В данной работе продемонстрировано использование средств Arduino IDE, MySQL, Apashe, а также микроконтроллеров ESP 8266 и датчиков DS18B20 для создания системы мониторинга температуры в помещениях с использованием mesh-сети. Разработанная система позволяет автоматически собирать данные по температуре с установленных мест и хранить их в базе данных. Система обладает высокой отказоустойчивостью и гибкой структурой, что позволяет с легкостью и без рисков изменять количество узлов в сети.

Список использованных источников

1. Киселев М. Ячеистые сети [Электронный ресурс] // «Экспресс Электроника», CITForum: [web-сайт]. – Режим доступа: http://citforum.ru/nets/wireless/mesh/

2. Блинова В.М. Метод контроля функционирования сетей передачи данных в автоматизированной системе управления промышленным предприятием. // Промышленные АСУ и контроллеры. 2012. №3.

3. Кучерявый А.Е., Прокопьев А.В., Кучерявый Е.А. Самоорганизующиеся сети. – СПб.: «Любавич», 2011. – 312 с.

УДК 004.056

А. Г. Ярцев[1,2], В. В. Лавров[1]

[1] ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина», г. Екатеринбург, Россия

[2] АО «СберТех», г. Екатеринбург, Россия

АЛГОРИТМЫ ОЦЕНКИ РИСКОВ И ПРИНЯТИЯ РЕШЕНИЙ ПО ОПРЕДЕЛЕНИЮ МОШЕННИЧЕСТВА В СОВРЕМЕННЫХ АНТИФРОД-СИСТЕМАХ

Аннотация. *В статье приводятся предпосылки и условия возникновения современных антифрод-решений на предприятиях банковского сектора, алгоритмы анализа, положенные в основу механизма их действия, а также функциональные и нефункциональные требования, предъявляемые к системам.*

Ключевые слова: *финтех, фрод, ФинЦерт, антифрод, Machine Learning.*

Abstract. The article presents the prerequisites and conditions for the emergence of modern antifraud solutions at enterprises of the banking sector, the analysis algorithms underlying the mechanism of their action, as well as functional and non-functional requirements for systems.

Key words: *fintech, fraud, FinCert, antifraud, Machine Learning.*

Цифровизация финансовой сферы является приоритетной задачей развития российской экономики, в целях решения которой посредством внедрения передовых технологий создаются условия для трансформации традиционных бизнес-моделей в инновационные [1, 2]. Согласно данным банковской

статистики, вышеуказанные мероприятия оказывают положительное воздействие на финансовое положение кредитных организаций, поскольку позволяют последним снижать операционные издержки, расходы на содержание персонала, сокращать риски невозврата денежных средств. Но оборотной стороной этого процесса выступает возросшее количество несанкционированных действий, совершаемых в электронной среде, в частности, направленных на информационные инфраструктуры банков. Данное явление получило название фрод (от англ. «fraud» – «мошенничество»). Злоумышленники производят атаки на системы межбанковских переводов, карточный процессинг, управление банкоматами, интернет – банкинг и платежные шлюзы. Одной из тривиальных разновидностей фрода является получение доступа к учетным данным клиентов финансово-кредитных учреждений и осуществление транзакций без получения на то их согласия (фишинг).

Согласно публичным данным, взятым с инфопортала АСОИ ФинЦерт ЦБ РФ [3], только в 2019 г. финансовые потери банковского сектора от фрода составили 6,4 млрд рублей. Статистика по несанкционированным операциям за 2017-2019 гг., представленная на рисунке 1, показывает, что число последних в сфере безналичных расчетов продолжает стремительно расти, а это значит, что и размер нанесенного ими материального ущерба будет приобретать все больший масштаб.

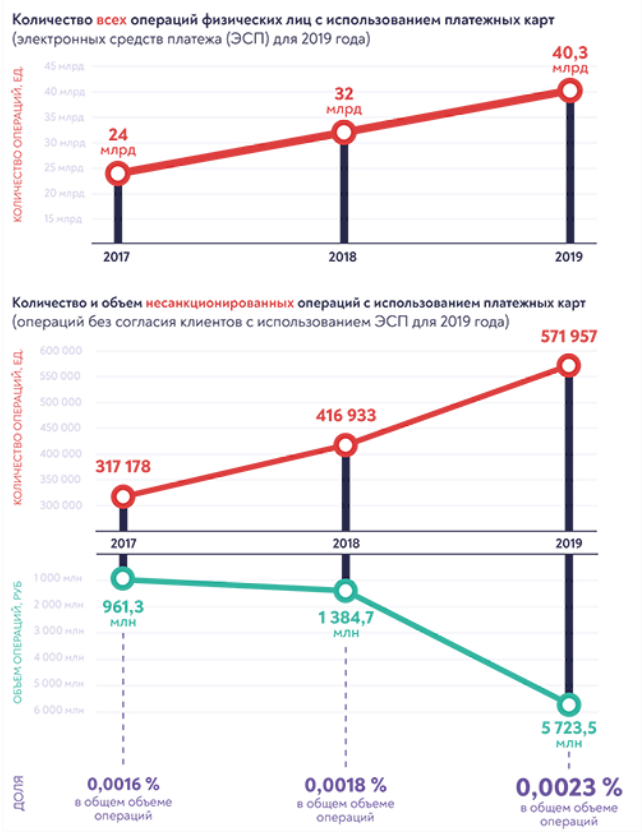

Рис. 1. Статистика по несанкционированным операциям за 2017-2019 гг. [3]

В связи с этим возникла необходимость найти технологическое решение, позволяющее обезопасить финансово-кредитные учреждения от незаконных атак на их информационные сервисы, чтобы свести к минимуму экономические риски. На законодательном уровне это нашло выражение в принятии Федерального закона от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты РФ в части противодействия хищению денежных средств», который был призван предотвращать операции по переводу денежных средств, совершаемых без согласия клиентов. Данная мера положила начало процессу разработки российский антифрод-решений.

Антифрод – системы – специализированные программные или программно-аппаратные комплексы, применяемые для предотвращения несанкционированных действий в финансовой сфере. Как правило, они включают в себя системы обнаружения (fraud detection), предотвращения (fraud prevention) и анализа (fraud analysis) мошенничества, а также интеллектуальной обучаемости (intellectual learning).

Следует отметить, что любая антифрод-система с точки зрения обеспечения непрерывности обслуживания управленческих и технологических процессов, а также требований к отказоустойчивости является business-critical системой, так как выход из строя ее отдельных компонентов будет вести к полной остановке бизнес-процессов, а их некорректное функционирование к увеличению рисков финансовых потерь для организации.

Отсюда к атрибутам качества, положенным в основу данных систем на этапе проектирования, можно отнести:

- распределенность;
- отказоустойчивость;
- надежность;
- безопасность хранения данных;
- высокая масштабируемость.

Помимо всего прочего, программная архитектура антифрод-систем определяется также законодательными ограничениями. В соответствии с требованиями стандарта PCI DSS, разработанного в целях повышения уровня безопасности данных владельцев платежных карт и содействия процессу повсеместного внедрения единообразных мер по их защите, запрещается хранить полный номер банковской карты (PAN) или кода безопасности (CVV). Вместо этого разрешается – только первые шесть и последние четыре цифры номера карты. К тому же, необходимо учитывать положения Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных», согласно которым передача имени держателя и периода эксплуатации карты возможна будет только по защищенным каналам связи.

Поскольку для банковской сферы характерен большой поток действий клиента, то проверка степени надежности транзакций может занимать длительное время, что отразится на общей производительности антифрод-системы. Чтобы оптимизировать этот процесс, повсеместно используется трехуровневые модели проверок, которые включают в себя:

– глобальные фильтры;
– простые эвристики;
– ядро классификатора.

Глобальные фильтры – списки значений параметров, при точном соответствии которых действие клиента автоматически отклоняется системой (рис. 2). Могут быть как статическими, так и динамическими. В данном блоке фильтрации используются правила (критерии) отбора по поиску в черных списках:

1) проверка IP-адреса, с которого пришел запрос на снятие средств с карты;
2) проверка банковской карты, с который совершается платеж;
3) проверка IP-адрес мерчанта и др.

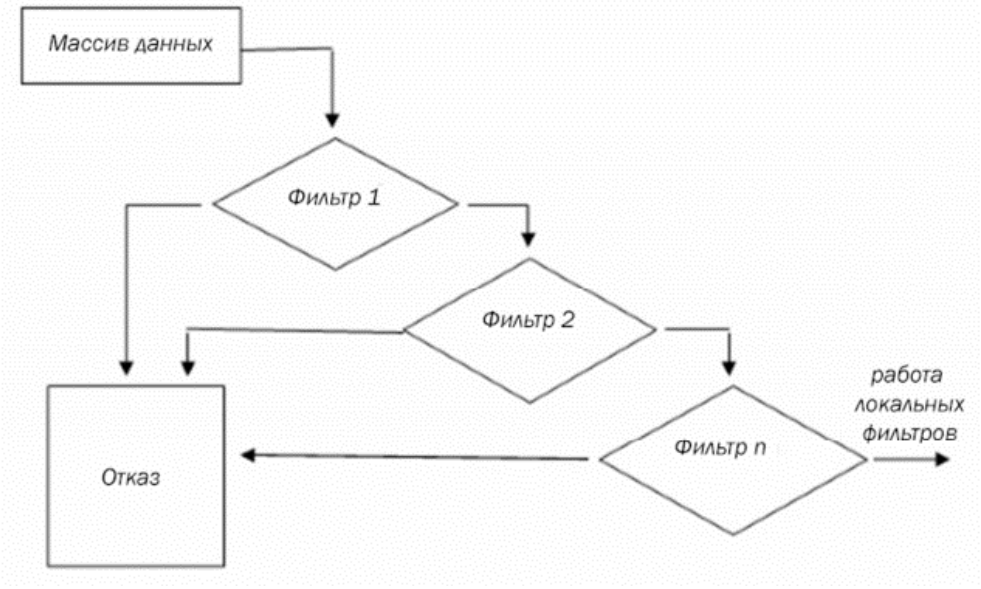

Рис. 2. Принцип работы глобальных фильтров

Если транзакция не проходит проверку хотя бы по одному из этих критериев, то процесс валидации прекращается, а запрос на списание средств с кары отклоняется.

Под простыми эвристиками принято понимать набор продукционных правил и условий, при срабатывании которых транзакции помечаются как небезопасные. Антифрод-системы могут включать в себя большое множество эвристик. К числу наиболее эффективных можно отнести следующие:

– одна банковская карта – много IP (инверсионный порядок: один IP – много банковских карт);
– одна карта – много транзакций;
– один клиент – много банковских карт;
– один клиент – много индексов, адресов электронной почты и др.;

Ядро классификатора – непосредственно алгоритмы, относящие активность пользователя к классу безопасности. В зависимости от того, к какому классу транзакция будет отнесена с точки зрения антифрод-системы, она будет

соответствующе обработана. Если подозрения не выявились, то клиент продолжает работать с сервисом без ограничений. В противном же случае происходит регистрация события подозрения на фрод, пользователь попадает в очередь проверки экспертом (администратором системы).

В настоящее время к ядрам классификации принято причислять алгоритмы машинного обучения: нейронные сети, логистическую регрессию, метод опорных векторов, систему графов, позволяющих проводить анализ на базе статистических правил, направленных на выявление уже известных случаев мошенничества, поведенческих профилей клиентов, сотрудников банка, счетов и операций, позволяющих идентифицировать неизвестные ранее мошеннические сценарии, а также применять расширенные аналитические методы (кластерный и регрессионный анализ, метод нечеткой логики, нейронные сети, прогнозное моделирование), которые служат для выявления сложных кросс-канальных сценариев мошенничества.

При всех очевидных достоинствах данный метод имеет ряд существенных недостатков, главным из которых является – негибкость к изменениям. Действительно, такой подход позволяет, имея обучающую выборку, настроить модель и использовать ее на новых данных для последующей классификации транзакций. Однако добавление нового параметра может привести к потере точности процесса определения степени надежности операции, т.е. к возникновению ложной корреляции. Выходом из ситуации служит обеспечение непрерывности процесса обучения модели, что требует дополнительных временных и человеческих ресурсов.

Список использованных источников

1. Программа «Цифровая экономика Российской Федерации»: Распоряжение Правительства Российской Федерации от 28.07.2017 № 1632-р.

2. Развитие Цифровой экономики в России. Программа до 2035 года. – [Электронный ресурс]. Режим доступа: http://innclub.info/wp-content/uploads/2017/05/strategy.pdf.

3. ФинЦЕРТ. Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере. [Электронный ресурс]. Режим доступа: https://www.cbr.ru/information_security/fincert/