Роль искусственного интеллекта в выявлении мошенничества в системах э-счетов 3/47/24

Старший менеджер проектов отдела налогового управления и бухгалтерского учёта, PwC Латвия

Juris Boiko

Внедрение систем э-счетов в финансовую деятельность предприятий способно значительно повысить эффективность и точность. Однако с цифровым развитием сопряжены новые риски, особенно в сфере мошенничества. Растущая роль технологий в финансовых сделках вынуждает предприятия укреплять свои системы безопасности и обращаться к современным решениям для выявления мошенничества. В этой сфере искусственный интеллект (ИИ) стал важным инструментом, обеспечивающим предприятия прогрессивными методами выявления, предотвращения и сокращения мошенничества. В данной статье мы рассмотрим возможности ИИ по выявлению мошенничества в системах э-счетов и практические выгоды для предприятий.

Что такое мошенничество в системах э-счетов?

Системы э-счетов, автоматизирующие обмен счетами между поставщиками и покупателями, рационализируют процессы, уменьшают издержки и повышают точность. Однако с распространением систем э-счетов растет и вероятность мошенничества. Мошенничество в системах э-счетов может проявляться по-разному:

- мошенничество со счетами – мошенники создают поддельные счета для использования предприятий, часто выдавая себя за законных поставщиков или используя схожие наименования предприятий, чтобы ввести контрагентов в заблуждение и завладеть средствами;
- дублированные счета – мошенники подают один и тот же счет неоднократно, из-за чего происходит дублирование платежей;
- завладение доступом к электронной почте предприятия – киберпреступники получают доступ к корпоративным учетным записям электронной почты, чтобы отправить фальшивые счета или изменить платежные реквизиты и перенаправить средства;
- фишинговые атаки – мошенники используют поддельные электронные адреса, чтобы побудить работников выдать чувствительную информацию или нажать на вредоносные ссылки.

Использование технологий ИИ для выявления мошенничества

ИИ и технологии машинного обучения стали немаловажным подспорьем при выявлении мошенничества в системах э-счетов. Управляемые ИИ системы выявления мошенничества используют алгоритмы машинного обучения, анализ данных и распознавание моделей, чтобы идентифицировать аномалии и мошеннические действия в режиме реального времени. К примеру, алгоритмы ИИ могут анализировать исторические данные счетов для определения моделей и норм законных сделок. Осуществляя непрерывный контроль над входящими счетами, эти системы

способны обнаружить отклонения, например необычно крупные суммы или нетипичные условия оплаты. Кроме того, технологии ИИ умеют постоянно совершенствоваться, обучаясь на новых данных и выявленных случаях мошенничества, что делает систему все более эффективной.

Преимущества выявления мошенничества с использованием ИИ

Выявление мошенничества с использованием ИИ обладает рядом преимуществ в сравнении с проверкой вручную:

- повышенная точность – алгоритмы ИИ способны быстро и точно анализировать большой объем данных, идентифицируя аномалии и потенциальные мошеннические схемы, тем самым снижая риск мошеннических действий;
- экономия издержек – предотвращая мошенничество до его возникновения, предприятия могут избежать значительного финансового ущерба;
- улучшенная безопасность – решения ИИ усиливают общие меры безопасности, затрудняя мошенникам использование уязвимостей;
- масштабируемость – системы ИИ легко адаптируются к растущему объему данных и сделок;
- непрерывное обучение – модели машинного обучения постоянно совершенствуются, обучаясь на новых данных и выявленных попытках мошенничества;
- круглосуточный надзор без выходных – технологии ИИ действуют непрерывно, обеспечивая постоянный надзор за системой и реагируя на любую подозрительную активность.

Выгоды для предприятий

Внедрив управляемую ИИ систему выявления мошенничества, предприятия могут значительно улучшить свои процессы управления финансами и защититься от мошенников. Технологии ИИ способны помочь предприятиям сэкономить время и ресурсы, а также уменьшить финансовый ущерб и репутационные риски. К тому же использование решений ИИ позволяет предприятиям повысить свою конкурентоспособность и адаптироваться к современной цифровой среде.

Проблемы и решения

Несмотря на то что технологии ИИ обладают множеством преимуществ, их внедрение для выявления мошенничества может быть сопряжено с проблемами. Одна из основных проблем – ложно положительные результаты, когда система ИИ ошибочно помечает законные счета как подозрительные. Это может привести к растрате времени и ресурсов на ненужное расследование. Такой риск может быть особенно выраженным, если модели ИИ недостаточно точно обучены или им недостает человеческого надзора при проверке отмеченных счетов. Чтобы снизить этот риск, важно тщательно обучать модели ИИ и обеспечивать человеческий надзор, который поможет верифицировать подозрительные счета.

Перспективы

ИИ обладает гигантским потенциалом, однако важно помнить, что это инструмент, а не замена

человеческих знаний. Предотвращение мошенничества с э-счетами в будущем, скорее всего, будет основываться на подходе сотрудничества. ИИ будет выполнять анализ большей части данных и работы по выявлению аномалий, а люди – обеспечивать надзор и принимать решения в наиболее сложных случаях. Такой подход позволит по максимуму использовать потенциал ИИ, обеспечивая высокую точность и эффективность выявления мошенничества, сохраняя при этом вовлечение человека в процесс принятия решений.

Выводы

Управляемые ИИ системы выявления мошенничества – это решение будущего для укрепления безопасности систем э-счетов. Они помогают предприятиям защититься от попыток мошенничества, улучшают безопасность и обеспечивают эффективное управление финансами. Внедрив решения ИИ, предприятия могут принимать превентивные меры и быть на шаг впереди мошенников, одновременно совершенствуя свои внутренние процессы и повышая конкурентоспособность в цифровую эпоху.