ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В БОРЬБЕ С МОШЕННИЧЕСТВОМ: ПРИМЕНЕНИЕ, АЛГОРИТМЫ И ПРЕИМУЩЕСТВА

Iana ZABOLOTNII*, Irina CERNEI

Departamentul Ingineria Software și Automatică; Facultatea Calculatoare, Informatică și Microelectronică; Universitatea Tehnică a Moldovei; Chișinău; Republica Moldova

*Автор-корреспондент: Iana Zabolotnii, zabolotnii.iana@isa.utm.md

Научный руководитель: **Irina CERNEI**, assistent universitar, UTM

Аннотация. *В данной статье представлен анализ феномена мошенничества в рамках различных аспектов предоставления финансовых услуг, в том числе банковской деятельности, страхования и проведения онлайн-платежей. Исследование детализирует специфику мошеннических операций в каждой из указанных областей, выявляя характерные приемы и стратегии, используемые преступниками для незаконного получения финансовых средств. Также акцентируется внимание на методах и технологиях, которые могут помочь в борьбе с мошенническими действиями и применяются для обеспечения надежности проведения финансовых операций.*
Статья также подробно рассматривает роль искусственного интеллекта в выявлении и предотвращении мошенничества. Описывается, как технологии машинного обучения применяются для анализа больших объемов данных и выявления аномальных или подозрительных паттернов, которые могут указывать на мошенническую деятельность. Приводятся примеры алгоритмов и методов, используемых в системах искусственного интеллекта для борьбы с мошенничеством.
Заключительная часть статьи посвящена оценке преимуществ и вызовов, связанных с интеграцией искусственного интеллекта в процессы выявления и противодействия мошенничеству. Акцентируется внимание на важности повышения эффективности и точности детектирования мошеннических схем за счет использования ИИ, а также на необходимость регулярного обновления и адаптации алгоритмов к эволюционирующим методам мошенничества.

Ключевые слова: *искусственный интеллект, машинное обучение, алгоритмы, финансы, обнаружение мошенничества, онлайн платежи*

Введение

В современном мире мошенничество неизменно остается актуальной и серьезной проблемой, затрагивающей множество сфер деятельности, включая банковские операции, страхование, онлайн-платежи и многие другие. Ежегодно миллионы людей становятся жертвами различных видов мошенничества, сталкиваясь с финансовыми потерями и разрушением доверия к существующим системам. Однако, вместе с вызовами, появляются и новые возможности, и в этом контексте особенно значимо становится использование искусственного интеллекта (ИИ) в борьбе против мошенничества.

С каждым днем ИИ становится все более интегральной частью нашей повседневной жизни, проникая в различные сферы деятельности и предоставляя новые инструменты для эффективного решения сложных проблем. В контексте противодействия мошенничеству, применение искусственного интеллекта открывает двери к широкому спектру инновационных подходов и технологий. Это включает в себя анализ больших данных для выявления аномалий и паттернов, создание алгоритмов машинного обучения для предсказания и предотвращения потенциальных мошеннических действий, а также разработку более интеллектуальных систем обнаружения и защиты [1].

Виды мошенничества

Мошенничество охватывает различные сферы человеческой деятельности, причиняя значительный ущерб как физическим, так и юридическим лицам. Среди наиболее распространенных видов мошенничества можно выделить банковские операции, онлайн-платежи, а также страхование.

Банковские операции — это одно из наиболее уязвимых мест для мошенников, где они могут осуществлять различные виды атак, включая кражу личных данных, фишинг, фальшивые транзакции и другие. Они используют различные методы, чтобы обмануть системы безопасности банков и получить доступ к финансовым средствам клиентов.

Онлайн-платежи также подвержены риску мошенничества из-за широкого использования электронных транзакций. Мошенники могут использовать украденные кредитные карты, взламывать аккаунты и обманывать пользователей с помощью фальшивых веб-сайтов и электронных платежных систем.

Страхование - еще одна сфера, где мошенничество встречается довольно часто. Это может включать в себя подачу ложных заявлений на страховые случаи, утверждение неправдивых сведений о страховых рисках или даже фальсификацию документов для получения неправомерных выплат [2].

Традиционные методы обнаружения мошенничества

Традиционные системы обнаружения мошенничества обычно основаны на правилах, которые задаются заранее. Эти правила включают в себя совокупность критериев, по которым проводится анализ транзакций и определяются подозрительные действия. Например, если сумма транзакции превышает определенный порог, или если транзакция происходит из страны или региона с высоким уровнем риска, она может быть отмечена как подозрительная и требующая дополнительной проверки [3].

Эти традиционные методы имеют свои ограничения, в том числе ограниченную способность адаптироваться к новым видам мошенничества и высокий уровень ложных срабатываний. Кроме того, они часто требуют постоянного обновления и настройки правил для поддержания актуальности в изменяющейся среде мошенничества.

Применение машинного обучения для обнаружения мошенничества

Внедрение машинного обучения в системы обнаружения мошенничества играет ключевую роль в современном мире безопасности. Процесс применения этих методов включает ряд этапов:

1. Сбор данных: начальным шагом является собирание информации о реальных транзакциях и возможных случаях мошенничества. Это включает в себя сведения о суммах транзакций, временных метках, географическом расположении операций и другие данные, связанные с мошенничеством. Для этого может использоваться интеграция с базами данных банков, системами мониторинга транзакций, сетевыми журналами и другими источниками данных о пользовательской активности.
2. Подготовка данных: данные очищаются от ошибок, дубликатов и аномалий, таких как неправильные суммы транзакций или некорректные временные метки. Данные преобразуются в удобный формат для анализа и обработки моделями машинного обучения. Это может включать в себя нормализацию числовых значений, кодирование категориальных признаков и выделение признаков, имеющих наибольшее значение для обнаружения мошенничества.
3. Выбор модели: на этом этапе происходит выбор наиболее подходящей модели машинного обучения для обнаружения мошенничества. Рассматриваются различные модели, такие как логистическая регрессия, деревья решений,

случайный лес и нейронные сети, с учетом их способности работать с различными типами данных и способности обнаруживать сложные паттерны мошенничества.

4. Обучение модели: выбранная модель обучается на обучающем наборе данных, чтобы выявить паттерны, характерные для мошеннических транзакций.
5. Тестирование и оценка модели: обученная модель тестируется на тестовом наборе данных для оценки ее производительности на новых, ранее не виденных данных. Метрики производительности модели на тестовом наборе данных позволяют оценить ее способность правильно классифицировать мошеннические и нормальные транзакции.
6. Внедрение и мониторинг: после успешного тестирования модель развертывается в производственной среде для реального обнаружения мошенничества. Устанавливаются механизмы мониторинга, которые следят за производительностью модели и обновляют ее при необходимости [4].

Техники и алгоритмы искусственного интеллекта в борьбе с мошенничеством

Искусственный интеллект (ИИ) играет ключевую роль в разработке эффективных методов обнаружения и предотвращения финансовых преступлений. В этом разделе мы рассмотрим основные техники и алгоритмы ИИ, используемые для борьбы с мошенничеством:

1. Машинное обучение: это область искусственного интеллекта, которая изучает методы анализа данных и построения моделей, позволяющих компьютерам извлекать знания и делать прогнозы на основе этих данных. Оно делится на три основных типа: обучение с учителем, без учителя и с подкреплением, каждый из которых имеет свои специфические методы и задачи. Машинное обучение широко применяется в различных областях, включая финансы, медицину, транспорт и многие другие, улучшая процессы анализа данных и принятия решений.
2. Анализ поведения: это процесс изучения и моделирования поведения объектов или систем на основе данных, с целью выявления закономерностей и прогнозирования будущих действий. Включает в себя методы машинного обучения, обработку сигналов и другие алгоритмы для анализа временных рядов и пространственных данных. Применяется в различных областях, включая финансовый мониторинг, прогнозирование клиентских предпочтений и управление рисками.
3. Нейронные сети: это сети искусственных нейронов, организованные в сложные архитектуры, способные обрабатывать большие объемы данных и выявлять сложные паттерны. Они используются в машинном обучении для решения разнообразных задач, включая классификацию, регрессию, обнаружение аномалий и генерацию контента. Нейронные сети могут обучаться как на основе наблюдаемых данных, так и с использованием методов обучения с подкреплением.
4. Кластеризация и классификация: это два основных подхода в машинном обучении. Кластеризация — это процесс группировки объектов на основе их сходства, без учета заранее известных категорий. Классификация, напротив, предполагает разделение объектов на заранее определенные классы или категории на основе характеристик [5].

Преимущества и вызовы использования искусственного интеллекта

Искусственный интеллект обладает рядом преимуществ при борьбе с мошенничеством, включая:

- Автоматизацию процессов обнаружения, что ускоряет реакцию на потенциальные преступления.
- Высокую точность анализа данных, обнаруживающую даже сложные мошеннические схемы.

- Способность адаптироваться к новым видам мошенничества, минимизируя риски [6].

Однако, внедрение искусственного интеллекта сопровождается вызовами:
- Недостаток данных для обучения моделей, что может снизить их эффективность.
- Постоянная адаптация мошенников к новым методам, требующая постоянного обновления систем ИИ.
- Возможность ложных срабатываний, что может привести к потере доверия к системам безопасности [6].

Заключение

В заключение, использование искусственного интеллекта в противодействии мошенничеству является мощным решением, способным улучшить безопасность финансовых транзакций в различных отраслях. Преимущества такого подхода включают высокую эффективность в обнаружении мошеннических действий с высокой точностью и скоростью, а также способность искусственного интеллекта быстро адаптироваться к новым видам мошенничества. Важно, однако, учитывать вызовы, такие как сложность обучения моделей и необходимость постоянного обновления алгоритмов, для успешной реализации данного подхода.

Использованные источники

[1] S. Qaadan and S. Friesike, “Fraud detection using machine learning”, 2023, doi: 10.13140/RG.2.2.12616.29441.
[2] “Искусственный интеллект в борьбе с мошенничеством.” [Online]. Available: https://nauchniestati.ru/spravka/vyyavlenie-moshennichestva-i-iskusstvennyj-intellekt-bankovskie-operaczii-strahovanie-onlajn-platezhi/
[3] Елена Багреева, Лилия Бобылева, “Искусственный интеллект как противодействие мошенничеству в банковской сфере”, 2022. doi 10.52068/2304-9839_2022_57_2_90.
[4] S. Leili, Fraud Detection in Banking Data by Machine Learning Techniques, 2022.
[5] H. I. Erdal and A. Ekinci, “A Comparison of Various Artificial Intelligence Methods in the Prediction of Bank Failures,” Comput. Econ., vol. 42, no. 2, pp. 199–215, Aug. 2013.
[6] R. Achary, C.Shelke, X. Chen, and R. Zhao, “Fraud Detection in Banking Transactions Using Machine Learning”, 2023, doi: 10.1109/IITCEE57236.2023.10091067.