Карташов Павел Григорьевич,
Студент магистратуры,
Поволжский государственный университет
телекоммуникации и информатики, г. Самара

ОБНАРУЖЕНИЕ МОШЕННИЧЕСТВА В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ: ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ АНАЛИЗА БАНКОВСКИХ ТРАНЗАКЦИЙ

Аннотация: В условиях роста электронных платежей крайне важно выявлять мошеннические банковские транзакции в реальном времени. Нейронные сети, особенно при правильной предобработке данных и оценке, демонстрируют высокую точность в обнаружении мошеннических операций, повышая безопасность и надежность банковских транзакций.

Ключевые слова: мошенничество, банковские транзакции, нейронные сети, машинное обучение, обнаружение мошенничества, режим реального времени.

Введение

Бурный рост объемов электронных платежей и онлайн-банкинга привел к значительному увеличению риска мошеннических операций. Традиционные методы обнаружения мошенничества, основанные на статистическом анализе и экспертных правилах, зачастую оказываются неэффективными в условиях динамично меняющихся стратегий мошенников [2]. В связи с этим, актуальной задачей является разработка и внедрение систем обнаружения мошенничества в режиме реального времени, способных оперативно выявлять подозрительные транзакции и предотвращать финансовые потери.

В последние годы нейронные сети зарекомендовали себя как мощный инструмент для решения задач классификации и прогнозирования в различных областях, в том числе и в сфере обнаружения мошенничества [6, 7]. Способность нейросетей к обучению на основе данных и выявлению сложных закономерностей позволяет им эффективно обнаруживать мошеннические операции, даже в условиях неполной или зашумленной информации [8].

Методы и материалы

Для исследования возможности применения нейронных сетей для обнаружения мошенничества в режиме реального времени были рассмотрены следующие архитектуры:

- Многослойный персептрон (MLP): Классическая архитектура нейронной сети, хорошо зарекомендовавшая себя в задачах классификации [6].
- Рекуррентные нейронные сети (RNN): Подходят для анализа последовательностей данных, таких как история транзакций пользователя [2].
- Автокодировщики (Autoencoders): Используются для выявления аномалий в данных путем обучения на нормальных транзакциях и выявления отклонений от этой нормы [5].
- Сверточные нейронные сети (CNN): Могут применяться для анализа признаков транзакций, представленных в виде матрицы [8].

В качестве данных для обучения и тестирования моделей использовался синтетический набор данных, сгенерированный на основе реальных данных о банковских транзакциях, а также общедоступные наборы данных [1]. Для предобработки данных применялись методы нормализации, масштабирования и обработки пропущенных значений [7]. Оценка эффективности моделей проводилась на основе метрик точности, полноты, F1-меры и AUC-ROC [3].

Результаты

Результаты исследования показали, что нейронные сети позволяют достичь высокой точности обнаружения мошеннических операций в режиме реального времени. Наилучшие результаты были получены при использовании рекуррентных нейронных сетей, что связано с их способностью учитывать последовательный характер транзакций [4]. Также было установлено, что предобработка данных и правильный выбор архитектуры нейронной сети играют важную роль в достижении высокой эффективности [5].

Обсуждение

Применение нейронных сетей для обнаружения мошенничества в режиме реального времени имеет ряд преимуществ по сравнению с традиционными методами:

Высокая точность: Нейронные сети способны выявлять сложные закономерности и обнаруживать мошеннические операции, которые не могут быть обнаружены с помощью статистического анализа или экспертных правил [2, 7].

Адаптивность: Нейронные сети могут автоматически адаптироваться к меняющимся стратегиям мошенников путем переобучения на новых данных [6].

Обработка больших объемов данных: Нейронные сети способны эффективно обрабатывать большие объемы данных в режиме реального времени [7].

Однако, внедрение нейросетевых моделей для обнаружения мошенничества требует решения ряда задач:

- Выбор архитектуры нейронной сети: Необходимо выбрать архитектуру нейронной сети, наиболее подходящую для конкретной задачи [6].
- Сбор и предобработка данных: Необходимо собрать и предобработать данные, необходимые для обучения нейронной сети [5].
- Обучение и настройка параметров: Необходимо обучить нейронную сеть и настроить ее параметры для достижения высокой эффективности [8].
- Интеграция в банковскую инфраструктуру: Необходимо интегрировать нейросетевую модель в банковскую инфраструктуру и обеспечить ее работу в режиме реального времени [4].
- Объяснимость моделей: Необходимо разрабатывать методы, позволяющие понимать и интерпретировать решения нейросетевых моделей, для повышения доверия к системе и облегчения аудита [3].

Заключение

Использование нейронных сетей является перспективным направлением для разработки систем обнаружения мошенничества в банковских транзакциях в режиме реального времени. Разработка и внедрение таких систем позволит значительно повысить безопасность и надежность банковских транзакций, предотвратить финансовые потери и повысить доверие клиентов к банковской системе.

Список литературы:

1. Fraud Detection Dataset, Kaggle. https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud (дата обращения: 26.10.2023).

2. Бернштейн, А. С., & Ильин, Д. А. (2018). Обнаружение мошеннических транзакций в банковской сфере с использованием методов машинного обучения., Труды СПИИРАН6 (61), 129-142.

3. Гусев, А. В., & Петров, В. В. (2020). Применение нейронных сетей для обнаружения мошеннических операций в банковских транзакциях., Информационные технологии26 (2), 112-118.

4. Левин, Д. А., & Смирнов, П. И. (2021). Анализ методов машинного обучения для обнаружения мошенничества в банковских транзакциях., Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления17 (3), 354-367.

5. Хорошкин, В.В. (2022). Обнаружение мошеннических транзакций в системах электронных платежей на основе машинного обучения., Автоматизация в промышленности1, 25-29.

6. Aggarwal, C. C. (2013).. Springer Science & Business Media.Outlier Analysis

7. Goodfellow, I., Bengio, Y., & Courville, A. (2016).. MIT Press.Deep Learning

8. Bishop, C. M. (2006).. Springer.Pattern Recognition and Machine Learning