СЕКЦИЯ «АКТУАЛЬНЫЕ ВОПРОСЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ И ПРАВА»

УДК 65 351.72(075.8)

АЗИАТСКАЯ ПРАКТИКА ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

***Акулова Софья Алексеевна**, студентка 4 курса бакалавриата Финансового Университета при Правительстве РФ, Sophia0105@mail.ru*

***Научный руководитель - Бабанская Анастасия Сергеевна**, к.э.н., доцент Кафедры экономической безопасности и управления рисками Финансового Университета при Правительстве РФ, ASBabanskaya@fa.ru*

***Аннотация**. Все больше ИИ применяется для противодействия мошенничеству на всех уровнях, поэтому представляется актуальным использование лучших практик других стран, в особенности тех, которые идут по траектории опережающего развития. В работе представлен опыт ОАЭ и Индии в направлении развития и использования ИИ, а также проанализированы векторы развития данного направления в России.*

***Ключевые слова:** искусственный интеллект, субтехнологии, мошенничество, финансовые риски, мониторинг финансовых операций.*

ASIAN PRACTICE OF COUNTERING FRAUD USING ARTIFICIAL INTELLIGENCE

***Akulova Sofya Alekseevna**, 4th year undergraduate student at the Financial University under the Government of the Russian Federation, Sophia0105@mail.ru*

***Scientific supervisor - Anastasia Sergeevna Babanskaya**, Ph.D. in Economics, Associate Professor of the Department of Economic Security and Risk Management at the Financial University under the Government of the Russian Federation, ASBabanskaya@fa.ru*

***Annotation**. More and more AI is being used to combat fraud at all levels, so it seems relevant to use the best practices of other countries, especially those that are on a trajectory of advanced development. The work presents the experience of the UAE and India in the development and use of AI, and also analyzes the vectors of development of this area in Russia.*

***Key words:** artificial intelligence, subtechnologies, fraud, financial risks, monitoring of financial transactions.*

ИИ может быть задействован в части противодействия мошенничеству ИИ может выявить подозрительные транзакции в организации, которые могут быть факторами мошенничества. ИИ-системы способны в режиме реального времени отслеживать транзакции и действия сотрудников во внутренних информационных системах [3, 4, 6]. Это позволит не только снизить нагрузку на сотрудников, предоставляя им время для более сложных контрольных процедур, требующих профессионального суждения, но и сократит вероятность человеческой ошибки в реализации рутинной работы. Алгоритмы ИИ можно направить на выявление рисковых ситуаций в бизнес-процессах, оценку финансовых рисков, идентификации неблагонадежных партнеров, что позволит менеджменту принимать проактивные действия для снижения рисков [1, 2, 5]. Также контроль деятельности сотрудников финансовых организаций, чьи недобросовестные действия могут способствовать совершению преступлений путем незаконной передачи персональных данных клиентов безусловно важен и одновременно сложен.

Рассматривая тему международной практики, нужно отметить что сотрудничество и обмен информацией в области ИИ складывается через платформу БРИСК, а XIV саммите (2022г.) принята Пекинская декларация. В ней выражается обеспокоенность этическим аспектом применения ИИ, рисками и дана оценка использованию технологии.

Нефтегазовая компания «ADNOC» в числе тех, кто первыми начал внедрять ИИ в операционную деятельность, так в 2017 году запущены два проекта Thamama и Panorama, а к 2020 году использование ИИ принесли выгоду в 2,1 млрд долларов, по заявлению компании.

В 2019 году *Федеральной налоговой службой ОАЭ* [4] запущена новая электронная мониторинговая система, использующая цифровые фискальные марки. Данная система отслеживает факты уплаты акцизного налога на табачную продукцию. Идея её создания заключается в использовании современных инструментов для борьбы с уклонением от уплаты акцизного налога и коммерческого мошенничества. Система включает в себя интегрированные электронные мониторинговые инструменты, которые фиксируются в таможенных пунктах, а также по всей цепи поставок в ОАЭ.

С целью снижения фактов мошенничества Советом по кибербезопасности Объединенных Арабских Эмиратов создан *онлайн-портал CheckMyLink* (Staysafe.csc.gov.ae) для проверки ненадежных и фальшивых веб-сайтов, позволяющий проверить, не связаны ли найденные веб-сайты с мошенниками [4]. Пользователи нейросервиса имеют возможность ввести адрес любого веб-сайта, а платформа проверит его на наличие вредоносного ПО, инструментов фишинга или другого мошенничества.

Не менее интересен опыт Индии. *Pramaan Exchange* признается одним из самых инновационных решений [7]. Это крупнейшая *биржа садоводства,* которая работает на основе Intello Labs. Данный агротехнический стартап применяет субтехнологию компьютерного зрения. Субтехнология на базе данных из 300 млн изображений плодоовощной продукции анализирует на

предмет соответствия продукцию поставщика, таким образом проверяя ее на качество.

Искусственный интеллект становится эффективным инструментом в борьбе с экономическими преступлениями. Чтобы противостоять преступникам, необходимо просто проявлять изобретательность аналогичную, мошенническим схемам.

Внедрение ИИ, безусловно, потянет за собой дополнительные расходы компаний, учреждений и организаций госсектора, вместе с тем, система внутреннего контроля выйдет на новый современный уровень и будет уравновешиваться обязательным внедрением обучающих программ и тренингов для сотрудников и топ-менеджеров.

Создание внутренних контролирующих нейромеханизмов для отслеживания подозрительных финансовых операций, использования фиктивных лиц или подставных компаний позволит сократить вероятность мошеннических проявлений на всех уровнях рабочего процесса, в том числе неосознанного участия российских компаний в противоправных действиях, и тем самым в разы снизит количество экономических преступлений.

Библиографический список

1. Бабанская, А.С., Груднева, А.А. Анализ и оценка финансовых рисков // Бухучет в сельском хозяйстве. - 2020. - № 4. - С. 66-75.

2. Хоружий, Л.И., Бабанская, А.С., Трясцина, Н.Ю. Мошенничество с финансовой информацией: анализ и оценка деловых партнеров // Бухучет в сельском хозяйстве. - 2018. - № 5. - С. 68-80.

3. ИТ-рынок России // TADVIER. Государство. Бизнес. Технологии. – 2024. - [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/ (дата обращения 20.10.2024)

4. ИТ-отрасль: ключевые показатели развития за 2019–2023 гг. // ИСИЭЗ ВШЭ. - 2024. - [Электронный ресурс]. – Режим доступа: https://issek.hse.ru/news/912948511.html (дата обращения 20.10.2024)

5. Ляжнева, Л. Строгость и предупреждения: в РФ появятся новые механизмы борьбы с мошенниками // Известия. – 2024. - [Электронный ресурс]. – Режим доступа: https://iz.ru/1768232/liubov-lezhneva/strogost-i-preduprezhdeniia-v-rf-poiaviatsia-novye-mekhanizmy-borby-s-moshennikami (дата обращения 20.10.2024)

6. Медведев, Ю. Как российский искусственный интеллект ловит мошенников // Наука. - 2024. - [Электронный ресурс]. - Режим доступа: https://rg.ru/2024/03/27/sledstvie-vedet-nejroset.html (дата обращения 20.10.2024)

7. Нилекани, Н., Бхлджвани, Т. Индию ждет трансформация, способная изменить ее экономическое и социальное будущее // Международный Валютный Фонд. - 2024. - [Электронный ресурс]. - Режим доступа:https://www.imf.org/ru/Publications/fandd/issues/2023/12/POV-unlocking-india-potential-with-AI-Nilekani-Bhojwani (дата обращения 20.10.2024)