

УДК 343

К вопросу об уголовно-правовых рисках использования искусственного интеллекта в банковской сфере¹

Бондарева-Битяй Евгения Вадимовна, студент, Владимирский государственный университет имени А. Г. и Н. Г. Столетовых, evgeniabondarevab@gmail.com

Статья посвящена рассмотрению использования искусственного интеллекта в банковской сфере и анализу связанных с этим уголовно-правовых рисков. Исследуются ключевые технологии искусственного интеллекта, а также потенциальные угрозы, включая мошеннические действия и кибератаки, совершаемые с его применением. Особое внимание уделяется вопросам этики, ответственности и необходимости разработки правовых норм, направленных на минимизацию негативных последствий внедрения искусственного интеллекта в финансовый сектор.

Ключевые слова: искусственный интеллект, безопасность, банковская сфера, персональные данные, дискриминация.

В настоящий момент мир переживает очередную промышленную революцию, характеризующуюся повсеместным внедрением искусственного интеллекта (ИИ) в быт обывателя. Сегодня наиболее популярными формами ИИ выступают ChatGPT, нейросети и голосовые помощники. Однако даже технологии, ставшие привычными, не останавливаются в развитии и уже появились их отдельные виды.

Самым ярким из них стал генеративный искусственный интеллект, который, в отличие от обычного, создает новое на основе той информации, которая ему предоставлена. Он может создавать оригинальный творческий контент, будь то текст, изображение, музыка или компьютерный код. Фактически генеративный ИИ может давать более точные решения. Так или иначе, каждый человек сталкивался с ним в обычной жизни, и если очевидные плюсы лежат на поверхности, то о минусах и возможных негативных последствиях использования ИИ говорить принято не всегда.

Особого внимания заслуживает вопрос о безопасности использования искусственного интеллекта и иных инновационных технологий в банковской сфере. В последние годы банковский сегмент стал активно применять новейшие технологии. Все началось с решения задачи кредитования, а затем распространилось и на другие банковские продукты.

В июне 2023 г. было опубликовано исследование о значимости ИИ для банков и его будущем в рассматриваемой сфере. В дальнейшем, а именно к 2030 г., инвестиции на разработку и внедрение таких алгоритмов составят 300 млрд долл. Ситуация в России отличается незначительно: большинство крупных банков активно пользуются благами прогресса, а некоторые создают собственные нейросети. Ярким примером можно считать GigaChat от Сбербанка [17].

Возникает вопрос: какие риски несет повсеместное использование нейросетей и других форм ИИ в банковской сфере? Если объединить возможные риски, то можно выделить две группы: безопасность и этические аспекты.

Говоря о безопасности, следует уточнить, что в первую очередь речь идет о персональных данных. Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу [1]. Сейчас в банках хранятся сотни тысяч персональных данных, а также сведения о коммерческих тайнах юридических лиц. В марте 2024 г. экспертно-аналитический центр исследований InfoWatch опубликовал

исследование утечек информации ограниченного доступа из российских организаций. Так, в 2022 г. утекло более 667 млн записей с персональными данными. Это в два с половиной раза больше, чем в 2021 г.

В отчете, опубликованном в марте 2025 г., также говорится об увеличении: в 2024 г. количество утечек записей с персональными данными достигло 1,5 млрд. Более того, 29 % всех утечек составляет аутентификационная информация пользователей (пароли, логины, номера мобильных телефонов и др.). Несмотря на лидерство маркетплейсов и иных торговых площадок среди компаний с наибольшим числом утечек, приложения банков также входят в этот список.

52 % компаний, использующих ИИ в своей деятельности, отмечают и понимают риски, связанные с утечкой персональных данных, что фактически создает барьер для дальнейшего развития новейших технологий и их алгоритмов в выбранной сфере.

Кроме того, системы ИИ подвержены рискам мошеннических атак на стадии как обучения (атаки данных), так и эксплуатации моделей (атаки моделей). Изменение данных приводит к ухудшению результативности работы алгоритмов машинного обучения и нарушению работы модели.

Деяния, совершаемые в рассматриваемых ситуациях, имеет смысл квалифицировать по ч. 1 ст. 13.11 Кодекса Российской Федерации об административных правонарушениях [3] или по ч. 1 ст. 137 Уголовного кодекса Российской Федерации. Понятия «частная жизнь» и «персональные данные» имеют схожее значение. Как отмечалось ранее, персональные данные — любая информация, относящаяся к одному определенному лицу. Частная жизнь — область жизнедеятельности человека, относящаяся к отдельному лицу, касающаяся только его и не подлежащая контролю со стороны общества и государства, если она не носит противоправного характера. Отсюда следует, что оба определения не только схожи по смыслу, но и имеют легальный характер. Соответственно, правонарушения, направленные на утечку персональных данных, следует понимать как посягательство на частную жизнь, что является логичным выводом.

Однако помимо рисков, связанных с личной жизнью, следует учитывать и вопросы этики, с которыми ситуация значительно сложнее. ИИ является в первую очередь инструментом, обучение которого осуществляет человек. Насколько глубоко будут прорабатываться вопросы пола, расы или национальной принадлежности? Если обратиться к примеру кредитования, то вполне вероятно, что

¹ Научный руководитель: Кисляков Антон Валерьевич — доцент кафедры уголовно-правовых дисциплин, Владимирский государственный университет имени А. Г. и Н. Г. Столетовых, кандидат юридических наук, доцент.

преимущество получит мужчина, т. к. мужчины, согласно результатам исследования Росстата 2023 г., зарабатывают больше.

Кроме того, существуют наглядные примеры дискриминации со стороны ИИ в сферах, далеких от банковской. Самым известным считается опыт компании Amazon. В 2014 г. компания решила использовать ИИ для найма сотрудников, однако идея не увенчалась успехом, т. к. алгоритмы исключали кандидатуры женщин и выбирали только мужчин, несмотря на то что они могли быть менее квалифицированными. Алгоритм основывался на данных десятилетней давности, согласно которым в отрасли доминировали мужчины. Анкеты, где были указаны женский пол, членство в женских клубах и иные данные, имеющие подобный контекст, алгоритм либо исключал, либо существенно снижал их рейтинг.

При наличии подобного опыта отсутствуют гарантии невозможности повторения допущенных ошибок. Российское законодательство предусматривает два вида ответственности: административную и уголовную. Встает вопрос о субъекте, который понесет ответственность. В рассматриваемом случае ИИ действовал самостоятельно и основывался на информации, предоставленной создателями. Однако ИИ не может стать субъектом в силу отсутствия правосубъектности. Более того, квазисубъектностью он также не обладает и в ближайшее время обладать не будет. С высокой долей вероятности ответственность будут нести либо владельцы ИИ, либо его создатели. В настоящее время российское законодательство не содержит регулирования деятельности подобных алгоритмов, вследствие чего вопросы ответственности остаются открытыми.

Следует отметить, что постепенно вопросы нормативно-правового регулирования ИИ становятся предметом государственного внимания. Более того, этические аспекты применения инновационных технологий уже получают развитие. Например, в 2021 г. на I Международном форуме «Этика искусственного интеллекта:

начало доверия» был принят Кодекс этики в сфере ИИ. На сайте указано, что Кодекс носит рекомендательный характер и общеобязательным не является, представляя собой совокупность правил, предназначенных для формирования доверительных отношений между компаниями, использующими ИИ [9].

Говоря о государственном регулировании, важно отметить, что первого апреля 2025 г. был принят закон «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» [5], который вступит в силу первого июня. Помимо данного ФЗ существуют и другие инициативы по противодействию киберпреступности. В сфере регулирования искусственного интеллекта можно выделить несколько правовых актов: Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» [2] и указы Президента Российской Федерации «О развитии искусственного интеллекта в Российской Федерации» [6] и «О Стратегии национальной безопасности Российской Федерации» [7].

Таким образом, использование искусственного интеллекта в банковской сфере является значительным риском и может способствовать как возникновению уже известных преступлений, так и появлению новых противоправных деяний. Государство относительно недавно приступило к решению проблемы использования ИИ, однако это уже приносит результаты. Следует учитывать, что инициатива частных компаний столь же важна, как и правовое регулирование.

Отсюда можно сделать вывод, что именно совместная работа государства в лице его органов и частного сектора не только приблизит достижение желаемого результата, но и обеспечит его справедливость для всех участников правоотношений.

Примечания

1. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 15.04.2025).
2. Федеральный закон от 31.07.2020 N 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 15.04.2025).
3. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 15.04.2025).
4. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ // Собрание законодательства РФ. 1996. N 25. Ст. 2954.

English version

On the criminal law risks of using artificial intelligence in the banking sector

Bondareva-Bityay Evgeniya Vadimovna, student, Vladimir State University named after A. G. and N. G. Stoletovs

This article examines the use of artificial intelligence in the banking sector and analyzes the associated criminal law risks. The study explores key AI technologies and potential threats, including fraudulent activities and cyberattacks carried out with the help of AI. Special attention is given to issues of ethics, liability, and the need to develop legal norms aimed at minimizing the negative consequences of introducing artificial intelligence into the financial sector.

Keywords: artificial intelligence, security, banking sector, personal data, discrimination.