УДК 05.13.00
DOI 10.52575/2687-0932-2024-51-4-919-925

Разработка и внедрение систем для борьбы с мошенничеством в финансовых транзакциях

Васильев Т.И.
Paybis LTD, Глазго, Шотландия, 1 Вест-Реджент-стрит, д. 1
E-mail: timurvasilev@gmail.com

Аннотация. В современном мире онлайн-транзакции являются неотъемлемой частью жизни большинства людей, поэтому финансовое мошенничество становится серьёзной угрозой для компаний, которые занимаются онлайн-платежами. Ежегодно потери от мошенничества только увеличиваются и достигают миллиардов долларов, при этом мошенники постоянно совершенствуют свои методы. В данной статье освещаются ключевые проблемы, с которыми могут столкнуться компании при борьбе с разными методами мошенничества, такими как фишинг, кража личных данных, инсайдерские атаки, метод фальшивых заказов или возврата средств. Также подробно рассматриваются эффективные способы создания антифрод-систем, с помощью которых осуществляется защита финансовых транзакций и снижение рисков. Особое внимание уделено использованию современных технологий, таких как искусственный интеллект, аналитика больших данных и блокчейн. С помощью данных технологий осуществляется поиск аномальных активностей при анализе данных в реальном времени и предпринимаются действия по борьбе с мошенническими операциями. Важной частью антифрод-систем является сбор и обработка данных, мониторинг операций и транзакций, а также создание инструментов отчётности и реагирования на подозрительные операции. Кроме технических вопросов, в статье произведён акцент на необходимости обеспечения масштабируемости и безопасности антифрод-систем. Под этим подразумевается защита данных с использованием современных протоколов шифрования и нормативных требований по безопасности. Данная статья предлагает пошаговое руководство по созданию, внедрению в проект систем для борьбы с мошенничеством, которое будет полезно как для крупных компаний, так и для малого и среднего бизнеса.

Ключевые слова: финансовое мошенничество, онлайн транзакции, защита данных, антифрод-системы, машинное обучение, фишинг-атаки, кража данных, блокчейн технологии

Для цитирования: Васильев Т.И. 2024. Разработка и внедрение систем для борьбы с мошенничеством в финансовых транзакциях. Экономика. Информатика, 51(4): 919–925. DOI 10.52575/2687-0932-2024-51-4-919-925

Development and Implementation of Systems to Combat Fraud in Financial Transactions

Timur I. Vasilev
Paybis LTD, 1 West Regent St, Glasgow, Scotland
E-mail: timurvasilev@gmail.com

Abstract. In today's world, online transactions are an integral part of most people's lives, making financial fraud a serious threat to companies that deal with online payments. Each year, losses from fraud continue to grow, reaching billions of dollars, as fraudsters constantly refine their methods. This article highlights key challenges that companies may face when combating fraud, such as phishing, identity theft, or insider attacks, as well as fraudulent schemes involving fake orders or chargebacks. It also provides an in-depth look at effective ways to build anti-fraud systems that protect financial transactions and reduce risks. Special attention is given to the use of modern technologies such as artificial intelligence, big data analytics, and blockchain. These technologies help identify anomalous activities through real-time data analysis and take action to fight fraudulent transactions. A crucial part of anti-fraud systems is data collection and

processing, transaction monitoring, and the creation of tools for reporting and responding to suspicious activities. In addition to technical matters, the article emphasizes the need to ensure the scalability and security of anti-fraud systems. This includes protecting data using modern encryption protocols and complying with security regulations. This article provides a step-by-step guide for implementing anti-fraud systems into a project, which will be useful for both large companies and small to medium-sized businesses.

Keywords: financial fraud, online transactions, data protection, anti-fraud systems, machine learning, phishing attacks, data theft, blockchain technologies

For citation: Vasilev T.I. 2024. Development and Implementation of Systems to Combat Fraud in Financial Transactions. Economics. Information technologies, 51(4): 919–925 (in Russian). DOI 10.52575/2687-0932-2024-51-4-919-925

Введение

Жизнь в современном мире подразумевает постоянное взаимодействие с онлайн-приложениями, мы ежедневно осуществляем множество покупок онлайн. С каждым годом количество онлайн-операций только возрастает, что существенно увеличивает риски, которые связаны с финансовыми мошенничествами. Мошенничество в онлайн-платежах стало одной из главных сложностей для компаний, которые работают в сфере финансовых услуг. Потери средств от мошенничества могут исчисляться в миллиардах долларов, и с каждым годом способы мошенников становятся все более сложными. В данной статье мы рассмотрим основные проблемы и их решения при создании и внедрении средств для борьбы с финансовым мошенничеством, которые помогут компаниям защитить свои операции с деньгами и снизить риски потери средств.

Основная часть

Для построения успешной антифрод-системы необходимо понимание основных мошеннических схем и угроз. Мошенничество может принимать множество форм, каждая из которых может нести серьёзные угрозы для бизнеса [Michael, 2014; Rodney, 2014]. Каждая компания должна понимать риски и возможные угрозы и заранее подготовить свои системы для борьбы с ними. Далее в статье разберём наиболее распространённые виды онлайн-мошенничества [Mitnick, Simon, 2002; Hunnifor, 2020].

Один из самых распространённых способов обмана – это фишинг, в данном способе мошенничества злоумышленник создаёт поддельные веб-сайты, письма или сообщения, которые имитируют реальные веб-приложения. Таким образом, пользователь, не подозревая подмены, вводит свои данные (это могут быть как логин и пароль, так и данные карты) в ненастоящем приложении. Впоследствии полученные данные будут использованы для кражи денег юзера. В качестве примера можно привести отправку электронных писем от имени известного банка с просьбой подтвердить учётные данные или транзакцию. Жертвы переходят по ссылке и вводят свои данные.

Следующим способом мошенничества является мошенничество с помощью карт, злоумышленник крадёт данные карты и далее использует их без разрешения владельца. Мошенники могут украсть информацию с помощью фишинга или установки скимминговых устройств на банкоматах, а также данные карт могут быть украдены вследствие несоблюдения PSI DSS или уязвимости в системах безопасности веб-приложений. Например, в одном известном магазине произошла утечка данных миллионов кредитных карт пользователей из-за уязвимости в платёжной системе. Данные впоследствии продали на чёрном рынке и были использованы в мошенничестве.

Инсайдерские атаки могут стать причиной большой потери средств компании. Это действия сотрудников или партнёров компании, которые имеют доступ к той или иной конфиденциальной информации и используют её в корыстных целях. Данный тип атаки сложно выявить, так как мошенниками являются сами сотрудники компании. Например,

сотрудник компании имеет доступ к базе данных, инициирует платёж и прямым доступом к базе данных меняет сумму на меньшую.

Также существует мошенничество в электронной коммерции, с помощью него осуществляются фальшивые заказы, использование украденных карт и мошенничество с возвратами. Преступники могут покупать товары с помощью украденных карт и далее требовать возврат средств.

Антифрод-системы используются для защиты от мошенничества и выявления аномалий и впоследствии предотвращения финансовых потерь. Они используют различные методы и технологии для анализа транзакций или данных платежей для обнаружения подозрительных действий или данных. Для корректной работы любой антифрод-системы есть методологии разработки, которые включают в себя несколько аспектов.

Первый аспект – это сбор данных, необходимых для работы с источниками, такими как транзакции, действия пользователей, устройства, данные, отправленные и полученные от платёжных систем, а также логирование важных событий и транзакций, с помощью которых система сможет провести последующий анализ.

Следующим этапом является анализ данных. Антифрод-система должна проверять собранные данные на аномалии или по заранее определённым правилам, например, ограничение на количество транзакций в час или день. Также проверять на известные мошеннические схемы или действия лиц, которым запрещены те или иные операции в интернете. Более сложные системы используют машинное обучение для анализа и выявления аномалий, которые могут указывать на мошенничество.

Впоследствии обнаружения сомнительных действий пользователя антифрод-система должна предпринять необходимые меры, например, оповещение разработчиков приложения или администраторов, чтобы человек мог принять адекватное ситуации решение. Также система может автоматически блокировать подозрительные операции или требовать дополнительной аутентификации, самым распространённым случаем является перевод операции в статус необходимой проверки и ожидания действия администратора системы.

Для корректной работы системы необходимо качественное построение инструментов отчётности и мониторинга. Антифрод-система должна генерировать отчёты о деятельности и подозрительных транзакциях, а также успешных попытках мошенничества для последующего улучшения системы. С помощью мониторинга появится возможность отслеживать эффективность системы в режиме реального времени.

Современные антифрод-системы строятся на основе передовых технологий, таких как искусственный интеллект, аналитика больших данных и блокчейн. Рассмотрим каждую из этих технологий подробнее.

Искусственный интеллект позволяет системам анализировать миллионы или миллиарды транзакций в реальном времени для выявления аномалий. Такие системы обучаются на основе исторических данных и с помощью постоянного обучения позволяют постоянно адаптироваться к новым схемам обмана [Murphy, 2012].

Финансовые системы ежеминутно генерируют большие объёмы данных, которые можно использовать для выявления подозрительных действий. Системы Big Data могут анализировать поведение клиентов и выявлять подозрительные действия и прогнозировать риски.

С помощью блокчейна системы обеспечивают прозрачность и неизменность данных, что делает их перспективным решениям для борьбы с мошенничеством. Блокчейн используется для регистрации транзакций, которые невозможно изменить или подделать, что значительно повышает безопасность.

Процесс создания антифрод-системы включает в себя тщательный анализ, проектирование, разработку и тестирование на всех этапах. Необходимо учитывать уникальные угрозы того или иного приложения и опираться на них при проектировании качественной системы. Это требует детализированного анализа исторических данных о мошенничестве и прогнозирования возможных будущих атак.

Ниже будут приведены шаги, которые необходимы для создания эффективной системы.

Первым шагом необходимо определить угрозы приложению, которые могут возникнуть в ходе эксплуатации. Например:

- Фальсификация транзакций. Несанкционированные операции, которые совершаются без владельца счета.
- Кража данных. Получение доступа к конфиденциальной информации пользователей, данным, таким как пароли или финансовые реквизиты.
- Мошенничество через возврат средств. Запросы на возврат средств после получения товаров или услуг.
- Мошенничество с идентификацией. Использование украденных иди поддельных документов для получения кредитов или иных операций.
- Отмывание денег. Использование операций для легализации средств, которые были получены незаконным путём.

После определения типов возможного мошенничества необходимо разработать сценарии их осуществления:

- Моделирование атак. Необходимо продумать возможные попытки мошенника по обходу существующих мер безопасности. Например, каким образом он может получить доступ к учётным записям или фальсифицировать операции.
- Уязвимости систем. Определите слабые места в системе, которые могут быть использованы мошенниками.
- Исторические данные. Проведите анализ уже произошедших мошеннических инцидентов в компании или сфере деятельности.

Следующим шагом построения системы борьбы с мошенничеством является оценка рисков. Необходимо определить вероятность возникновения каждого типа мошенничества, это можно оценить на основании статистических данных или экспертных оценок. Также необходимо определить степень воздействия на бизнес в случае успешного мошеннического действия, это включает как финансовые потери, так и ущерб репутации с последующими юридическими издержками. Необходимо создать таблицу классификации рисков по степени вероятности и серьёзности последствий, таким образом можно визуализировать критичные угрозы.

Далее необходимо проработать функциональные требования системы. Главным требованием к системе является анализ транзакций или платежей, антифрод-система должна уметь собирать данные о платежах и пользователях, их совершающих, в реальном времени, такие как сумма, информация о клиенте, географическое расположение, время и так далее. Также обязана анализировать собранные данные с помощью алгоритмов выявления аномалий и сравнивания текущих данных с историческими и обрабатывать большой объём данных без задержки и отказов системы, чтобы своевременно выявлять подозрительные операции.

Также система должна предоставлять понятный интерфейс для операторов и аналитиков, с помощью которого не возникнет проблем для быстрого реагирования на инциденты. Предоставлять настраиваемые отчёты и дашборды, которые отображают основные метрики и инциденты, и своевременно оповещать операторов или администраторов в режиме реального времени о случившихся инцидентах или подозрительных операциях через различные способы, такие как SMS, email, push-уведомления или сообщения в мессенджеры, например, telegram.

Помимо функциональных требований необходимо проработать нефункциональные требования, чаще всего их список выглядит следующим образом. Одним из самых важных моментов построения системы борьбы с мошенничеством является производительность. Система должна обрабатывать требуемое количество операций в секунду без потери скорости или качества анализа. Обеспечить низкую задержку при обработке данных для предотвращения мошенничества до завершения платежа.

Система должна иметь возможность горизонтально масштабироваться с помощью добавления дополнительных серверов и ресурсов для обработки увеличивающихся данных. Стоит рассмотреть использование облачных технологий и платформ для гибкого масштабирования и распределения нагрузки, например, AWS или Google Cloud.

Немаловажным пунктом является безопасность разрабатываемой системы. Необходимо шифровать данные при передаче и хранении, используя современные протоколы и стандарты (TLS, AES). А также следовать стандартам безопасности в зависимости от юрисдикции и отраслевых требований (PSI DSS, GDPR, ISO 27001) [Что такое PCI DSS и как происходит проверка на соответствие стандарту?].

При построении антифрод-системы самым проблемным местом может стать хранение обрабатываемых или исторических данных. В случае использования реляционных баз данных, например, PostgreSQL или MySQL, вы сможете структурировать данные и обеспечить надёжность транзакций с помощью ACID, но при росте нагрузок реляционные базы данных могут добавить массу сложностей как при добавлении данных, так и при получении, иногда простейший запрос без индекса может увеличить значительно нагрузку на базу данных и на всю систему в целом, как итог система перестанет быть отказоустойчивой. Чаще всего при построении такого рода систем используются NoSQL базы данных, с помощью них достаточно просто хранить большой объём неструктурированных данных и обеспечить высокую производительность и масштабируемость, в качестве примера можно привести MongoDB, Cassandra или DynamoDB. Для быстрого доступа к часто используемым данным стоит использовать системы кеширования, например, Redis или Memcached.

Для построения собственной платформы на основе машинного обучения можно использовать существующие фреймворки и инструменты:

- TensorFlow: Популярный фреймворк от Google для создания и обучения моделей глубокого обучения.
- PyTorch: Гибкий инструмент для исследований и разработки моделей машинного обучения.
- Scikit-learn: Библиотека для классического машинного обучения с большим количеством алгоритмов и инструментов.
- H2O.ai: Для автоматизации процесса обучения моделей и поиска оптимальных параметров.
- Tableau, Power BI: Для создания интерактивных дашбордов и отчетов.

После выбора подходящих инструментов, которые помогут в построении вашей системы, необходимо разработать ее архитектуру, лучше разделить систему на независимые компоненты:

- Сбор данных. Модуль, с помощью которого приложение будет собирать и хранить данные для обработки, а также исторические данные для обучения AI или машинного обучения.
- Анализ данных. С помощью данного модуля будет осуществлена обработка и анализ данных с помощью моделей машинного обучения или AI [Goodfellow, Bengio, Courville, 2016; Anderson R. 2020].
- Реагирование на аномалии. Данный модуль будет отвечать за оповещение или блокировку операций, а также за взаимодействие с администратором или оператором.
- Отчетность и визуализация данных. Инструмент для мониторинга работы системы и представления данных для операторов.

После успешной реализации антифрод-системы наступает этап её тестирования. Необходимо покрыть с помощью функционального тестирования все сценарии системы и проведение нагрузочного тестирования, в ходе которого будет возможно провести оценку производительности с учётом вероятного количества операций и имитации пиковых нагрузок. Также необходимо провести замеры на время отклика, потребление ресурсов и стабильность. Для нагрузочного тестирования можно использовать инструменты, например, JMeter, LoadRunner или Яндекс.Танк.

Последующим этапом становится развёртывание системы, для этого необходимо разработать детальный план и этапы внедрения, работу системы стоит начать с ограниченного внедрения на небольшом сегменте пользователей или операций.

В мире множество примеров успешного внедрения антифрод-систем, множество крупных компаний могут позволить себе построение собственных систем для минимизации рисков и зависимости от других компаний, например, в статьях [Запуск умной антифрод-системы: опыт Своего Банка; Банки Кыргызстана внедряют антифрод-системы для борьбы с мошенничеством] есть успешные примеры внедрения. Но для небольших компаний чаще всего стоит задуматься об использовании уже реализованных систем других компаний, распространяемых по платной модели, с помощью которых в достаточно короткие сроки возможно интегрировать антифрод-систему в бизнес. В таком случае компании минимизируют сроки выполнения интеграции и перекладывают большой пласт работы на внешнюю компанию, что позволяет сосредоточиться на других сферах деятельности для увеличения прибыли. В качестве примера можно привести следующие известные антифрод-системы:

- ArkOwl: Инструмент для проверки электронной почты и телефонов в режиме реального времени, помогающий обнаруживать мошенничество на этапе регистрации и транзакций.
- SEON: Платформа для предотвращения мошенничества, предоставляющая инструменты для оценки рисков транзакций и проверки цифровых следов пользователей.
- Feedzai: Платформа для управления рисками в области финансовых преступлений, которая помогает банкам и платежным системам обнаруживать и предотвращать мошенничество. Использует машинное обучение и анализ больших данных.
- Sift: Платформа цифрового доверия и безопасности, которая использует машинное обучение для обнаружения и предотвращения мошенничества. Sift помогает компаниям защититься от различных типов мошеннических действий, включая захват аккаунтов и спам.

Заключение

Разработка и внедрение систем для борьбы с мошенничеством требует тщательного подхода и планирования, необходимо использовать современные технологии и регулярно обновлять систему. Компании, которые внедряют антифрод-системы, могут значительно снизить риски финансовых потерь и защитить данные клиентов. Важно понимать, что борьба с мошенничеством – это непрерывный процесс, которые требуют постоянного внимания и адаптации к новым угрозам.

Список литературы

Банки Кыргызстана внедряют антифрод-системы для борьбы с мошенничеством. URL: https://economist.kg/novosti-kompanii/2024/04/09/banki-kyrghyzstana-vniedriaiut-antifrod-sistiemy-dlia-borby-s-moshiennichiestvom/

Запуск умной антифрод-системы: опыт Своего Банка. URL: https://companies.rbc.ru/news/qcDHrgo7p1/zapusk-umnoj-antifrod-sistemyi-opyit-svoego-banka/

Что такое PCI DSS и как происходит проверка на соответствие стандарту? URL: https://habr.com/ru/companies/payonline/articles/303330/

Anderson R. 2020. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley. 497-527.

Goodfellow I., Bengio Y., Courville A. 2016. Deep Learning. MIT Press. 96-161.

Hunnifor G. 2020. The little book of big scams. Metropolitan police. 4-45.

Michael R. 2014. Young. The Big Book of Fraud: A Comprehensive Guide to Preventing and Detecting Financial Fraud. Wiley. 3-19.

Mitnick K.D., Simon W.L. 2002. The Art of Deception: Controlling the Human Element of Security. Wiley. 16-32.

Murphy K.P. 2012. Machine Learning: A Probabilistic Perspective. MIT Press. 35-45.

Rodney T. 2014. Fraud Prevention and Detection. CRC Press. 15-20.

References

Banki Kyrgyzstana vnedryayut antifrod-sistemy dlya bor'by s moshennichestvom [Kyrgyz banks are integrating an anti-fraud system for fighting fraud]. URL: https://economist.kg/novosti-kompanii/2024/04/09/banki-kyrghyzstana-vniedriaiut-antifrod-sistiemy-dlia-borby-s-moshiennichiestvom/

Zapusk umnoj antifrod-sistemy: opyt Svoego Banka [Launching a smart anti-fraud system: the Svoy Bank experience]. URL: https://companies.rbc.ru/news/qcDHrgo7p1/zapusk-umnoj-antifrod-sistemyi-opyit-svoego-banka/

CHto takoe PCI DSS i kak proiskhodit proverka na sootvetstvie standartu? [What is PCI DSS and how does compliance testing take place?]. URL: https://habr.com/ru/companies/payonline/articles/303330/

Anderson R. 2020. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley. 497-527.

Goodfellow I., Bengio Y., Courville A. 2016. Deep Learning. MIT Press. 96-161.

Hunnifor G. 2020. The little book of big scams. Metropolitan police. 4-45.

Michael R. 2014. Young. The Big Book of Fraud: A Comprehensive Guide to Preventing and Detecting Financial Fraud. Wiley. 3-19.

Mitnick K.D., Simon W.L. 2002. The Art of Deception: Controlling the Human Element of Security. Wiley. 16-32.

Murphy K.P. 2012. Machine Learning: A Probabilistic Perspective. MIT Press. 35-45.

Rodney T. 2014. Fraud Prevention and Detection. CRC Press. 15-20.

Конфликт интересов: о потенциальном конфликте интересов не сообщалось.
Conflict of interest: no potential conflict of interest related to this article was reported.

Поступила в редакцию 17.10.2024	Received October 17, 2024
Поступила после рецензирования 01.12.2024	Revised December 01, 2024
Принята к публикации 05.12.2024	Accepted December 05, 2024

ИНФОРМАЦИЯ ОБ АВТОРЕ

Васильев Тимур Игоревич, ведущий разработчик платежных систем, финтех компания Paybis.com, Глазго, Шотландия

INFORMATION ABOUT THE AUTHOR

Timur I. Vasilev, Leading Developer of Payment Systems, Paybis LTD, Glasgow, Scotland