УДК 336.71

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СНИЖЕНИИ РИСКА МОШЕННИЧЕСТВА В БАНКОВСКИХ СИСТЕМАХ

Кузьминых М. А.

студент,

Вятский государственный университет,

Киров, Россия

Халтурина Т. А.

студент,

Вятский государственный университет,

Киров, Россия

Казанцева А. В.

Преподаватель,

Вятский государственный университет,

Киров, Россия

Аннотация. В статье проводится комплексное исследование роли технологий искусственного интеллекта в противодействии финансовому мошенничеству в банковском секторе. Ключевыми барьерами остаются необходимость в качественных данных и киберриски. В заключении обосновывается неизбежность перехода к предиктивной и адаптивной кибербезопасности на основе ИИ как основы устойчивости цифровой финансовой экосистемы.

Ключевые слова: банковское мошенничество, финансовые риски, искусственный интеллект, ИТ-технологии, мошенники, банковская система.

THE ROLE OF ARTIFICIAL INTELLIGANCE IN REDUCING THE RISK OF FRAUND IN BANKING SYSTEMS

Kuzminykh M.A.

student,

Vyatka State University,

Kirov, Russia

Khalturina T.A.

student,

Vyatka State University,

Kirov, Russia

Kazantseva A.V.

Teacher,

Vyatka State University,

Kirov, Russia

Annotation. The article provides a comprehensive study of the role of artificial intelligence technologies in countering financial fraud in the banking sector. The key barriers remain the need for high-quality data and cyber risks. In conclusion, the article argues for the inevitability of transitioning to predictive and adaptive AI-based cybersecurity as a foundation for the sustainability of the digital financial ecosystem.

Keywords: banking fraud, financial risks, artificial intelligence, IT technologies, fraudsters, and the banking system.

Цифровая трансформация банковской сферы и экспоненциальный рост объема онлайн-операций привели к параллельной эволюции методов финансового мошенничества. По данным Ассоциации российских банков, ущерб от мошеннических операций в 2023 году составил десятки миллиардов рублей, демонстрируя устойчивый рост. Традиционные правила (rule-based systems), основанные на статических порогах и сигнатурах, не справляются с адаптивностью и изощренностью современных атак, таких как социальная инженерия, подмена SIM (SIM-swap) или скоординированные атаки «тихих» мультиаккаунтов. Это создает системные риски как для финансовых институтов (прямые убытки, репутационный урон, регуляторные санкции), так и для экономики в целом, подрывая доверие к цифровым сервисам. В этом контексте технологии искусственного интеллекта и машинного обучения представляют собой качественный скачок в возможностях проактивного и прецизионного противодействия мошенничеству.

Сокращение масштабов мошенничества и необоснованных транзакций является первостепенной задачей для банковских работников, так как напрямую влияет на итоговый результат их деятельности. Клиенты банка, поставщики, финансисты, деловые партнеры первоначально смотрят на статус банка, на который влияет мошенничество, вернее, как с ним борется банк. Действительно, мошеннические действия наносят существенный ущерб репутации, а также финансовый ущерб, что влечет за собой отрицательный пользовательский опыт и снижают уровень доверия клиентов. [3]

В настоящее время мошенники становятся более убедительными в создании убедительных звонков, электронных писем (SMS) и сайтов, что затрудняет защиту жертв. Примером банковского мошенничества может быть кража аккаунта в маркетплейсе. Представляясь сотрудниками службы безопасности, мошенники звонят людям и выманиваю коды, приходящие им на телефон, под предлогом отмены операции. И далее, чтобы получить коды

от наиболее значимых сервисов, таких как Госуслуги или онлайн-банки, мошенники используют скомпрометированный аккаунт магазина.

Так, например, в 2024 году мошенники похитили у россиян рекордные 27.5 млрд. руб. с банковских счетов – на 74,4% больше, чем в 2023 году. Основной объем средств (26,9 млрд. руб.) был украден у физических лиц. По оценке Сбербанка, ущерб от телефонного мошенничества в 2024 году составил не менее 295 млрд. руб. Согласно опросу Банка России, 34% граждан сталкивались с различными видами кибермошенничества, при этом (% из них потеряли деньги.

Из представленной выше информации следует вывод о том, что мошенники с каждым годом становятся более убедительны и изобретательны, что влечет за собой финансовые потери населения. Именно поэтому искусственный интеллект, расцветающий в настоящее время, является наиболее эффективным, кроме того, быстрым способом выявления мошенничества.

По исследованию статистических данных, было выявлено, что в 2021 году финансовые учреждения потратили более 220 млрд. долл. США на внедрение приложений ИИ с целью устранения мошенничества и оценки рисков. [1] Тем не менее, 66% финансовых учреждений считают, что ИИ может определить мошеннические действия до того, как человек потеряет деньги.

По данным RG.RU, каждый четвертый банк в России использует искусственный интеллект для решения различных задач. Ведь именно использование ИИ позволяет банкам экономить примерно 15-20% операционных расходов.

Как же в России вводят ИИ в банковскую систему? К слову, «Свой Банк» находится на стадии реализации кросс-канальной системы антифрода с использованием алгоритмов машинного обучения, который автоматически предоставит банку обнаруживать изменения в поведении активности

клиентов, свести к минимуму уровень мошеннических ситуаций, и, конечно же, усилить меры безопасности. Technical Project Manager, Сергей Волынец, утверждает, что именно интеллектуальные системы обеспечивают необходимый баланс между скоростью, безопасностью и удобством, и потому Банк намерен продолжать развивать эти решения, чтобы идти в ногу с тенденциями рынка и запросами клиентов. [2]

Следующим примером можно привести разработку и тестирование Банком России совместно с участниками рынка технологии, которая «подкрепит потребителя искусственным интеллектом». Данный ИИ-помощник будет читать и разбирать договор (мелкий шрифт, непонятные фразы и т.д.) «от корки до корки». "Договор упростить сложно: у нас много требований законодательства и регулирования. Регулирование тоже нельзя убрать - оно направлено на защиту от рисков", - пояснила Набиуллина. А вот пересказывать юридический документ простыми словами закон не препятствует. Этот ИИ-помощник – не продукт продавца, а независимый продукт. То есть он не будет подкручен под нужды того, кто продает его. В данном проекте готовы участвовать 10 розничных банков. Планируется к концу марта 2026 года уже протестировать самые востребованные продукты. [4]

Внедрение умных алгоритмов позволяет банкам сокращать издержки и делать свои продукты более качественными и доступными для клиентов. Общение в чатах поддержки, на горячих линиях, с голосовыми помощниками уже происходит не с живыми людьми, а с алгоритмами, что позволяет сэкономить средства на заработные платы консультантов банков. Кроме того, ИИ настолько виртуозно имитирует речь, используя интонацию, речевые паузы, делая акценты на определенных словах. Причем ответы на поставленные вопросы ИИ даст быстро, четко и без ошибок.

По оценкам McKinsey, экономический эффект от внедрения продуктов генеративного ИИ в разных секторах мировой экономики составит 2,6–4,4

трлн долларов США в год, а 75% прироста даст использование генеративного ИИ в маркетинге, клиентских сервисах и разработке программного обеспечения. Также развитие клиентских сервисов (чат-боты и голосовые помощники) позволяет увеличить выручку банков на 200-340 млрд долларов США.

Несмотря на потенциал, масштабирование ИИ сталкивается с серьёзными вызовами. Во-первых, сложные модели (особенно нейросети) не предоставляют понятных причин для принятия решения. В таком случае это вступает в конфликт с регуляторными требованиями, например, с Федеральным законом №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», о необходимости объяснять причины блокировки и правами клиента на информацию.[5]

Во-вторых, мошенники начинают использовать методы генеративного ИИ для создания ложных паттернов транзакций, обходящих обученные модели. Что, в свою очередь, требует постоянного «состязательного» обучения моделей. Так, например, Количество афер через Систему быстрых платежей (СБП) выросло на 217% по данным ЦБ. За первый квартал 2024 года через СБП было похищено 1,13 млрд рублей, что в два раза превысило показатель первого квартала 2023 года.

В-третьих, использование искусственного интеллекта может привести к дискриминации. Регуляторы, такие как Центральный Банк России, развивают принципы ответственного ИИ, требуя управляемости, прозрачности и справедливости. По данным Gartner, к 2027 году 60% ИИ-систем будут проходить обязательную сертификацию на этичность.

И, в-четвертых, внедрение требует модернизации ИТ-архитектуры и наличия редких специалистов, обладающих высокой квалификацией. По данным консалтинговой компании «Яков и Партнёры», 91% российских банков отмечают нехватку квалифицированных специалистов уровня senior и

выше в областях data science, машинного обучения и сопровождения ИИ-платформ.

В ответ на выявленные вызовы предлагается концепция адаптивной экосистемы фрод-мониторинга, которая построена на трёх принципах:

1. Федеративное обучение как основа кооперации. Вместо централизованного хранилища данных предлагается модель, при которой ИИ-модель обучается децентрализовано — на устройствах или серверах отдельных банков. Обновления моделей (градиенты), а не сами конфиденциальные данные, агрегируются на центральном сервере. Это позволяет преодолеть ключевые барьеры (дефицит данных, соблюдение конфиденциальности и т.д.);

2. Объяснимый ИИ. Система не только блокирует операцию, но и генерирует понятное для клиента и регулятора обоснование (например: «Операция отклонена из-за аномально высокой суммы, нехарактерного времени суток и использования нового устройства, что в совокупности даёт 94% вероятность мошенничества»).

3. Многоуровневая архитектура с генеративными симуляторами. Эти симуляторы позволят проводить «стресс-тестирование» основных моделей детекции в безопасной среде и проводить их опережающее дообучение, создавая эффект упреждающей адаптации.

В заключении следует отметить, что технологии искусственного интеллекта предоставляют качественно новый уровень защиты банковских систем, смещая парадигму от реактивного к предиктивному и адаптивному фрод-мониторингу. Экономический эффект от внедрения носит многокомпонентный характер и складывается не только от предотвращенных прямых убытков, но и сохранения операционных расходов, клиентской базы и репутации банка. Ключевым ограничением массового внедрения является не технологическая сложность, а совокупность вызовов, связанных с интерпретируемостью моделей, дефицитом данных и кадров. Перспективы

дальнейших исследований видятся в изучении возможностей квантового машинного обучения и анализа сверх больших графов, развитии федеративного обучения для межбанковского сотрудничества без обмена конфиденциальными данными, а также в глубоком экономико-математическом моделировании макроэкономического эффекта от массового внедрения ИИ-систем в финансовом секторе.

Библиографический список:

1. How is AI transforming fraud detection in banks? [Электронный ресурс]. URL: https://www.telusinternational.com.

2. Интеллектуальный щит: как ИИ защищает банки от мошенников. [Электронный ресурс]. URL: https://companies.rbc.ru/news/uyG2zxjiMi/intellektualnyij-schit-kak-ii-zaschischaet-banki-ot-moshennikov/.

3. Багреева Е.Г., Исмаилов Н.Э., Бобылева Л.М. Искусственный интеллект как противодействие мошенничеству в банковской сфере // Евразийская адвокатура. – 2022. - №2 (57). – С.90. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-kak-protivodeystvie-moshennichestvu-v-bankovskoy-sfere/viewer .

4. Поможет людям и снизит риск недобросовестных практик. Банк России разрабатывает ИИ-помощника для чтения сложных договоров. [Электронный ресурс]. URL: https://rg.ru/2025/11/18/centrobank-sdelaet-finansovye-uslugi-chelovechnee-s-pomoshchiu-robotov.html.

5. Федеральный закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" от 07.08.2001 N 115-ФЗ. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_32834/.