**Алгоритм выявления подозрительных операций QIWI**

**1. Что послужило причиной создания продукта**

Обеспечение высокого уровня информационной безопасности и противодействие мошенничеству - одни из ключевых задач для любой финансовой организации. Безопасность для нее крайне важна, потому что любой бизнес - и QIWI не исключение - не может позволить себе проявить безответственность в отношении данных его пользователей. Кроме того, чем лучше, популярнее и удобнее для пользователя ваш продукт - тем, к сожалению, он более привлекателен для недобросовестных клиентов.

Для обеспечения безопасности финансовых операций QIWI использовала различные продукты - в частности, IBM Safer Payments, но ни один из них не имел требуемых технологических возможностей для предотвращения подозрительных транзакций в режиме реального времени, отвечающих потребностям нашего бизнеса.

Поэтому в определенный момент QIWI столкнулась с необходимостью построения принципиально новой системы противодействия мошенничеству, которая позволила бы использовать технологии big data и машинного обучения и системы анализа поведения пользователей (UBA) для принятия решения о легитимности транзакций в режиме реального времени. Аналогов продукта на рынке, подходящего QIWI, компания не увидела, поэтому приняла решение разработать его самостоятельно.

**2. Какую задачу решает продукт**

Алгоритм отслеживает исторические потоки незаконных операций и формирует на их базе поведенческую модель, которая оценивает как сумму, потенциальное назначение, так и причастность к кластерам недобросовестных клиентов. Модель обогащается данными из внешних источников и позволяет обнаруживать потенциально "плохие" платежи с высокой точностью. При подозрении они попадают на дополнительную проверку для проведения как автоматизированного, так и ручного анализа. Это помогает выявлять и блокировать подозрительные операции эффективнее, чем раньше.

**3. Продукт разрабатывался силами сотрудников компании или с привлечением подрядчиков**

Разработка продукта велась силами сотрудников QIWI. В ней принимали участие 12 человек: 4 разработчика ядра системы, 4 разработчика, обеспечившие рабочее место оператора, и 4 сотрудника, отвечавшие за анализ данных и построение моделей.

**4. Срок и этапы создания продукта**

Разработка алгоритма выявления подозрительных операций состояла из следующих этапов:

* Исследование задачи - с декабря 2018 года по март 2019 года;
* Разработка прототипа - с марта по июль 2019 года;
* Разработка MVP - с июля по декабрь 2019 года;
* Эксплуатация и доработка - с декабря 2019 года по настоящее время.

В рамках исследования был проведен анализ задачи, опробованы методики её решения, выбраны средства и инструменты реализации и сформирована команда.

В рамках демонстрации работоспособности концепции был разработан прототип, реализующий основной функционал системы и позволяющий решать необходимые задачи по выявлению подозрительных транзакций.

В MVP продукта вошли:

* Исправленное и оптимизированное ядро системы;
* Пользовательский интерфейс оператора для решения основных задач управления системой;
* Коннекторы к основным используемым процессинга.

Эксплуатация и доработка включает в себя улучшение существующего и разработку нового функционала согласно запросам пользователей и заказчиков системы. Этот этап реализуется QIWI в итеративном режиме, где результатом каждой итерации становится повышение эффективности и улучшение ключевых характеристик продукта.

**5. Имеет ли продукт аналоги в России и/или зарубежом**

В качестве аналогов могут рассматриваться международные банковские системы антифрода - такие, как RCA, ThreatMetrix или IBM Safer Payments. Однако стоит учесть, что это не прямые аналоги продукта, запущенного QIWI. Такие системы сходны с разработанным QIWI алгоритмом рядом общих характеристик - например, возможностью настраивать проверку транзакционных данных.

**6. Ключевые характеристики продукта**

Решение QIWI основано не на транзакционном анализе, а на анализе поведения пользователей с применением технологий искусственного интеллекта.

При разработке системы применялся принцип обеспечения максимальной гибкости и вариативности полученного решения. Кроме того, сама задача обработки транзакционных данных подразумевает необходимость высокой производительности системы. Разработанная система соответствует поставленным задачам и обеспечивает следующие ключевые характеристики:

* **Масштабируемость.** В рамках продукта реализована возможность развертывания системы в кластерах kubernetes с обеспечением автоматического масштабирования при увеличении нагрузки. Такой подход позволяет обрабатывать практически любые разумные потоки транзакций, сохраняя перцентиль 99.5 на уровне 50 миллисекунд;
* **Отказоустойчивость.** Система показала надежную работоспособность в условиях распределенных и множественных кластеров развёртывания, обеспечивая обработку свыше 99.9% транзакций в соответствии с заданным SLA;
* **Высокая производительность.** Система обеспечивает время обработки транзакции от 5 миллисекунд, до 94 миллисекунд на перцинтиле 99.9;
* **Высокая скорость применения изменений.** Измененные правила анализа в течении минуты распределяются по всему ядру системы, не вызывая потери производительности в процессе обновления;
* **Гибкость описания правил анализа.** Для анализа транзакций используются правила, записанные на скриптовом языке. Сотрудники, не являющиеся программистами, осваивают разработку правил достаточно быстро;
* **Гибкость конфигурации и расширения.** Модульность системы позволяет оперативно подключать к ней различные процессинги, в том числе учитывать при обработке транзакций агрегированные данные от других процессингов.
* **Единый антифрод-комплекс.** Функционал системы позволяет интегрироваться "поверх" существующих решений, расширяя их функциональность, а также объединять множественные системы антифрода в единый комплекс.

В рамках системы применяются технологические алгоритмы, которые позволяют с помощью технологий искусственного интеллекта обрабатывать массив данных, - поэтому искусственный интеллект влияет на оптимизацию самого расчета.

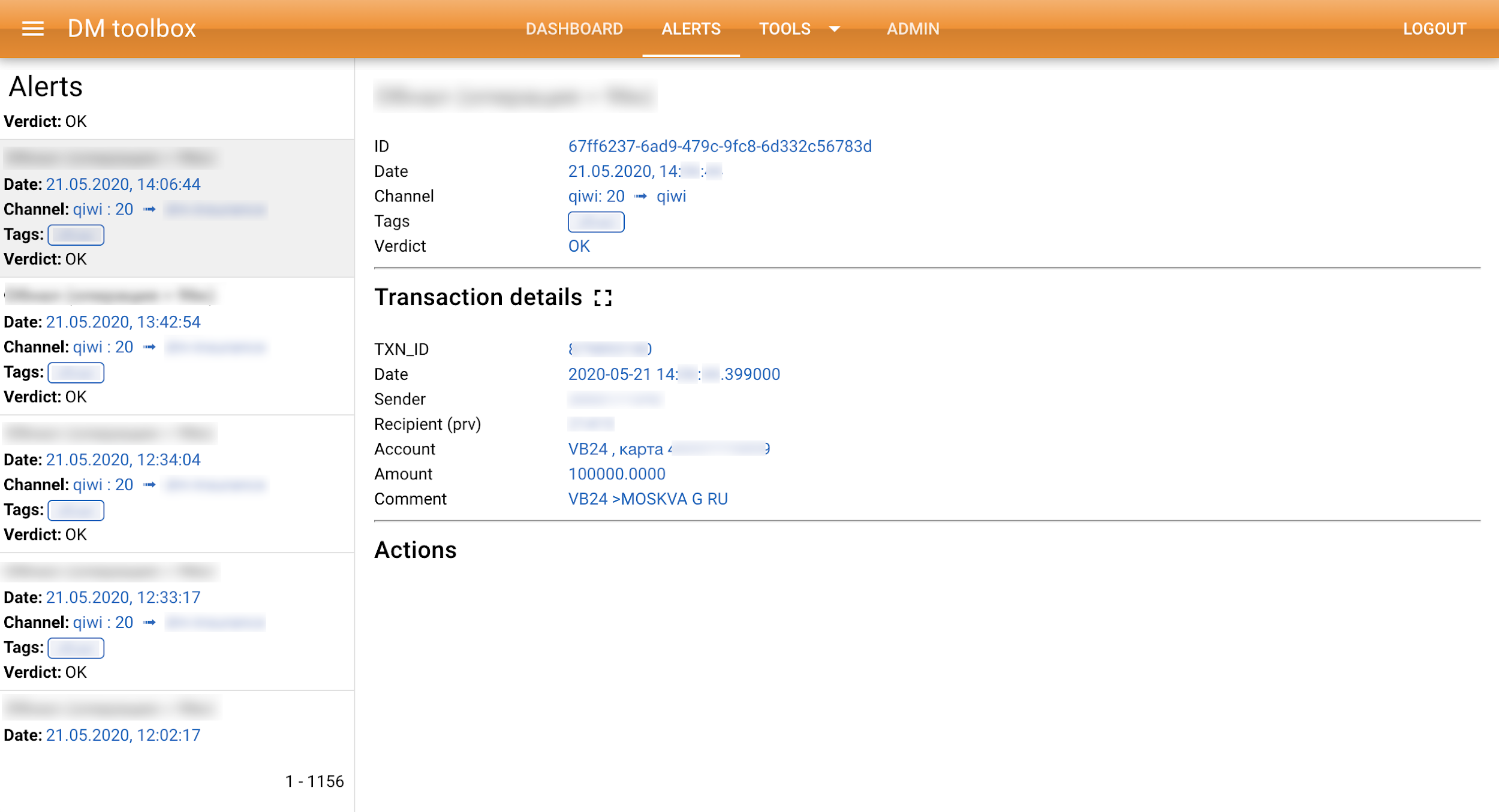
Для расчета и выявления подозрительных операций применяются алгоритмы и графовая нейронная сеть, которая позволяет уменьшить объем требуемых вычисляемых данных. Любая пользовательская активность представляется в виде графов, которые подаются на вход графовой нейронной сети. В результате образуются пользовательские кластеры, внутри которых видна любая мошенническая активность.

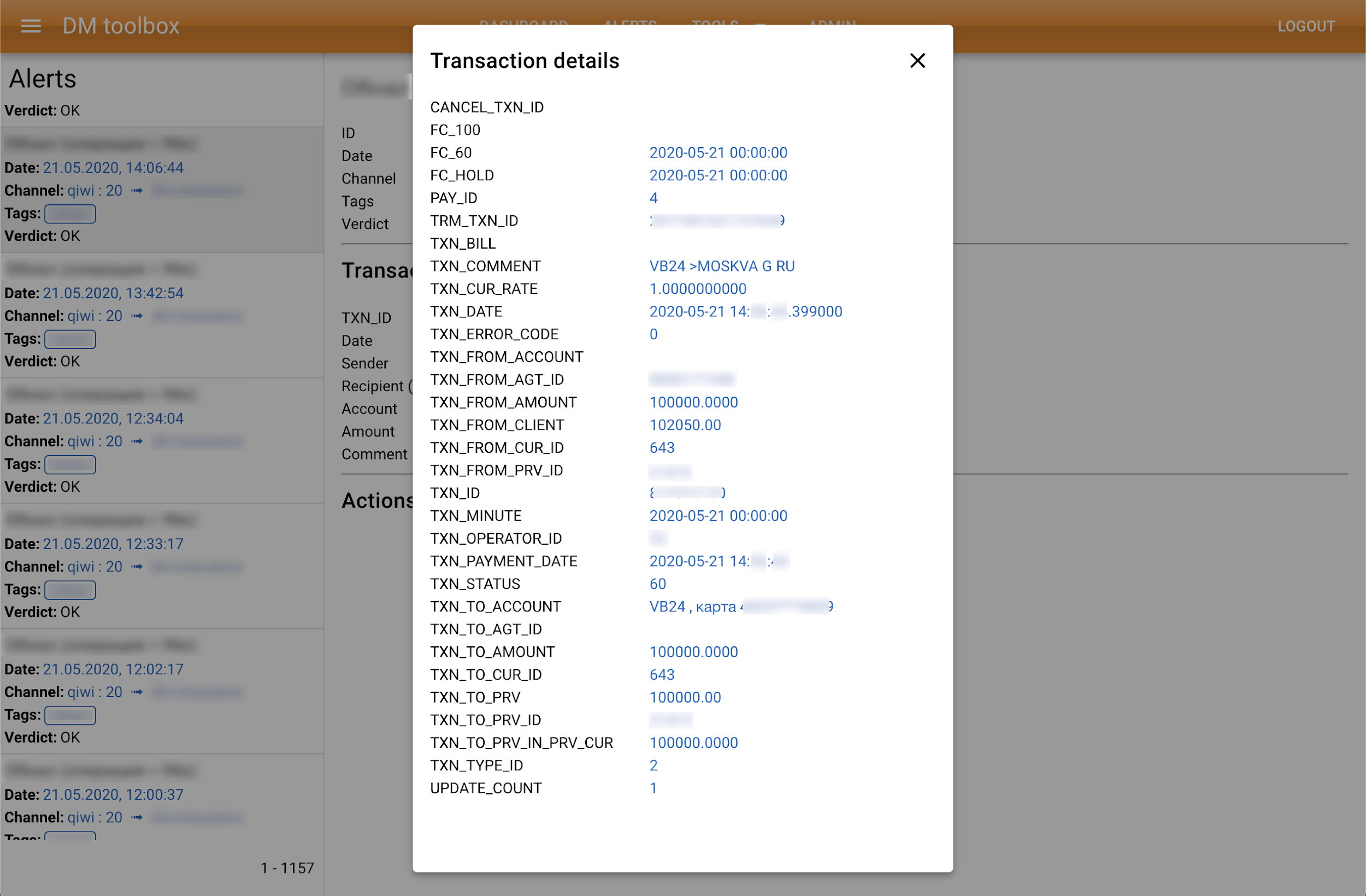
Графовая нейронная сеть дает готовый ответ, который обрабатывается в режиме реального времени. Это одно из ключевых преимуществ продукта: с момента поступления запроса до момента принятия по нему решения проходят считанные миллисекунды.

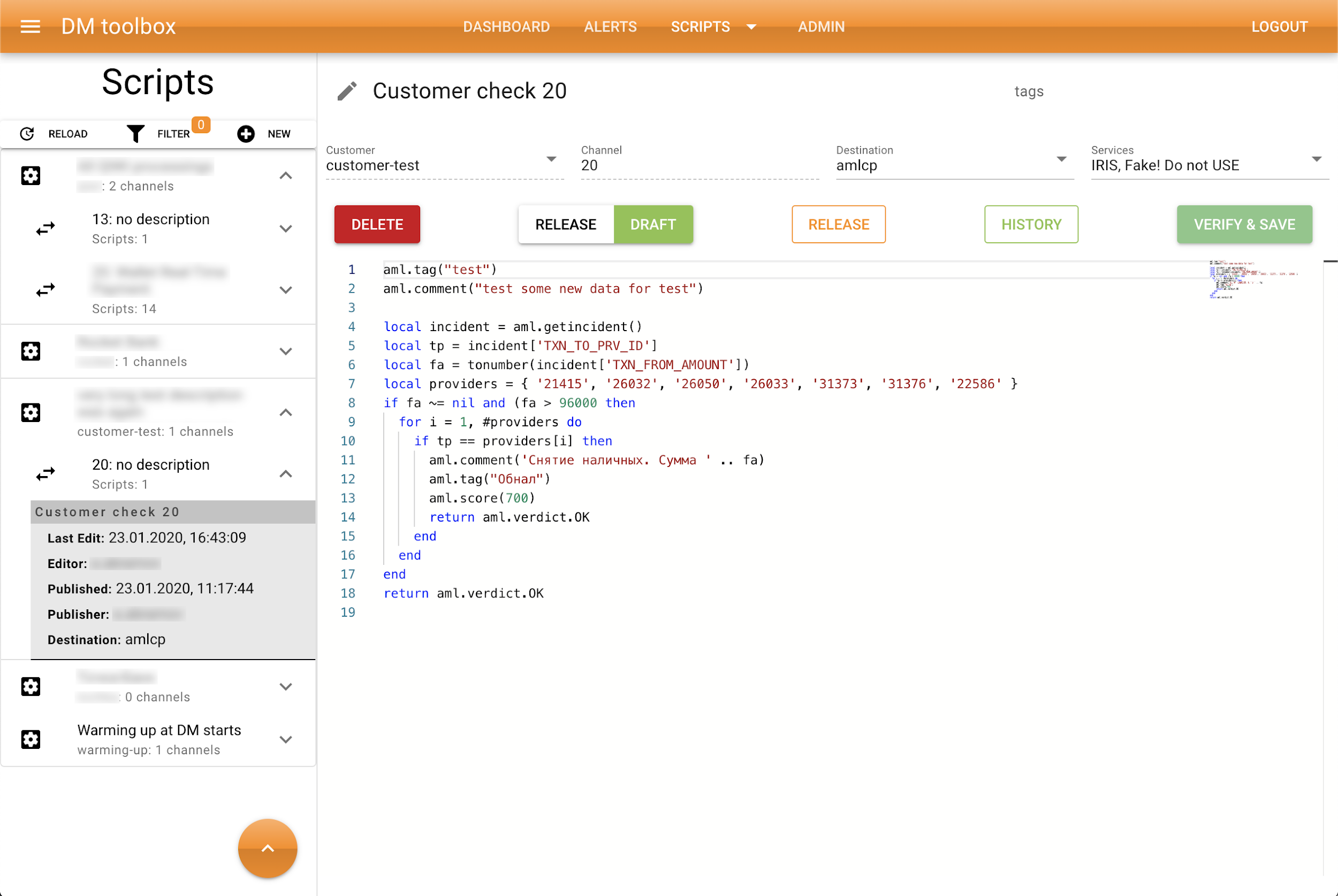
В результате тестирования и моделирования работы алгоритма QIWI увидела, что он крайне эффективно блокирует проведение подозрительных платежей.

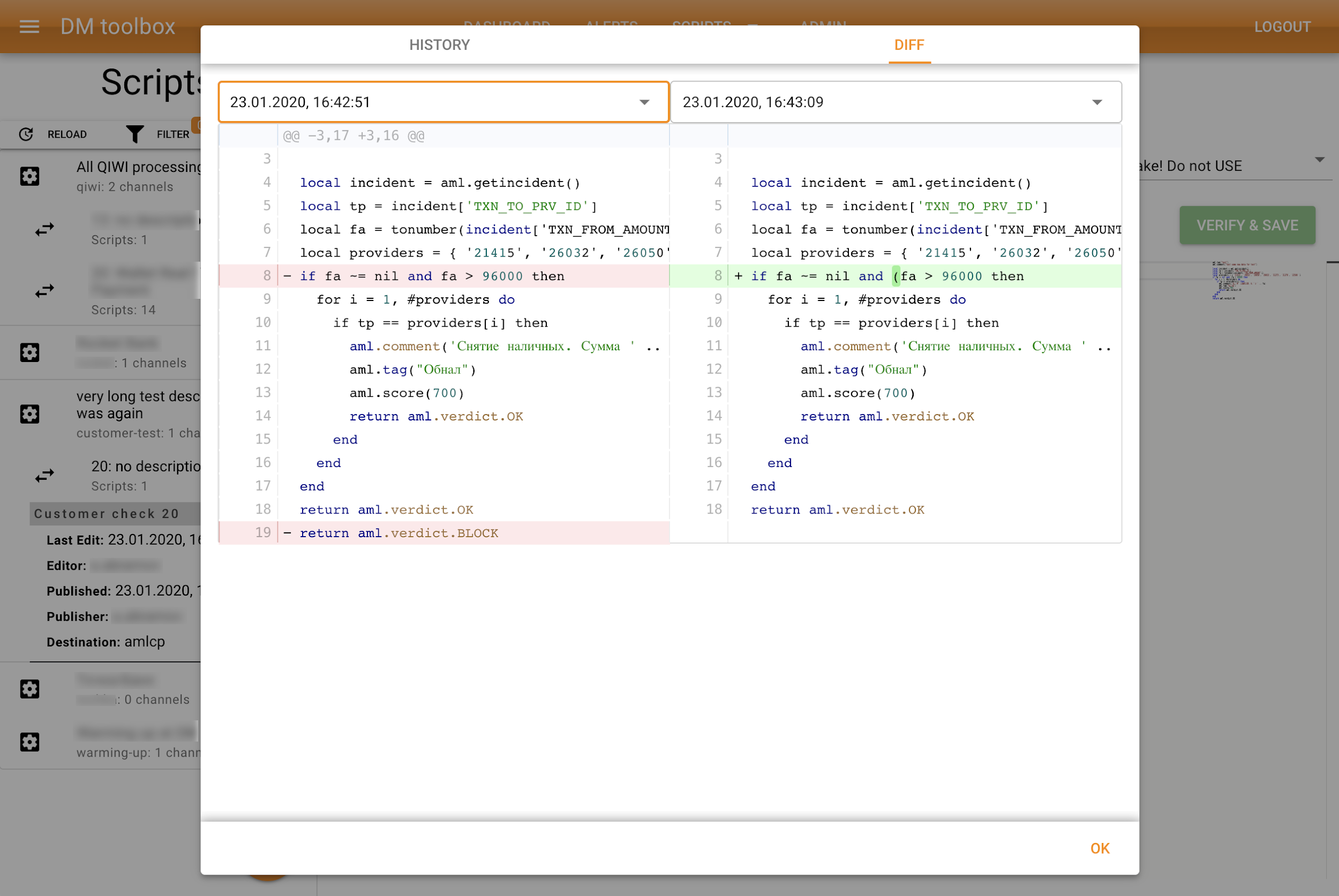
Внешний вид интерфейса управления.











**7. Продукт используется только компанией или есть возможность внешнего использования**

На текущий момент продукт используется только QIWI, но обладает потенциалом внешнего использования - поэтому представители других компаний могут обратиться к QIWI за дистрибуцией.

**8. Ключевые показатели использования продукта компанией**

Основными показателями эффективности использования алгоритма выявления подозрительных операций с момента его внедрения в декабре 2019 года QIWI считает следующие:

* Снижение количества подозрительных операций в системе;
* Проактивная защита клиентов от совершения платежей в пользу недобросовестных поставщиков услуг;
* Уменьшение популярности QIWI Кошелька среди пользователей скрытых сетей - “даркнета”.

**Публикации о продукте в СМИ**

<https://ria.ru/20191225/1562833724.html>

<https://news.rambler.ru/other/43413677-qiwi-vnedrila-novyy-algoritm-vyyavleniya-podozritelnyh-operatsiy/>

<https://kod.ru/qiwi-novyi-algoritm-na-baze-ai/>