Секция «10.5 Компьютерное право и информационная безопасность»

Проблемы и перспективы искусственного интеллекта в обеспечении информационной безопасности банков

Научный руководитель – Зуева Анна Сергеевна

Демидова Софья Леонидовна
Студент (бакалавр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра государственного аудита, Москва, Россия
E-mail: demidovasl2005@mail.ru

Проблемы и перспективы искусственного интеллекта в обеспечении информационной безопасности банков

Демидова Софья Леонидовна
Студентка 3 курса
Московский государственный университет имени М.В. Ломоносова, Москва, Россия
факультет Высшей школы государственного аудита
E-mail: demidovasl2005@mail.ru
Научный руководитель: Зуева Анна Сергеевна, к.э.н., доцент
Преподаватель кафедры компьютерного права и информационной безопасности
Московского государственного университета имени М.В. Ломоносова
E-mail: dgastin@mail.ru

В настоящее время технологии искусственного интеллекта (ИИ) применяются практически во сферах жизни – от профессиональных задач до повседневной деятельности. Масштаб внедрения данных технологий можно подтвердить статистикой: согласно отчету Стэндфордского университета за 2025 год, объём мировых частных инвестиций в генеративный ИИ достигли 33,9 млрд долларов в 2024 году[1]. В России также наблюдается устойчивый рост интереса: совокупные инвестиции «СберБанка» в развитие генеративного искусственного интеллекта в 2024-2026 годах составили около 600 млрд рублей.[2].

Особенно интенсивно искусственный интеллект используется в банковском секторе. Искусственный интеллект в банковской сфере развивался не одно десятилетие. Первые попытки внедрения информационных технологий в банках относятся еще к 1987 году, когда Security Pacific National Bank (один из крупнейших банков США) применил алгоритмы для противодействия мошенничеству с дебетовыми картами. Дальнейшее развитие технологий связано с становлением вычислительных мощностей, распространением облачных технологий и накоплением больших массивов данных (Big Data).

Ключевая перспектива применения ИИ в обеспечении информационной безопасности в банковской сфере заключается в превентивных мерах. В настоящее время алгоритмы машинного обучения уже способны в реальном времени выявлять аномалии и признаки подозрительных транзакций, прогнозировать финансовые риски на основе Big Data, усиливать биометрическую аутентификацию и идентификацию клиентов, а также автоматизировать реагирование на инциденты информационной безопасности[3]. Использование ИИ позволяет оптимизировать нагрузку работников по безопасности, повысить обнаружение/нейтрализацию угроз и минимизировать ущерб от кибератак. Лидерами внедрения ИИ в российской финансовой сфере выступают такие крупные банки, как «Сбербанк» «Газпромбанк», «ВТБ», «Росбанк», «Банк Хоум Кредит», «Россельхозбанк» и «Московский кредитный банк»[4].

Однако массовое внедрение ИИ в сфере банковских услуг связано с рядом существенных рисков[5]. Во-первых, использование больших массивов данных для обучения моделей

ИИ кратно увеличивает потенциальный ущерб от утечек информации, ставя под угрозу не только отдельные записи, но и сами алгоритмы, составляющие основу интеллектуальной собственности кредитной организации. Во-вторых, проблема предвзятости моделей влечет за собой финансовые потери и дискриминацию клиентов, возникающая из-за некачественных данных. В-третьих, ни один алгоритм не обеспечивает абсолютной точности в обнаружении мошеннических операций, что создает прямую угрозу достоверности информации, предоставляемой клиентам. Наконец, угрозу представляет собой проблема «предодобренных кредитов», когда мошенники, получают доступ к мобильному банку клиента путем внедрения вредоносного программного обеспечения[6].

Таким образом, искусственный интеллект способствует развитию информационной безопасности в банковской сфере. Его применение позволяет повысить уровень защиты, основанный на прогнозировании и адаптации к постоянно меняющимся угрозам. Вместе с тем, внедрение ИИ порождает новые уязвимости и риски – от дискриминации клиентов из-за некачественных данных до использования самих алгоритмов в качестве вектора кибератак. Дальнейшее развитие технологий требует не только инвестиций в вычислительные мощности, но и разработки комплексных стратегий по вопросам этики, прозрачности моделей, правового регулирования и устойчивости к новым видам мошенничества.

[1] https://hai.stanford.edu/ai-index/2025-ai-index-report/economy

[2] https://tass.ru/ekonomika/25868201

[3] Болонина С.Е., Лев М.Ю. Искусственный интеллект в обеспечении безопасности финансового сектора:

превентивные меры и управленческие решения // Экономика, предпринимательство и право. – 2025. –

Том 15. – № 6. – С. 4349–4364.

[4] Городецкая О.Ю. Проблемы внедрения технологий искусственного интеллекта в банках и пути их преодоления / О. Ю. Городецкая, Я. Л. Гобарева // Инновации и инвестиции. – 2023. – № 3. – С. 212–217.

[5] Семеко Г.В. Искусственный интеллект в банковском секторе: возможности и проблемы / Г. В. Семеко // Социальные новации и социальные науки. – 2021. – № 2. – С. 81–97.

[6] Сиземова О. Б. Правовое регулирование использования технологий искусственного интеллекта в банковской деятельности / О. Б. Сиземова // Вестник Университета имени О.Е. Кутафина. – 2024. – № 9. – С. 132–140.