

Секция «Управление рисками и страхование: новые вызовы и возможности»

Искусственный интеллект как инструмент противодействия кибератакам и мошенничеству в российских банках

Научный руководитель – Саблукова Юлия Геннадьевна

Абрамова Мария Владимировна

Студент (бакалавр)

Московский государственный университет имени М.В.Ломоносова, Москва, Россия

E-mail: osama2004526@gmail.com

На волне цифровизации во все сферы экономики внедряются новые технологии, особенно популярны технологии на основе искусственного интеллекта. Данный тренд не обошел стороной и банковскую сферу. Наиболее важными направлениями использования искусственного интеллекта в банках по данным анкетирования 50 российских банков из топ-100 банков России, проведенным рейтинговым агентством “Эксперт РА”, являются кредитный скоринг, выявление мошеннических транзакций, взыскание задолженности [2]. Мошенничество в российских банках является достаточно большой проблемой, так, например, в 2023 году по сравнению с 2022 годом объем операций без добровольного согласия клиентов (ОБДС) вырос на 11,48%, а в 2024 году данный показатель вырос на 74% по сравнению с 2023 годом [1]. Таким образом, можно сказать, что с каждым годом число мошеннических операций только увеличивается [1]. К тому же наибольший объем хищений денежных средств в 2024 году по ОБДС среди физических лиц приходился на системы дистанционного банковского обслуживания и составил 9 602.57 млн рублей. Стоит отметить, что наиболее распространенным методом мошенничества является фишинг, на него в 2023 году приходилось 55% от общего числа средств, используемых злоумышленниками, а в 2024 году на данный тип ресурса приходилось уже 58%. Таким образом, в российских банках проблема мошенничества стоит достаточно остро [1]. Как было упомянуто ранее, одним из перспективных направлений использования искусственного интеллекта (ИИ) в российских банках является мошенничество, так как он способен не только анализировать большие объемы данных в реальном времени, выявлять подозрительные транзакции и реагировать на них, но и адаптироваться к новым видам мошенничества, так как адаптивные модели искусственного интеллекта имеют способность обучаться на исторических данных [3]. Например, модель может составить профиль клиента, путем анализа его паттернов поведения, в случае если клиент проявит необычную активность, то система безопасности на основе ИИ сможет приостановить транзакцию и известить банк об инциденте. Однако использование ИИ имеет ряд проблем, например, ложное срабатывание систем безопасности, при котором ИИ неправильно определяет характер транзакции, определяя ее как аномальную и приостанавливая ее. Вследствие этого сотрудникам службы безопасности приходится реагировать на данную проблему и тратить время на выяснение обстоятельств и причин срабатывания, а доверие клиента к банку может подорваться вследствие блокировки транзакции без причины. Другая проблема состоит в сложности интерпретации результатов ИИ, она исходит из нехватки квалифицированных специалистов на рынке. Также еще одной проблемой является обеспечение качественных данных для обучения систем ИИ [3]. Таким образом, несмотря на все проблемы, сопутствующие внедрению и использованию искусственного интеллекта, он остается одним из наиболее перспективных инструментов противодействия мошенничеству благодаря его способностям анализировать большие объемы данных, выявлять аномалии в реальном времени и адаптироваться к новым видам мошенничества.

Источники и литература

- 1) Центральный банк Российской Федерации. Обзор операций в теневом секторе: анализ транзакционной активности. 2024. URL: https://www.cbr.ru/analytics/ib/operations_survey/2024/ [дата обращения: 07.03.2025].
- 2) Эксперт РА. Искусственный интеллект в банковском секторе России: аналитический обзор. 2018. URL: https://raexpert.ru/researches/banks/bank_ai2018/ [дата обращения: 07.03.2025].
- 3) Hafez I.Y., Hafez A.Y., Saleh A. et al. A systematic review of AI-enhanced techniques in credit card fraud detection // J Big Data. 2025. Т. 12, № 6. DOI: 10.1186/s40537-024-01048-8 [дата обращения: 07.03.2025].