Шушаков Алексей Игоревич
студент
Савдерова Алина Федоровна
канд. экон. наук, доцент

ФГБОУ ВО «Чувашский государственный
университет им. И.Н. Ульянова»
г. Чебоксары, Чувашская Республика

СОХРАННОСТЬ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ В БАНКОВСКОЙ СФЕРЕ ПРИ ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация*: актуальность выбранной темы обоснована важностью сохранности конфиденциальных данных банков на фоне использования искусственного интеллекта, а также мерами безопасности, связанными с соблюдением нормативных требований и повышением защиты данных клиентов.*

Ключевые слова*: искусственный интеллект, риск-аналитика, кредитование, конфиденциальность, коммерческий банк.*

Внедрение искусственного интеллекта (ИИ) положительно влияет на работу банковской отрасли, увеличивая эффективность и скорость кредитования. При этом стоит учитывать и риски для безопасности, возникающие от внедрения ИИ, так как банки собирают и обрабатывают большие объемы конфиденциальных данных, что делает их привлекательными для кибератак. Исследование в этой области имеет решающее значение для разработки эффективных мер по защите персональных данных в банках.

Целью работы выступает определение рисков конфиденциальности данных, связанных с использованием ИИ в банковской отрасли, а также выработке рекомендаций при его внедрении в банковскую сферу.

В настоящее время в экономику активно внедряются технологии, связанные с искусственным интеллектом [1]. В свою очередь, это повышает значимость исследований в областях, связанных с информационной безопасностью, ведь это помогает улучшать современные процессы в организациях, обеспечивая стабильную, бесперебойную работу, благодаря чему улучшается их экономическое положение и устойчивость [2]. ИИ предлагает множество возможностей для работы банковском секторе:

− анализ непрерывного потока данных, который не может быть выполнен человеком, – ИИ способен обработать огромные объемы финансовых данных в режиме реального времени, включая транзакции, экономические и рыночные тенденции, также потребительское и корпоративное поведение;

− прогноз паттернов поведения отрасли, так как значительная часть данных и процессов в индустрии регулярно повторяется через различные комбинации, в чём и состоит преимущество ИИ перед человеком – это позволяет быстрее, точнее и эффективнее оценивать будущие риски;

− автоматизация повторяющихся, рутинных процессов, связанных с обработкой заявок, управлением и анализом запросов, что сокращает затраты времени и увеличивает эффективность.

ИИ также может быть использован в качестве консультанта при обслуживании клиентов, помогая снимать нагрузку на сотрудников горячей линии и увеличивать скорость обработки запроса клиента по интересующим их вопросам [3].

Несмотря на преимущества использования ИИ, у него есть ряд проблем и ограничений, требующих решения для безопасного функционирования [4].

В банковском деле сохранность и конфиденциальность данных банковских структур и клиентов играет немаловажную роль в процессе кредитования и управлении рисками. Мошенничество, связанное с утечкой данных клиента как со стороны банка, так и со стороны клиента или посредника может привести к колоссальным убыткам каждого участника процесса.

Эксперты отметили, что использование данных системами ИИ может привести к раскрытию конфиденциальных или защищенных законом данных [5].

Исследование AvePoint, проведенное в 2024 году, показало, что конфиденциальность и безопасность данных вызывают наибольшую озабоченность у компаний. Для обучения искусственного интеллекта часто собираются персональные данные, чтобы улучшить результаты запросов, но, как показал случай, произошедший с одним из самых популярных ИИ-помощников в 2023 году, к таким данным можно получить доступ, не являясь при этом пользователем, которому доступ был разрешен изначально [6].

Еще один случай произошел с моделями ИИ, которыми владели такие крупные компании как OpenAI, Uber и Amazon. Из-за массированных и долгих атак злоумышленникам удалось получить доступы к моделям, что позволило им изменять поведение моделей по своему усмотрению, без риска быть замеченными [7].

Безопасность данных в банковском секторе сопряжена со многими факторами, например, с защитой персональных данных клиентов, так как банки хранят большое количество конфиденциальной информации о своих клиентах, таких как персональные данные, финансовое состояние и историю транзакций. Защита этих данных от несанкционированного доступа и утечки является одной из главных целей банковской деятельности. Также стоит учитывать, что банки являются привлекательными объектами для массированных кибератак, направленных на кражу таких данных.

Для защиты конфиденциальных данных необходима надежная система безопасности, включающая в себя защиту от фишинга и атак с использованием уязвимостей и других угроз. При этом контроль доступа к конфиденциальным данным и аутентификация пользователей являются наиболее важными аспектами защиты данных в банковском секторе. В дополнение к этому можно отнести обучение и повышение осведомленности персонала.

Банки также часто обмениваются данными с партнерами, поставщиками услуг и другими финансовыми учреждениями, что является еще одним риском утечки данных, поэтому обеспечение безопасности и конфиденциальности данных при обмене информацией является важной задачей. Соблюдение данных

требований является обязательным для безопасности банковской деятельности, а нарушения могут привести к значительным штрафам. Банки должны постоянно оценивать риски, связанные с утечкой конфиденциальных данных.

Безусловно, одним из важных для ИИ требований являются высокое качество данных, предоставляемых для обучения моделей, ведь если данные неверны или неполны, ИИ в последствии может принимать неверные решения. Также процесс обучения должен сопровождаться экспертами, которые смогут модерировать трек обучения моделей в случае отклонения от требуемых результатов.

Требование к надежной и доступной инфраструктуре для работы ИИ также является одним из препятствий. Необходимо обеспечить ИИ бесперебойной работой и скоростью обработки данных, для чего необходима регулярная поддержка и своевременное обновление.

Стоит также отметить рекомендации, которым должны следовать банки при внедрении ИИ для работы с конфиденциальными данными: необходимость четко определять цели его использования и оценивать потенциальные риски.

Важно перед запуском ИИ провести определенные тестирования полученных результатов, чтобы понять, соответствует ли полученная модель ожиданиям по функционалу, обрабатывает ли запросы точно и непредвзято. Это также включает тестирование на уязвимость и защиту от кибератак.

Персонал, работающий с системами искусственного интеллекта, должен быть обучен работе как с конфиденциальными данными, так и с информационными системами. Он должен понимать принципы защиты данных. Это предполагает обучение персонала работе с данными, сохранности их конфиденциальности и цифровой этике.

Банки и другие финансовые организации также могут сотрудничать с экспертами в области искусственного интеллекта и защиты данных, чтобы получить наилучший опыт и знания по внедрению искусственного интеллекта при работе с конфиденциальными данными. Соблюдение этих рекомендаций позволит бан-

кам и финансовым учреждениям эффективно и безопасно внедрять искусственный интеллект в свою деятельность, что приведет к улучшению в обслуживании клиентов и повышению уровня безопасности.

Использование искусственного интеллекта в банковской отрасли создает значительные риски для сохранности конфиденциальности данных, которые должны быть компенсированы надежными мерами безопасности и передовыми практиками для защиты конфиденциальных данных клиентов и соблюдения нормативных требований.

Список литературы

1. Фомина М.В. Работа коммерческих банков с проблемной задолженностью и методы её оптимизации в условиях цифровизации / М.В. Фомина, А.Ф. Савдерова // Цифровая трансформация государственного и муниципального управления: сборник материалов Всероссийской научно-практической конференции (Чебоксары, 1 июля 2021 года) / ФГБОУ ВО «Чувашский государственный университет им. И.Н. Ульянова». – Чебоксары: Среда, 2021. – С. 141–143. – EDN PVCPFJ.

2. Kondratyeva M.N., Svirina D.D., Tsvetkov A.I. The role of information technologies in ensuring banking security // IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2021. – Т. 1047. – №. 1. – С. 012069.

3. Thisarani M., Fernando S. Artificial intelligence for futuristic banking // 2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC). – IEEE, 2021. – С. 1–13.

4. Scaling gen AI in banking: Choosing the best operating model [Electronic resource]. – Access mode: https://www.mckinsey.com/industries/financial-services/our-insights/scaling-gen-ai-in-banking-choosing-the-best-operating-model (date of application: 05.11.2024).

5. A24 advantages and disadvantages of AI [Electronic resource]. – Access mode: https://www.techtarget.com/searchEnterpriseAI/tip/Top-advantages-and-disadvantages-of-AI (date of application: 05.11.2024).

6. AI & Information Management Report. The Data Problem That's Stalling AI Success [Electronic resource]. – Access mode: https://cdn.avepoint.com/pdfs/en/shifthappens/AI-IM-Whitepaper-v4.pdf (date of application: 05.11.2024).

7. Thousands of servers hacked in ongoing attack targeting Ray AI framework [Electronic resource]. – Access mode: https://arstechnica.com/security/2024/03/thousands-of-servers-hacked-in-ongoing-attack-targeting-ray-ai-framework/ (date of application: 05.11.2024).