УДК 004.031.43

АНТИФРОД СИСТЕМЫ И АЛГОРИТМЫ ВЫЯВЛЕНИЯ МОШЕННИЧЕСКИХ ОПЕРАЦИЙ

Хандуев Ц.Б.

магистрант,

Национальный исследовательский ядерный университет «МИФИ»,

Москва, Россия

Фазульянов Д.В.

аспирант,

Национальный исследовательский ядерный университет «МИФИ»,

Москва, Россия

Аннотация

В статье рассматриваются антифрод-системы как критически важные программно-аппаратные комплексы для предотвращения мошенничества в финансовой сфере. Описаны основные подходы, включая использование сигнатурного метода, его преимуществ и ограничений. Отмечается необходимость внедрения современных алгоритмов машинного обучения для выявления скрытых корреляций в пользовательском поведении, что позволяет повысить эффективность систем, сократить затраты ресурсов и минимизировать количество ложных срабатываний.

Ключевые слова: антифрод-системы, мошенничество, финансовая безопасность, сигнатурные правила, машинное обучение

ANTIFRAUD SYSTEMS AND ALGORITHMS FOR DETECTING FRAUDULENT TRANSACTIONS

Khanduev T.B.

Master's student,

National Research Nuclear University «MEPhI»,

Moscow, Russia

Fazulyanov D.V.

National Research Nuclear University «MEPhI»,

Moscow, Russia

Abstract

The article considers anti-fraud systems as critical hardware and software complexes for fraud prevention in the financial sphere. The main approaches are described, including the use of signature method, its advantages and limitations. The necessity of implementing modern machine learning algorithms to identify hidden correlations in user behavior is noted, which allows to increase the efficiency of systems, reduce resource costs and minimize the number of false positives.

Keywords: antifraud systems, fraud, financial security, signature rules, machine learning

Антифрод-системы представляют собой специализированные программно-аппаратные комплексы, разработанные для предотвращения несанкционированных действий в финансовой сфере. Обычно они включают модули для обнаружения, предотвращения и анализа мошенничества (fraud detection, fraud prevention, fraud analysis), а также элементы интеллектуального обучения (intellectual learning).

Важно отметить, что такие системы являются критически важными (business-critical) для обеспечения непрерывной работы управленческих и технологических процессов. Сбои в их работе могут привести к остановке бизнес-процессов, а некорректная работа — к повышению финансовых рисков для компании.

Ключевые качества, которые учитываются при проектировании антифрод-систем, включают:

- распределенность;

- безопасность хранения данных;
- надежность;
- высокую масштабируемость.
- отказоустойчивость;

Кроме того, архитектурная модель подобных систем должна соответствовать законодательству. Стандарт PCI DSS, разработанный для обеспечения безопасности данных владельцев платежных карт, запрещает хранить полный номер карты (PAN) и код безопасности (CVV). Допускается сохранять только первые шесть и последние четыре цифры номера карты. Кроме того, в соответствии с Федеральным законом №152-ФЗ «О персональных данных», передача имени владельца карты и срока ее действия возможна исключительно через защищенные каналы связи. [1]

Системы обнаружении мошенничества, основанные на сигнатурных методах.

Для банковской сферы характерен высокий объем клиентских операций, что может замедлять процесс проверки надежности транзакций и снижать производительность антифрод-систем. Для ускорения этих процессов разработаны алгоритмы автоматического выявления подозрительных операций и меры по защите средств пользователей.

Одним из наиболее распространенных методов, применяемых в современных антифрод-системах, является использование сигнатурного метода выявления мошеннических операций. Сигнатурный метод подразумевает использование антифрод-правил, которые представляют собой простые шаблоны, описывающие известные виды мошеннической активности. Их применяют для выявления таких действий, как использование украденных кредитных карт, создание ботов для массовых операций или попытки взлома аккаунтов.

Сигнатурный метод, работает за счет активации триггеров, настроенных экспертами. Примеры распространенных триггеров включают слишком крупные

или частые транзакции, операции в необычных геолокациях и другие случаи, которые требуют дополнительной проверки. Для обнаружения мошенничества часто используется комбинация нескольких таких правил. В среднем современная антифрод-система включает около 500 антифрод-правил.

Однако у данного подхода есть ограничения: необходимость постоянного обновления существующих правил, создание новых для защиты от актуальных угроз, а также невозможность выявления скрытых корреляций. Нередко такие системы используют упрощенное программное и аппаратное обеспечение, которое не способно эффективно обрабатывать большие объемы данных в режиме реального времени.

Схема работы антифрод-системы на основе сигнатурного метода показана на рис. 1.

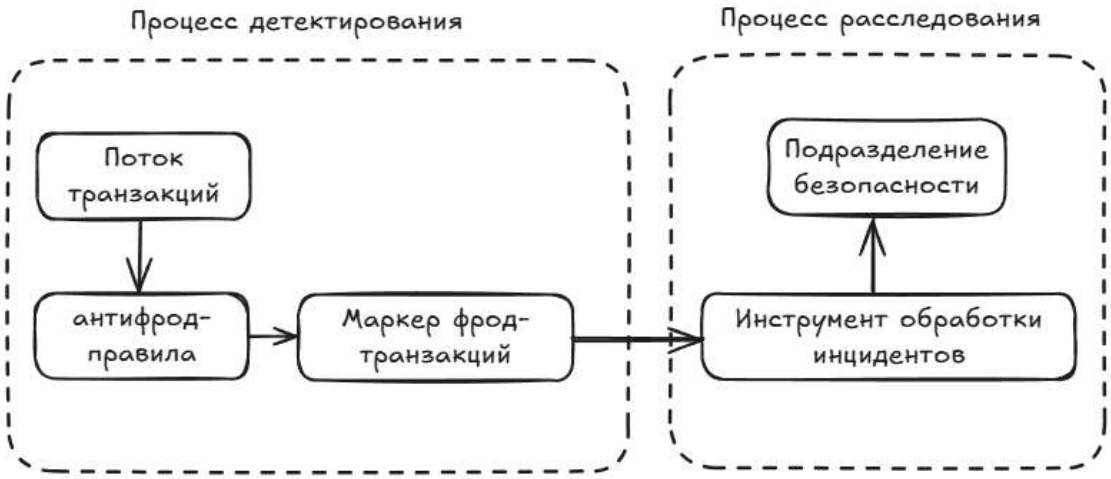

Рис.1 – Процесс работы антифрод-системы, базирующейся на сигнатурном методе. [составлено авторами]

Системы обнаружении мошенничества, основанные на машинном обучении.

Антифрод-правила сигнатурного метода хорошо справляются с обнаружением очевидных случаев мошенничества, однако в поведении пользователей могут проявляться скрытые признаки, указывающие на возможный фрод. Для их выявления используются алгоритмы машинного

обучения, которые способны обнаруживать скрытые взаимосвязи между действиями пользователей и риском мошенничества. Это помогает уменьшить вероятность пропуска угроз и сократить количество ложных срабатываний. Процесс работы антифрод-системы, основанной на машинном обучении, представлен на рис. 2.

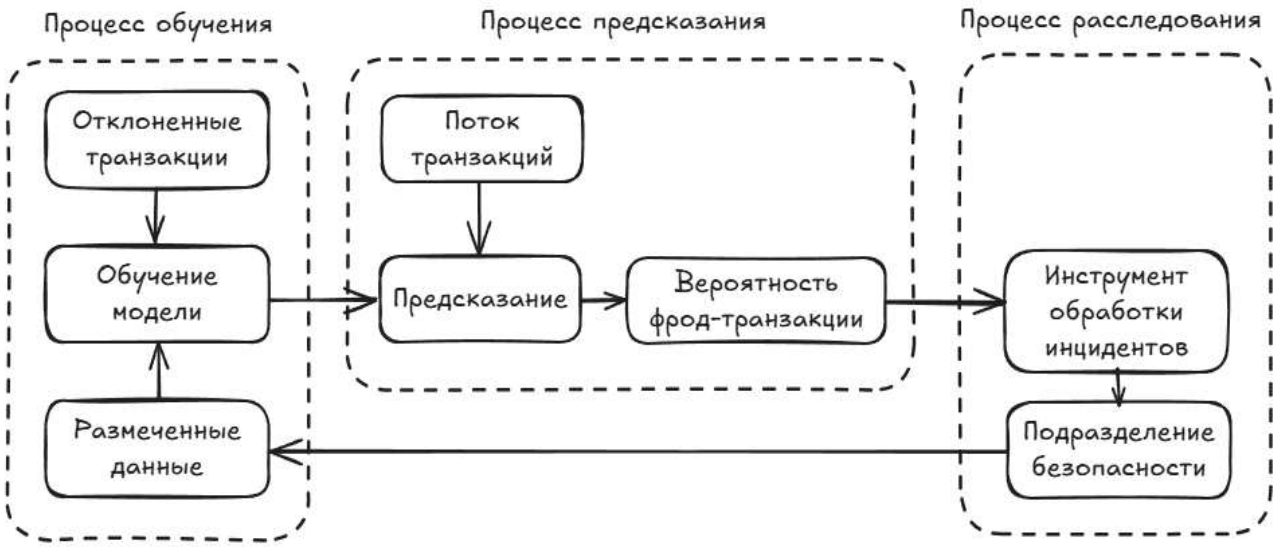

Рис.2 – Процесс работы антифрод-системы, основанной на машинном обучении. [составлено авторами]

Антифрод-системы на базе машинного обучения оснащены передовыми инструментами для обработки и анализа данных, что значительно уменьшает затраты времени и ресурсов на выявление мошенничества.

Сложность выявления мошеннической активности и ограниченная эффективность сигнатурного подхода свидетельствуют о необходимости внедрения новых методов. Сегодня машинное обучение признано одним из самых эффективных методов создания современных антифрод-систем.

Таблица 1 содержит сравнительный анализ основных алгоритмов, применяемых в современных антифрод-системах. Оценка проводилась по частоте использования и ранее описанным критериям, где 1 означает «низкий», 2 — «средний», 3 — «высокий».

Таблица 1. Сравнительный обзор алгоритмов, применяемых в антифрод-системах. [4]

Алгоритм	Тип алгоритма	Частота использования	Точность	Покрытие	Стоимость
Artificial Neural Network (ANN)	С учителем	40%	2	2	3
Decision Tree (DT)	С учителем	38%	2	2	3
Support Vector Machine (SVM)	С учителем	34%	3	3	3
Genetic algorithm (GA)	Без учителя	26%	2	2	1
K-nearest Neighbors (KNN)	Без учителя	20%	2	2	3
Bayesian Network (BN)	С учителем	16%	3	2	3
Hidden Markov Model (HMM)	Без учителя	16%	1	1	3
Logistic Regression (LR)	С учителем	16%	3	2	2
Random Forest (RF)	С учителем	16%	3	2	2
Fuzzy Logic Based system (FL)	С учителем	8%	3	2	3

Из сравнительного анализа следует, что наиболее эффективным и дорогостоящим алгоритмом по обнаружению мошеннических действий является SVM. Тем не менее, зачастую в антифрод-системах используется несколько алгоритмов, взаимно дополняющих друг друга. Такой подход необходим для оптимизации оценки и достижения более высокой точности. [4]

Заключение

Выявление мошенничества требует комплексного подхода, включающего анализ данных, выбор технологий и инструментов для детектирования. Хотя машинное обучение решает большинство задач антифрод-систем, оно требует больших объемов качественно размеченных данных, подходящего стека и экспертов, что затрудняет его использование малыми организациями. Для них

предпочтительны системы на основе сигнатурного метода, эффективного при формализованных типах угроз.

Крупным компаниям, сталкивающимся с динамичными угрозами и большим потоком операций, сложно поддерживать антифрод-правила. С увеличением объема данных и скорости их обработки такие правила теряют свою актуальность. В таких условиях самообучающиеся модели становятся оптимальным решением, адаптируясь к изменениям и новым рискам.

Библиографический список

1. О персональных данных: федеральный закон от 27 июля 2006 г. N 152-ФЗ // Собрание законодательства Российской Федерации. — 2006. — № 31 (часть I). — Ст. 3451.

2. Развитие Цифровой экономики в России. Программа до 2035 года. – [Электронный ресурс]. URL: http://innclub.info/wpcontent/uploads/2017/05/strategy.pdf. (Дата обращения: 15.12.2023)

3. ФинЦЕРТ. Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере. [Электронный ресурс]. URL: https://www.cbr.ru/information_security/fincert/ (Дата обращения: 02.12.2024)

4. An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection [Электронный ресурс]. URL: https://www.researchgate.net/publication/332268831_An_Analysis_of_the_Most_Used_Machine_Learning_Algorithms_for_Online_Fraud_Detection (Дата обращения: 01.12.2024)

5. Comparative Analysis of Machine Learning Techniques for Detecting Insurance Claims Fraud. [Электронный ресурс]. URL: https://www.wipro.com/analytics/comparative-analysis-of-machine-learning-techniques-for-detectin/ (Дата обращения: 25.11.2024)

6. Deep feature representation for anti-fraud system. [Электронный ресурс]. URL: https://www.sciencedirect.com/science/article/abs/pii/S1047320319300409 (Дата обращения: 15.12.2024)

Оригинальность 77%