УДК 004.051

РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ДЛЯ ВЫЯВЛЕНИЯ ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ В БАНКОВСКОМ СЕКТОРЕ

Г.А. Геворгян
ИКБ РТУ МИРЭА
Россия, 107076, Москва, Стромынка ул., 20
E-mail gevorgyan@edu.mirea.ru

П.И. Карасев
ИКБ РТУ МИРЭА
Россия, 107076, Москва, Стромынка ул., 20
E-mail karasev@mirea.ru

Almali Ahmed Adnan Lateef
ТГТУ
392000, Тамбов, ул.Советская, 106
E-mail: AlmaliAhmedAdnan@mail.ru

Al-Ameedee Mustafa Abdulkadhim Dhahir
ТГТУ
392000, Тамбов, ул.Советская, 106
E-mail: AmeedeeMustafa@mail.ru

Ключевые слова: банковский сектор, искусственный интеллект, Треугол, Арбитраж.

Аннотация: В современной эпохе цифровизации и развития технологий информационной безопасности, проблема мошенничества и противоправных действий в банковском секторе приобретает особую актуальность. Распространение различных видов финансовых преступлений требует активного применения новейших инструментов для выявления и предотвращения таких действий. В данной статье предлагается разработка интеллектуальной системы для выявления противоправных действий в банковском секторе, объединяющей в себе методы искусственного интеллекта, анализа данных и машинного обучения.

1. Введение

Банковский сектор является одной из самых важных отраслей экономики, в которой происходит активное использование информационных технологий для обеспечения экономической активности.

Однако, увеличение объемов электронных транзакций и операций также приводит к возрастанию преступной активности в данной сфере.

Мошенничество в банковском секторе, кража личных данных и другие противоправные действия могут нанести серьезный ущерб, как клиентам банков, так и самим финансовым учреждениям.

2. Методы

Блок «Методы» предполагает использование комбинации методов искусственного интеллекта, анализа данных и машинного обучения для разработки интеллектуальной системы, способной выявлять противоправные действия в банковском секторе.

Одним из распространенных видов мошенничества в банковской сфере является треугольниковая схема, также известная как схема «Треугол».

В этой схеме, мошенник устанавливает три основных элемента: потенциальную жертву, оформляет поддельные документы, и создает фиктивные аккаунты или компании. Затем мошенник дает инструкции жертве о том, как перевести деньги на счет фиктивной компании. Мошенник присваивает себе переведенные деньги и исчезает, оставив жертву с потерянными средствами.

Искусственный интеллект может значительно помочь банкам в выявлении и предотвращении подобных случаев мошенничества. Например, с помощью алгоритмов машинного обучения и анализа данных система может проследить и проанализировать связи между различными счетами и транзакциями [1].

Система может оценить рисковые факторы, такие как несоответствия между транзакциями и обычным поведением клиента, большие суммы денег, необычные географические перемещения средств и другие аномалии.

ИИ может также применяться для определения финансовых аномалий, таких как несоответствия в документации, необычная активность на счетах или подозрительные платежи. Анализируя большие объемы данных, система может быстро и точно отслеживать необычные паттерны и сигнализировать о потенциальных случаях мошенничества банку [2].

Кроме того, машинное обучение может использоваться для создания моделей, которые улучшаются с течением времени, анализируя данные о мошеннических схемах и адаптируясь к новым видам мошенничества. Это позволяет системе не только выявлять известные схемы, но и обнаруживать новые методы мошенничества, которые могут быть неизвестны на данный момент.

В целом, использование интеллектуальных систем и алгоритмов анализа данных в банковском секторе позволяет осуществлять более эффективное выявление и предотвращение противоправных действий, что способствует защите интересов как банков, так и их клиентов[3].

3. Арбитраж

Арбитраж криптовалюты – это стратегия, когда трейдеры пытаются получить прибыль от разницы в ценах на различных торговых площадках. Они одновременно покупают криптовалюту на одной бирже по более низкой цене и одновременно продают на другой бирже по более высокой цене. Разница в ценах позволяет трейдерам заработать прибыль.

Искусственный интеллект может быть важным инструментом для банков для контроля и предотвращения использования карт чужих людей для финансовых потоков. С использованием машинного обучения и анализа данных, ИИ может проанализировать множество факторов, чтобы выявить подозрительные транзакции и предупредить о мошеннической деятельности.

Например, ИИ может оценивать необычные паттерны транзакций, такие как большие переводы с использованием разных карт или множественные покупки с использованием разных учетных записей. Он также может анализировать данные о

местоположении, определять, не является ли место, откуда делается транзакция, необычным для данного клиента.

Искусственный интеллект может даже учитывать контекстуальные данные, такие как информация о клиенте, его покупках и поведении в прошлом. Это позволяет системе определить, является ли транзакция типичной для данного клиента или является аномалией.

Другая возможность использования ИИ состоит в создании моделей, которые способны обнаруживать злоумышленников на основе сходства в их поведении. Анализируя и сравнивая множество факторов, таких как типы транзакций, общая сумма расходов и привычки клиентов, система может идентифицировать карты, которые могут быть использованы мошенниками.

Банки могут также использовать технологии биометрической аутентификации, такие как сканирование отпечатков пальцев или распознавание лица, чтобы подтвердить подлинность владельца карты и сравнивать эти данные с предыдущими транзакциями. Это дополнительный уровень защиты от мошенничества и предотвращает использование карт чужих людей.

С учетом всех этих факторов, искусственный интеллект может быть мощным инструментом для банков в борьбе с мошенничеством и предотвращении незаконного использования карт чужих людей для финансовых потоков. Он помогает автоматизировать процессы анализа и обнаружения подозрительных транзакций, что позволяет банкам оперативно реагировать на потенциальные риски и защищать интересы своих клиентов.

4. Подходы выявления схем

Для выявления случаев схем Треугол и Арбитража криптовалюты можно применить несколько подходов, использующих алгоритмы машинного обучения:

1. Кластерный анализ: этот подход основан на группировке данных в подобные кластеры. В случае схемы Треугол можно выделить кластеры, которые содержат транзакции, характерные для такой схемы. Кластерный анализ позволяет обнаружить аномалии в данных и выявить связи между транзакциями.

2. Анализ временных рядов: для выявления схемы Арбитража можно использовать анализ временных рядов курса криптовалют. При этом можно искать ситуации, когда разница в курсах на разных биржах становится достаточно большой для возможности реализации арбитражных сделок. Алгоритмы машинного обучения, такие как авторегрессионные модели или рекуррентные нейронные сети, могут быть использованы для предсказания и анализа временных рядов курса.

3. Анализ сетей: в случае схемы Треугол можно проанализировать транзакции и выявить связи между различными участниками сети криптовалюты. Нейронные сети или алгоритмы обработки графов могут быть применены для выявления необычных паттернов или аномалий в сети.

4. Обработка естественного языка: для выявления подозрительных транзакций и общих черт схемы Арбитража или Треугол можно использовать алгоритмы обработки естественного языка. С помощью таких алгоритмов можно анализировать текстовые описания сделок или комментарии пользователей криптовалютных платформ и выявлять подозрительные или необычные паттерны.

В целом, алгоритмы машинного обучения могут быть эффективным инструментом для выявления схем Треугол и Арбитража криптовалюты. Однако, важно учитывать, что успешность такого анализа зависит от доступности и качества данных, а также от выбора и настройки соответствующих алгоритмов.

Ожидаемые результаты:

Интеллектуальная система для выявления противоправных действий в банковском секторе позволит повысить эффективность раннего выявления и предотвращения противоправных действий.

Система будет способна автоматически анализировать данные и выявлять аномалии в режиме реального времени. Это значительно сократит время реакции и позволит банкам принимать меры по предотвращению ущерба для клиентов и финансовых учреждений.

Заключение

Разработка интеллектуальной системы для выявления противоправных действий в банковском секторе является важным шагом в обеспечении информационной безопасности и защите интересов клиентов финансовых учреждений.

Применение методов искусственного интеллекта и машинного обучения позволяет повысить эффективность работы в условиях постоянно меняющейся ситуации на рынке финансовых услуг. Реализация данной системы поможет минимизировать риски противоправных действий и улучшить уровень безопасности в банковском секторе.

5. Заключение

Имитационное моделирование является мощным инструментом, который может быть использован для визуализации технических средств защиты информации. Оно позволяет решать широкий спектр задач, таких как создание моделей угроз, анализ реакции системы, тестирование стратегий безопасности и визуализация процессов защиты. Использование имитационного моделирования может помочь специалистам повысить эффективность защиты информации и снизить риски возникновения инцидентов информационной безопасности.

Список литературы

1. Распоряжение Правительства Российской Федерации от 17.12.2010 № 2299-р. https://digital.gov.ru/common/ upload/2299p.pdf (дата обращения: 22.11.2023).
2. Об утверждении Методических рекомендация по использованию свободного программного обеспечения в деятельности федеральных органов исполнительной власти, включая критерии определения государственных информационных систем, при создании которых необходимо использовать свободное программное обеспечение, в том числе государственных информационных систем, предназначенных для оказания государственных и муниципальных услуг в электронном виде. Приказ Минкомсвязи России от 19.08.2015 № 305. https://digital.gov.ru/ru/documents/ 4805/ (дата обращения: 22.11.2023).
3. Об утверждении методических рекомендаций по переходу государственных компаний на преимущественной использование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения. Приказ Минкомсвязи России от 20.09.2018 № 486. https://digital.gov.ru/ru/documents/ 6294 (дата обращения: 22.11.2023).