪ Создание и хранение настроек логики и результата расчета агрегата, ▪ запуск и расчет агрегатов по заданным параметрам (в т.ч. по заданному расписанию). ▪ предоставление необходимых для работы модуля анализа результатов расчета.

	Агрегат - это сущность, которая позволяет создать вычисление на промежутке времени по разным объектам системы.
jd-dictionary-service	Обеспечивает создание, настройку и хранение глобальных переменных и объектов поиска. Предоставляет необходимые для работы cep-engine глобальные переменные и осуществляет поиск по спискам (в т.ч. полнотекстовый поиск). Производит настройку структуры списочных данных и логику их загрузки.
jd-report-service	Сервис отвечает за работу с отчетами в системе и выполняет следующие функции: ▪ загрузка, хранение и выгрузка шаблонов отчетов, ▪ формирование отчетов по шаблонам в различных форматах, ▪ формирование отчета по шаблону согласно заданному по расписанию; ▪ сохранение сформированных отчетов в отдельном журнале, ▪ размещение отчетов в папку, отправка на e-mail, ▪ сохранение истории запросов отчета со значениями входных параметров, по которым он был сформирован; ▪ повторное получение ранее сформированного отчета.
jd-email-service	Сервис отвечает за отправку сообщений по электронной почте.
jd-schedule-service	Сервис отвечает за создание и выполнение задачи по расписанию. Сервис используется при выполнении расчета агрегатов и при формировании отчетов.

Доступ к базе данных и к API приложения при взаимодействии модулей осуществляется с использованием технологических учетных записей (ТУЗ) по протоколу http с применением метода basic auth.

5 Ограничения среды окружения

Поддерживаемые ОС:

- RHEL/Centos версий 7.5 и выше.
- RedOs
- Альтлинукс 8СП

Специализированные требования к платформам виртуализации отсутствуют.

В качестве аппаратной платформы должно использоваться x86/64 совместимое оборудование. Другие ограничения, накладываемые на аппаратные средства, определяются на этапе расчет сайзинга оборудования и зависят от требований к функционалу системы со стороны Заказчика.

В состав Jet Detective включены следующие OpenSource решения:

- Nginx 1.16
- AdoptOpenJDK 11
- Grafana 7.3.4
- Prometheus 2.29
- Apache Kafka 2.8.0

В качестве внутренней базы данных Jet Detective использует:

- PostgreSql версии выше 12 ИЛИ
- Oracle версии выше 12.2.0.1.