УДК 004.8

М. А. Солодуха, З. В. Черноус
Учреждение образования «Полесский государственный университет», Пинск, Республика Беларусь

ЗАРУБЕЖНЫЙ ОПЫТ ВНЕДРЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Введение. Современная информационная безопасность представляет собой сложную и многогранную проблему, требующую постоянного совершенствования и применения передовых технологий. Искусственный интеллект (ИИ) в последнее время приобрел огромное значение в контексте обеспечения безопасности информационных систем в банковской системе. Особенности деятельности банковских систем таковы, что негативные последствия информационных сбоев в работе отдельных банков могут привести к быстрому развитию кризиса на платежном рынке в целом, нанести ущерб интересам собственников и клиентов. Для противостояния таким угрозам, эффективного и своевременного устранения неблагоприятных последствий в банках должен быть обеспечен достаточный уровень информационной безопасности, который необходимо сохранять и поддерживать на постоянной основе. Следовательно, актуальным представляется изучение зарубежного опыта внедрения и использования искусственного интеллекта для обеспечения информационной безопасности.

Основная часть. ИИ-технологии используются в системе мидл-офиса с целью защиты объектов критической информационной инфраструктуры банковского и финансового секторов. В то же время, они могут быть использованы в инструментах кибератак (например, вредоносных программ — malware). Банковские учреждения могут использовать ИИ-технологии как при самостоятельной разработке систем информационной безопасности, так и прибегать к уже готовым решениям, предлагаемым частным сектором. Трудности в использовании ИИ-технологий заключаются как в технологическом аспекте (повышение скорости реагирования и ликвидации источника и последствия таких атак), так и в организационно-правовом. Среди задач развития ИИ следует отметить две, тесно связанные с безопасностью банковского и финансового секторов: разработка и развитие программного обеспечения, в котором используются ИИ-технологии, и создание комплексной системы регулирования общественных отношений, возникающих в связи с развитием и использованием ИИ-технологий [1, с. 250—253].

Указом Президента РФ утверждена стратегия, включающая развитие технологий искусственного интеллекта (ИИ), создание открытых библиотек и программного обеспечения (ПО), направленных на повышение эффективности управленческих процессов, автоматизацию производственных операций, обеспечение безопасности и удовлетворенности клиентов[2]. Сбербанк разработал чат-бот GigaChat с открытой архитектурой, способностью грамотного общения на русском языке, созданием текстов и изображений по описаниям. Банк планирует выложить код нейросети в открытый доступ, что делает его уникальным на рынке [3].

ВТБ банк разработал модель для прогнозирования спроса на услуги в различных точках города с использованием Big Data, что позволяет сократить время доступности отделений для клиентов. Алгоритмы анализируют более 5000 параметров для определения потенциальных клиентов и объемов продаж. Альфа-Банк использовал модель машинного обучения для распознавания несанкционированных операций. Робот оценивает каждую операцию по множеству параметров и быстро реагирует на подозрительные случаи, обеспечивая безопасность транзакций [4].

Великобритания использует модели Archetype, Virgin Money для точного определения потенциальных клиентов, готовых сменить эмитента кредитных карт. Evolution AI помогает Royal Bank of Scotland обнаруживать мошенническую активность при регистрации клиентов, экономя до 200 тысяч часов ежегодно. HSBC запустил AI Markets для улучшения взаимодействия с рынками через NLP, предоставляя институциональным инвесторам более продвинутые инструменты и доступ к данным через различные платформы.

Китай принял программу развития искусственного интеллекта до 2030 года с государственным и частным финансированием. Среди сервисов — Смарт-финансы, интеллектуальное обслуживание, мониторинг и система раннего предупреждения. Южная Корея активно развивает производство чипов для ИИ. Три крупнейшие компании Южной Кореи — Rebellions, Sapeon и FuriosaAI — вносят значительный вклад в эту область. DeepBrain из Южной Кореи создает цифровых банкиров-клонов для консультирования клиентов в банке, снижая нагрузку на реальных сотрудников.

В ближайшие годы в Республике Беларусь планируется практическое внедрение цифровой валюты Национального банка и расширение безналичных платежных инструментов, таких как бесконтактные платежи с использованием NFC, QR-кодов и биометрии. Будут созданы открытые банковские платформы и API для интеграции сторонних финансовых сервисов с инфраструктурой банков, произойдет глубокая модернизация систем электронных платежей и переводов, включая ЕРИП. В целях упрощения удаленного доступа к финансовым услугам получат развитие технологии онлайн-идентификации клиентов и электронной цифровой подписи. Для повышения эффективности банковского надзора запланировано практическое внедрение новых регулятивных технологий SupTech и RegTech на базе инноваций. На уровне банков будет проводиться масштабная цифровизация бизнес-процессов: внутренних операций, анализа данных, клиентского сервиса и др., с особым вниманием к практическим мерам по обеспечению

кибербезопасности финансовой сферы. Реализация Концепции позволит вывести Беларусь в лидеры по уровню цифровизации финансовых услуг и платежной инфраструктуры [2].

Несмотря на уже существующие программные решения с ИИ для обеспечения кибербезопасности банков, следует отметить их относительную примитивность и высокую затратность. Только крупные банки и финансовые учреждения располагают достаточным бюджетом и персоналом для использования ИИ-технологий, в то время как качество выполненных программами заданий еще далеко от идеального. Следующий момент касается уязвимости ИИ перед злонамеренным манипулированием данными (создание фиктивных данных, массовое увеличение данных, замедляющее процессы обработки). В результате инструменты ИИ будут принимать решения, основанные на ложных посылках, и дискредитировать (вплоть до дискриминации) определенных субъектов. Еще одной проблемой может стать взаимосвязанность систем, подключенных к ИИ, а также использование ИИ во вредоносных программах, поражающих информационные системы банков. В итоге решение всех названных проблем лежит в плоскости осуществления постоянного наблюдения специалистов. Как видно из вышесказанного, обеспечение кибербезопасности в условиях внедрения ИИ зависит от ряда условий как технического, так и организационноправового характера. Наряду с проблемами защиты прав и законных интересов субъектов банковских и финансовых отношений возникают проблемы определения вида и пределов ответственности в случае аутсорсинга некоторых процессов и услуг, а также вопросы оценки и управления рисками. Зарубежный опыт использования технологий искусственного интеллекта возникающие в зарубежных странах, еще не находят однозначного решения, что затрудняет расширение сферы применения искусственного интеллекта в банковском секторе.

Список цитируемых источников

1. *Ломакин, Н. И.* Финансовые технологии и искусственный интеллект банковского сектора в новой финансово-технологической экосистеме будущего / Н. И. Ломакин, С. Р. Киселева, И. А. Самородова // Будущее науки-2017 : сб. науч. статей / отв. ред. А. А. Горохов. — М., 2017. — С. 250—253.
2. Концепция развития платежного рынка Республики Беларусь и цифровизации банковского сектора на 2023—2025 годы : постановление Правления Национального банка Республики Беларусь 27.07.2023 № 267. — Режим доступа: https://www.nbrb.by/payment/koncepcija-rasvitija-platioznogo-rinka_2023-2025.pdf//. — Дата доступа: 15.04.2024.
3. *Горян, Э. В.* Институциональные механизмы обеспечения безопасности критической информационной инфраструктуры Российской Федерации и Сингапура: сравнительноправовой аспект / Э. В Горян // Административное и муниципальное право. 2018. —№ 9. — С. 49—60.
4. О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»): указ Президента Российской Федерации от 10 октября 2019 г. №490 СПС «КонсультантПлюс» [Электронный ресурс]. — Режим доступа: https://www.consultant.ru/document/20cons_doc_LAW_335184/ .— Дата доступа: 15.04.2024.

УДК 331.1

И. Х. Тысевич, И. С. Харкевич
Учреждение образования «Барановичский государственный университет», Барановичи, Республика Беларусь

ПРИНЦИПЫ, КРИТЕРИИ И МЕТОДЫ ОЦЕНКИ ОРГАНИЗАЦИИ И НОРМИРОВАНИЯ ТРУДА НА ПРЕДПРИЯТИЯХ РЕСПУБЛИКИ БЕЛАРУСЬ

Введение. Одним из основополагающих факторов, напрямую влияющих на экономическую эффективность деятельности любого предприятия, является организация и нормирование труда. Этот параметр характеризуется процессом анализа трудовой деятельности работников и установлением норм труда для каждого конкретного участка или рабочего места. Обоснованный научными и техническими расчётами подход к управлению численностью персонала и к развитию систем материальной мотивации позволяет минимизировать расходы компаний при гарантированном выполнении планов производства и соблюдении всех стандартов качества. На данный показатель оказывает непосредственное влияние многочисленные производственные факторы: технологии производства, применяемые материалы, степень технологичности оборудования и другие. От организованности данного процесса напрямую зависит удовлетворённость работников условиями труда, которая в свою очередь непосредственно влияет на производительность труда. В связи с этим, появляется необходимость в систематической оценке состояния организации и нормирования труда на предприятиях.

Основная часть. Основные аспекты политики Республики Беларусь в области нормирования труда представлены в статье министерства труда и социальной защиты «Нормирование труда и рекомендации по межотраслевым нормам труда». Помимо этого, организация нормирования труда регламентируется Трудовым кодексом Республики Беларусь, постановлениями и рекомендациями Министерства труда и социальной защиты, решениями органов управления, а также тарифными соглашениями и коллективными договорами [1].

В Трудовом кодексе для регулирования порядка разработки нормативных материалов в статье 87 определены следующие требования:

– наниматель обязан устанавливать нормы труда, обеспечивать их замену и пересмотр с участием профсоюза;