Вестник Томского государственного университета. Право. 2025. № 55. С. 43–59
Tomsk State University Journal of Law. 2025. 55. pp. 43–59

Научная статья
УДК 340.1+342.7
doi: 10.17223/22253513/55/4

Теоретико-правовой анализ рисков внедрения технологий, основанных на искусственном интеллекте, в социально-экономической сфере

Александр Сергеевич Киселев[1]

[1] *Финансовый университет при Правительстве Российской Федерации, Москва, Россия, alskiselev@fa.ru*

Аннотация. Рассмотрены основные риски использования искусственного интеллекта (ИИ) в социально-экономической сфере и меры, которые можно применить для их минимизации. Выявлены следующие риски: исчезновение многих профессий, потеря рабочих мест, уязвимость систем, основанных на ИИ, к хакерским атакам, формирование монополий, дискриминации отдельных граждан и социальных групп и т.д. Рекомендованы правовые методы минимизации рисков внедрения ИИ, определены перспективы дальнейших исследований в данной сфере.

Ключевые слова: государство, искусственный интеллект, право, риски, теоретико-правовой анализ

Для цитирования: Киселев А.С. Теоретико-правовой анализ рисков внедрения технологий, основанных на искусственном интеллекте, в социально-экономической сфере // Вестник Томского государственного университета. Право. 2025. № 55. С. 43–59. doi: 10.17223/22253513/55/4

Original article
doi: 10.17223/22253513/55/4

Theoretical and legal analysis of the risks of introducing technologies based on artificial intelligence in the socio-economic sphere

Aleksandr S. Kiselev[1]

[1] *Financial University under the Government of the Russian Federation, Moscow, Russian Federation, alskiselev@fa.ru*

Abstract. In this paper the main risks of application of artificial intelligence in the socio-economic sphere and measures that can be utilized to minimize them have been considered. The following risks have been identified: disappearance of many professions, loss of jobs, vulnerability of AI-based systems to hacker attacks, formation of monopolies, discrimination of individual citizens and social groups, etc.

Methodology: the work applied general scientific methods of research - analysis, synthesis, induction, deduction, systematic method and method of abstraction, as well as private-scientific methods: comparative-legal and formal-legal.

Legal methods to minimize the risks of AI implementation were recommended, and prospects for further research in this area were identified.

1. Standards (GOSTs) should be created to which AI systems will be obligatorily compliant. These standards should regulate the transparency of operation and contain security protocols for AI-based systems, as well as protect human and civil rights and freedoms. The key principles, in our view, should be security, transparency and respect for human rights and freedoms. Defining ethical standards also involves making decisions about the collection and use of personal data.

2. Any AI-based systems must be understandable not only to operators and programmers, but also to the majority of citizens. Accordingly, it is necessary to develop a scale for assessing the degree of explainability of the functioning of individual AI-based technologies. This can help both the developers themselves and educators in developing appropriate educational programs, advanced training courses and professional retraining.

3. AI operation in experimental mode. It is important that before its direct implementation in any sphere of human activity, developers receive and take into account feedback from users. This approach allows identifying and correcting possible errors, errors in operation that may occur during the operation of the AI.

4. Systematic and continuous monitoring of AI-based systems by the authorities. That is why we should think about creating special interdepartmental expert commissions consisting of specialists in legal, technical, ethical and other issues of AI application.

5. When developing AI systems, the socio-cultural characteristics and needs of each particular community must be taken into account.

We believe that the following laws are needed: on transparency of algorithms to ensure that they work in various sectors of the economy from commerce to social services; on the verification of the proper functioning, whereby AI should be available for systematic auditing and monitoring to ensure that it works properly and complies with government standards; on non-discrimination; and on fair distribution of AI-based high-tech to all members of society.

Keywords: state, artificial intelligence, law, risks, theoretical and legal analysis

For citation: Kiselev, A.S. (2025) Theoretical and legal analysis of the risks of introducing technologies based on artificial intelligence in the socio-economic sphere. *Vestnik Tomskogo gosudarstvennogo universiteta. Pravo – Tomsk State University Journal of Law.* 55. pp. 43–59. (In Russian). doi: 10.17223/22253513/55/4

Введение

Искусственный интеллект (ИИ) в последние десятилетия стал неотъемлемой частью нашей повседневной жизни. Его применение простирается от автоматизации промышленного производства до медицины, финансов и создания произведений искусства. Технологии, основанные на элементах ИИ, могут принести многочисленные блага в развитии многих отраслей производства и положительно повлиять на сферу оказания социальных услуг. Вне всякого сомнения, технологии, основанные на элементах ИИ, могут дать нам новые решения ключевых проблем общества, таких как преступность, безработица, загрязнение природы, неэффективное использование ресурсов, и т.д. Но они также сопряжены с определенными рисками, вызывая серьезное беспокойство по поводу возможных негативных последствий. Применение искусственного интеллекта, особенно в социально-экономических отношениях, рискованно. Но этот риск поддаётся расчёту и сокращению.

А отказываться или отставать от конкурентов в применении столь перспективных инструментов, как ИИ, тоже рискованно. В данной статье мы рассмотрим некоторые из этих рисков, оценим возможные неблагоприятные последствия и предложим правовые методики их минимизации.

О рисках и угрозах внедрения ИИ в социально-экономическую сферу

Развитие технологий искусственного интеллекта и внедрение их в жизнь несут не только положительные эффекты, но также и определённые риски. Одним из часто упоминаемых социально-экономических рисков является угроза безработицы [1. С. 330]. Так как ИИ автоматизирует многие задачи, ранее выполнявшиеся людьми, это может привести к резкому сокращению потребности в рабочей силе во многих отраслях экономики [2]. Многие профессии, особенно те, которые требуют низкой квалификации и предполагают несложные механические действия (погрузчик, фасовщик, продавец, кассир), могут быть заменены автоматизированными системами, основанными на ИИ. К примеру, кассиры в супермаркетах уже заменяются системами самообслуживания, а курьеры – беспилотными доставочными роботами. Уже существуют роботы-повара и роботы-парикмахеры, дизайн и многие прикладные творческие функции ИИ выполняет быстрее и порой качественнее человека. Генерация текстов и изображений, уборка улиц, перевозка в такси и многие другие сферы уже подвергаются автоматизации с использованием новых технологий, основанных на программах ИИ. Такие профессии, как художник, писатель, переводчик, дизайнер, обычно относятся к творческим. Однако, как показывает практика, современный ИИ способен обучиться на накопленном материале и выполнять такие функции вполне успешно. Ведь, на самом деле, и люди «творят» по тому же принципу: по-новому организуя уже имеющиеся образцы.

Приведем статистическую информацию. С начала «кассовой реформы» в нашей стране количество онлайн-касс выросло в 2,5 раза – до 3,6 млн штук. Через них проводится более 200 млн операций в сутки. Сумма ежедневной выручки по онлайн-кассам составляет около 130 млрд руб. [3]. Подобная тенденция будет продолжаться и дальше. Электронные кассы не допускают ошибок, они во многом удобнее для потребителя и экономически оправданы для супермаркетов, если стоимость их обслуживания ниже зарплат людей, выполняющих те же функции в том же объёме. Со временем, когда стоимость установки электронной кассы снизится настолько, что любой индивидуальный предприниматель сможет позволить себе её приобрести, вопрос о целесообразности существования профессии кассира будет разрешён в пользу машины. По прогнозам, прежде всего, начнут «исчезать» кассиры в продуктовых супермаркетах, затем в других учреждениях сферы услуг. Некоторые исследователи говорят о высоком вреде этой профессии для здоровья, отмечая, что «величина двигательной активности сотрудников, занимающих должности “заместитель директора” и “продавец-кассир”, может быть охарактеризована как очень высокая (чрезмерная)» [4. С. 46].

Во время пандемии новой коронавирусной инфекции в 2019–2021 гг. нагрузка на продавцов-кассиров, мерчандайзеров, работников торгово-выставочного зала постоянно росла. При этом росла доля онлайн-заказов – как следствие необходимости соблюдать ограничительные меры. Ввод касс самообслуживания был очевидным, и, как показала практика, рентабельным решением. Данная практика наблюдалась как в сетевых супермаркетах России, так и в алогичных магазинах большинства развитых стран, испытавших серьёзное воздействие пандемии COVID-19. Иными словами, руководство компаний сознательно проводило такие меры во избежание падения уровня доходов сети. Похожим образом коронавирус изменил и некоторые другие вещи в нашей жизни, поспособствовав более интенсивному вводу различных элементов самообслуживания, оказав влияние на весь рынок услуг. Кроме того, во время пандемии выросло число работающих удалённо. Многие из этих сотрудников и после отмены ограничений остались в удалённом режиме работы, что также меняет рынок труда, ещё более увеличивая роль цифровых технологий в экономике.

Сегодня существует реальная угроза исчезновения профессии курьера-доставщика – профессии, ставшей популярной и даже необходимой во время пандемии. Для России в этом плане актуален опыт компании «Яндекс», которая уже с 2015 г. занимается реализацией проекта по внедрению так называемых роверов – роботов-доставщиков. Роверы – это компактные и автономные роботы, созданные специально для доставки предметов в условиях городской среды. Их оснащение включает современные датчики, такие как лидары, камеры и радары, которые обеспечивают точную навигацию и обнаружение препятствий. Информация с датчиков обрабатывается искусственным интеллектом «ровера», самостоятельно принимающим решения об изменении маршрута. Благодаря этим системам роверы безопасно передвигаются по городским улицам и избегают столкновений [5. С. 262]. Они отлично показывают себя в городских условиях, и, несмотря на имеющиеся проблемы, с каждым годом их системы навигации и технические характеристики постоянно улучшаются.

Представители компании заверяют, что «в будущем роботы-доставщики станут неотъемлемой частью индустрии доставки, улучшая нашу жизнь и повышая эффективность процесса доставки». При этом «Яндекс» заявляет, что стоимость доставки снизится, поскольку не надо будет платить зарплату курьерам. Данное обстоятельство потенциально выгодно и для компании, и для клиентов. При сохранении этих тенденций и темпов роста технологий, профессия доставщика через несколько лет исчезнет [6]. Стоит отметить, что для доставки сейчас применяются и управляемые оператором небольшие и дешёвые беспилотные летательные аппараты – компромиссный вариант между доставкой человеком и самостоятельной машиной.

Возможные последствия полной автоматизации обслуживания клиентов продуктовых магазинов и замены курьеров-людей курьерами-роботами предполагают рост безработицы и увеличение социального неравенства. Люди, потерявшие свою работу из-за применения ИИ, могут столкнуться с

трудностями в поиске новой профессии, особенно если их навыки устарели, а времени и денег на получение новой профессии у них нет. Кроме того, растущая безработица может привести к экономическому спаду и ещё больше усилить социальное неравенство в обществе.

Искусственный интеллект даёт новые инструменты и для противоправной деятельности. Сегодня он уже массово используется для создания и распространения самой разной информации, в том числе фальшивой. В последние годы в нашу жизнь вошли так называемые дипфейки (от англ. deep – «глубокий» и «fake» – подделка) – продукты программ, основанных на ИИ, представляющие собой фальшивые, но крайне реалистичные видео- и аудиоматериалы, которые могут быть использованы для манипуляции общественным мнением или совершения преступлений. Например, фальшивые новостные репортажи, созданные с помощью ИИ, могут привести к распространению недостоверной информации и падению доверия к СМИ в целом как к источнику информации.

Опаснейшим результатом такого применения ИИ могут стать социальные конфликты, в том числе и вооружённые, если вовремя и эффективно не пресечь распространение недостоверной информации. Специалисты по этому вопросу заявляют, что борьба с фальсификацией и манипуляцией информацией становится всё сложнее, поскольку ИИ развивается и становится все более совершенным. Н.Р. Красовская и А.А. Гуляев в своем исследовании обращают внимание, что «с каждым годом всё большее место среди дипфейков занимает политическая продукция. Тревогу по этому поводу начали бить в 2017 г., отмечая, что политические дипфейки могут повлиять на исход выборов, вызвать панические настроения в стране. Основой действия политических дипфейков являются техники манипулирования людьми. Копии изображения политического деятеля или видео оказывают психологическое воздействие на зрителя. Это воздействие будет тем больше, чем меньше зритель сомневается в подлинности изображения или видео. В психологическом инструментарии воздействия на индивидуальное и массовое сознание одну из главных ролей играют техники манипулирования, лежащие в основе концепции “подталкивания” человека к нужному для манипулятора поведению. Эти техники создают у человека ложную иллюзию свободы и самостоятельности в принятии решений» [7. С. 94].

Дополняя мысли данных авторов, отметим, что подобные манипуляции могут быть гораздо более вариативными. Основная вредоносная цель такой деятельности – дестабилизация общества через разжигание социальной вражды между представителями различных религий и конфессий, представителями конкурирующих компаний или представителями одной сферы бизнеса, между другими социальными группами. В принципе совершенно неважно, какие социальные слои общества будут затронуты. Главные средства, которые использует манипулятор, распространяющий дипфейк, – высокая скорость распространения информации и её психологический характер. Манипуляция работает успешно в тот момент, когда человек не может критически мыслить и поддается влиянию эмоций, не обращает внимания

на детали, несостыковки, которые в обыденном состоянии нелегко заметить и идентифицировать видео как подделку. Именно поэтому дипфейкмейкеры стараются сделать эмоционально насыщенные видео с нарочито примитивным сленгом, что придаёт им в глазах целевой аудитории реализм. В случае если такие видео не блокировать и не делать своевременное опровержение, манипулятор достигнет цели, вызвав социальные волнения и вражду. Сложным, но наиболее эффективным способом борьбы с распространением вредоносной фальшивой информации является повышение общего уровня критического мышления населения через повышение качества всеобщего образования. Также важно, чтобы государство мгновенно реагировало на подобную информацию, убедительно опровергая её и доказывая её фальшивость.

Другим риском работы ИИ с информацией является возможность нарушения конфиденциальности данных [1. С. 330–331]. Применение программ, основанных на элементах ИИ, в социальной сфере сопряжено со сбором и обработкой больших объёмов персональных данных. Теоретически, при наихудшем сценарии, это может привести к нарушению конфиденциальности и безопасности этих данных. Хакеры и злоумышленники могут использовать слабые места в системах ИИ для получения доступа к конфиденциальным данным граждан, секретной информации бизнеса и государства.

Потеря персональных данных может повлечь за собой серьёзные последствия, включая кражу финансов, секретной и личной информации, шантаж со стороны злоумышленников, посягательства на честь, достоинство и деловую репутацию и т.д. Исследователи считают, что «термин “кража личности” (англ. Identity theft), получивший распространение в начале 2000-х гг., представляет собой такое преступное посягательство, при котором незаконно используются персональные данные человека для получения материальной выгоды, т.е. противоправно обладая персональной или финансовой информацией другого человека, злоумышленник использует их в своих целях, при этом действуя от его имени пострадавшего» [8. С. 18].

Стоит сделать оговорку, что так называемая кража личности – это не совсем корректный перевод с английского языка. Речь, разумеется, идёт о краже удостоверяющей информации, которая относится к определённому человеку. Личность предполагает наличие уникальных и персонифицированных качеств, такие как чувства, мысли, характер, поведение и прочее. Вполне очевидно, что саму личность украсть невозможно, а вот получение конфиденциальной информации позволяет злоумышленнику эксплуатировать имя человека, его социальное и экономическое положение. Собственно, именно этим и пользуются многочисленные мошенники, получая доступ к чужим аккаунтам. Распространены ситуации, при которых злоумышленники создают правдоподобных цифровых двойников. С учётом возможностей дипфейков и быстрого развития ИИ, отличить их от оригинала в краткосрочный период времени будет практически невозможно.

Искусственный интеллект уже применяется крупными банками для принятия решений, таких как выдача кредитов или определение уровня страхо-

вого покрытия. Ошибка или сбой работы ИИ здесь может привести к необоснованным или дискриминационным решениям, основанным на неправильной интерпретации данных. Во избежание подобных ситуаций требуются системы проверки, обжалования и отмены таких решений.

К другим рискам использования ИИ может привести тот факт, что искусственный интеллект может совершенно неожиданным образом воспринимать отдельные явления и ситуации, в которых люди принимают решения, опираясь на морально-этические или правовые нормы. Искусственный интеллект, не имеющий подобных ограничений или воспринимающий их не так как человек, может принимать логические, но неприемлемые для общества решения.

В ближайшем будущем возможно появление новых видов кибератак, направленных на системы искусственного интеллекта и использующих их уязвимости. Например, ИИ может быть настроен или перепрограммирован на осуществление дискриминации или нарушение конфиденциальности данных пользователей. К примеру, если руководство социальной сети оставит право за ИИ блюсти режим персональных данных, то это может стать основой для возможных противоправных действий. Особое внимание нужно сосредоточить на том, кто будет обучать ИИ и каким образом это будет происходить, какие ограничения и способы контроля будут разработаны, а также применены в случае нарушения режима безопасности персональных данных.

Однако, ИИ может помочь и лучше защитить информацию. Как отмечают Е.А. Долгочуб и А.Н. Поликанин «шифрование электронной информации необходимо не только для того, чтобы держать некоторую информацию в секрете от других, но и является ключевой частью таких технологий, как криптовалюты, такие как биткойн. Кроме того, скандалы вокруг широко распространенного подслушивания разведывательных служб показали миру, что на самом деле ни одна из используемых сегодня процедур не является действительно безопасной» [9. С. 79].

Для максимальной защиты от таких рисков необходимо строгое соответствие стандартам безопасности и внедрение передовых технологий шифрования. Одной их таких технологий является квантовое шифрование.

Современные методы шифрования (RSA) основаны на простых математических операциях с использованием «ключей», неизвестных стороннему пользователю. Теоретически их можно подобрать, но эта процедура может потребовать неприемлемого количества времени. Однако «как только будет создан квантовый компьютер, состоящий из 1 000 кубитов и более, вся информация, зашифрованная алгоритмом RSA, будет моментально скомпрометирована, что поставит под угрозу информационную безопасность общества» [10]. Квантовая криптография сделает в принципе невозможными взлом и утечку информации.

В названии метода квантовой криптографии отражается его суть: использование поляризованных фотонов света для шифрования информации. Е.А. Долгочуб и А.Н. Поликанин указывают, что алгоритмы квантового

шифрования уже применяются в зарубежных системах государственного управления, например, «штат Женева в Швейцарии уже использует квантовую криптографию на выборах в течение десяти лет», подобные технологии финансируются правительством КНР и являются приоритетными для стран Европы и США… С приходом на свободный рынок квантовых компьютеров традиционная криптография устареет», так как «совмещение квантовых алгоритмов шифрования с математическими может дать устойчивый к атакам метод шифрования» [9. С. 82–83].

Стоит отметить, что актуальная практика методов защиты и похищения информации должна быстро находить отражение в действующем законодательстве.

Следующим риском является тот факт, что частные компании или государство в некоторых аспектах работы могут полностью доверять и полагаться на искусственный интеллект при принятии решений в социально-экономической деятельности. Сбои в системе или недоступность технологии ввиду хакерской атаки могут привести к значительным проблемам, в том числе глобального характера.

Другим минусом повсеместного внедрения ИИ в социальную сферу считается риск роста зависимости индивидов и организаций от технологий и сокращение вовлечённости и влияния человека на различные процессы. Это может привести к потере гуманизма и недостатку коммуникации, так как ИИ не обладает эмоциональным интеллектом и способностью эмпатии, что является важным аспектом социальной работы.

Следующим важным риском применения ИИ в социально-экономической сфере является возможность формирования новых монополий и нарушения распределения ресурсов. Искусственный интеллект может дать преимущество крупным игрокам, которые могут иметь доступ к большему объёму данных и ресурсов для улучшения своей деятельности. Передовые технологии, основанные на ИИ, как правило, являются дорогостоящими и недоступными для широкой аудитории. Разработчики, получающие крупные гранты или госзадания на их разработку, как правило, передают исключительные права на использование изобретения, соответственно, они не имеют права использовать технологию и им самим выгодно реализовать свой результат интеллектуального труда как можно дороже согласно условиям рынка. Заказчиком в этом случае выступает либо государство, имея монополию на использование соответствующего НИР, направляя данную технологию для реализации государственно важных задач в экономике или для обеспечения информационной безопасности, либо крупная коммерческая компания, которая, несомненно, не будет заинтересована в распространении данной технологии, так как она является конкурентным преимуществом перед другими участниками рынка.

Если технология, основанная на ИИ, может в разы повысить скорость операций, улучшить производительность выпускаемого компанией товаров,

то это может привести к появлению новых монополий, что порождает проблемы с конкуренцией и стимулирует значительное перераспределение ресурсов, денег и власти.

Чтобы нивелировать данные риски, необходимо на государственном и международном уровнях разработать эффективные правила и нормы использования уникальных технологий, основанных на ИИ, которые могут стать средством монополизации определенной экономической сферы или всего рынка целиком одной или несколькими компаниями с целью предотвращения формирования новых монополий и обеспечения равных возможностей для всех игроков на рынке.

Для сведения к минимуму новых рисков в экономической сфере, необходимо создать стройную и прозрачную систему правил и нормативных требований, которая будет регулировать применение ИИ. Важно выстроить законодательство, которое будет регулировать максимальный объём и порядок использования данных. Также государству, возможно, следует регулировать цены на технологии, которые могут поставить большую часть игроков в заведомо невыгодное положение, а также иными способами содействовать созданию равных условий для всех участников экономической системы. Одновременно с этим следует уделить максимальное внимание обучению как будущих, так и действующих специалистов правилам этики использования ИИ. Любой человек, вне зависимости от сферы своей деятельности в будущем, обязан знать, каковы будут последствия неправомерного использования технологий, основанных на ИИ, и ответственность, которую он понесёт в случае нарушения норм права. Обучение таким правилам целесообразно осуществлять на всех уровнях и направлениях образования.

Одним из мировых лидеров в гонке цифровых технологий является КНР [11. С. 88], где государство занимается контролем кибербезопасности, развитием ИИ и правовым сопровождением этих процессов с 1986 г., когда была принята «Национальная программа исследований и разработок в области высоких технологий» («программа 863») [12. С. 55]. С 2003 г. начала реализовываться друга программа по обеспечению государственной информационной безопасности «Золотой щит». Китайские власти получили посредством реализации данного проекта практически полный контроль не только над китайским национальным сегментом Интернета, но и надо всей информационной сетью страны. Власти КНР имеют возможность контролировать деятельность всех компаний, индивидуальных предпринимателей и граждан в сфере информационных технологий. Стоит обратить внимание, что «Золотой щит» является первым из нескольких «золотых проектов» по контролю различных важных областей жизни страны. Система «Золотого щита» располагает ранжированными по гражданской благонадёжности списками жителей страны, которые легли в основу системы «социального рейтинга». Эта же система контролирует камеры наружного наблюдения, расположенные по всей стране с целью сообщений о правонарушениях, разграничивает китайский и зарубежный Интернет, блокирует СМИ, критикующие власть КНР, и пропаганду насилия, блокирует нежелательные доменные имена и IP-адреса.

С 2014 г. в КНР началась реформа национальных проектов и законодательства, относящихся к сфере цифровых технологий. В 2016 г. был принят 13-летний план экономического и социального развития КНР, в котором важное место отводится информационным технологиям нового поколения: обозначены конкретные инженерные и организационные действия по развитию сети и совершенствованию системы безопасности. С 2017 г. с той же целью в КНР действует закон о кибербезопасности.

В КНР существует национальный департамент кибербезопасности, контролирующий вышеуказанную деятельность. Кроме того, на уровне регионов для этого создаются специальные подразделения муниципальных органов власти.

Для доступа в сеть все граждане КНР обязаны проходить аутентификацию: предоставлять настоящие данные о своей личности. Эта простая мера иногда обсуждается и в других странах (в том числе в России), и в недалёком будущем, вероятно, будет введена повсеместно.

М.Г. Бреслер, А.В. Сердюк и А.Р. Сулейманов указывают, что при всех этих мерах вопросы регулирования искусственного интеллекта в КНР оставались открытыми до 2017 г., в котором было принято сразу несколько важных для этой отрасли документов, и до 2025 г. планируется сделать ИИ главной движущей силой преобразований в промышленности и в обществе. Однако указанные авторы считают, что в КНР пока недостаточно для этого технических средств, технологий и специалистов, что преодолевается как собственными усилиями, так и с помощью зарубежных наработок [12. С. 58–59].

Находясь вне КНР, трудно оценить, насколько хорошо работают все перечисленные меры, в том числе потому, что они работают («Золотой щит» и другие ограничения). Однако тот факт, что иностранные компании, желающие работать в КНР или поставлять туда свою продукцию, подчиняются требованиям правительства этой страны и вносят требуемые правки в свою продукцию, показывает, что в какой-то мере власти КНР своих целей достигают.

В других развитых странах эти процессы также находятся в стадии становления, с учётом местного уровня развития технологий и политических режимов. Более того, сегодня даже определения ИИ отличаются в разных правовых системах [11. С. 87–88].

В Европейском союзе существует необходимость учёта интересов государств-членов с разным уровнем развития экономики. Схожая ситуация и в США, где штаты обладают значительной автономией в правовой и экономической деятельности, поэтому в США нет общенационального законодательства о многих важнейших элементах технологий ИИ [12. С. 95]. Кроме того, в США традиционно значительное участие в разработке передовых технологий принимают Министерство обороны и разведывательное сообщество. Поэтому многие технологии и практики применения новейших технологий носят военный характер и засекречены [1. С. 324–325]. В период своего президентства Д. Трамп поставил целью для США достижение лидерства в технологиях ИИ. Для этого меняется законодательство и создаются специальные правительственные структуры. Также предполагается

финансирование исследований, сотрудничество с союзниками, создание максимально лояльного к разработчикам законодательства. Министерство обороны играет важнейшую роль в этих процессах, так, правительство США рассматривает ИИ в первую очередь как инструмент обеспечения национальной безопасности.

Для эффективного развития и внедрения ИИ и обеспечения безопасности, важно исследовать опыт всех, без исключения, участников этой деятельности. Однако более ценен опыт стран, чья экономическая и политическая системы в наибольшей степени схожи с отечественными. А так как полностью идентичных экономик и обществ всё-таки не существует, то просто копировать чужой опыт не получится – он должен быть адаптирован под отечественные условия.

Методики минимизации рисков применения ИИ

Внедрение искусственного интеллекта в социально-экономические отношения должно, по нашему мнению, сопровождаться следующими мерами по минимизации возможных рисков:

1. Необходимо создавать регламенты и стандарты (ГОСТы), которым должны соответствовать системы искусственного интеллекта. Эти стандарты должны регулировать прозрачность функционирования и содержать протоколы безопасности систем, основанных на ИИ, а также защищать права и свободы человека и гражданина. Они также должны включать в себя соблюдение принципов справедливости, непротиворечивости, непричинения вреда и уважения к человеку и человеческому достоинству. Некоторые компании (Tesla, Amazon) уже начинают создавать корпоративные стандарты для работы с ИИ, Евросоюз идёт по пути стандартизации данных технологий. Не вызывает сомнений тот факт, что разработка этических стандартов искусственного интеллекта является крайне важной задачей на текущем этапе.

Ключевыми принципами, на наш взгляд, должны стать безопасность, прозрачность и уважение к правам и свободам человека. Определение этических стандартов также подразумевает принятие решений о сборе и использовании персональных данных. Искусственный интеллект способен обрабатывать большие объёмы данных, и это может подразумевать потенциальное нарушение режима конфиденциальности и прав человека на приватность. Поэтому необходимо разработать строгие правила относительно сбора, хранения и использования данных.

Так, например, сегодня системы ИИ имеют доступ к большому объему личной информации, например, личным данным пациентов поликлиник и больниц. К примеру, чат-боты, функциональные помощники нередко собирают персональные данные. Хотя данные обезличены и часто не раскрывают личности людей, ИИ все равно собирает и сохраняет информацию, которая в теории может быть скомпрометирована. Пользователи должны быть в курсе того, какие данные собираются системами, основанными на ИИ, как

они используются и как влияют на принимаемые решения. Особенно если речь идёт о здоровье пациентов. В то же время государство должно поощрять развитие средств безопасности ИИ разработчиками, и коммерческими организациями, а также способствовать распространению наиболее успешных практик.

2. Любые системы, основанные на ИИ, должны быть понятными не только для операторов и программистов, но для большинства граждан. К примеру, визуализация процессов может помочь проще понять, как работает тот или иной алгоритм. Помимо этого, целесообразно выявлять и фиксировать признаки, которые влияют на принятие решений ИИ. Разумеется, стоит задуматься о разработке шкалы для оценки степени объяснимости функционирования отдельных технологий, основанных на ИИ. Это может помочь как самим разработчикам, так и педагогам при разработке соответствующих образовательных программ, курсов повышения квалификации и профессиональной переподготовки.

3. Работа ИИ в экспериментальном режиме. Важно, чтобы перед его непосредственным внедрением в любую сферу жизнедеятельности человека, разработчики получали и учитывали обратную связь от пользователей. Такой подход позволяет выявить и исправить возможные ошибки, погрешности в работе, которые могут возникнуть в ходе эксплуатации ИИ.

4. Осуществление систематического и постоянного мониторинга систем, основанных на ИИ, со стороны органов власти. Например, в США в 2018 г. создана Комиссия национальной безопасности по искусственному интеллекту (NDAA), которая оценивает последствия использования ИИ для безопасности США, включая этическую сторону вопроса. Специальные органы со схожими функциями создают и наиболее развитые штаты [1. С. 328]. Именно поэтому нам стоит задуматься о создании специальных межведомственных экспертных комиссий, состоящих из специалистов по правовым, техническим, этическим и иным вопросам применения ИИ. Основная цель данных комиссий, на наш взгляд, должна состоять не только в оценке соответствия ИИ правовым нормам, но и учитывать возможные технические риски.

5. При разработке систем ИИ необходимо принимать во внимание социокультурные особенности и потребности каждого конкретного сообщества. К примеру, должны быть исключены возможные риски нарушения религиозных норм и культурных ценностей народов, отдельных социальных групп граждан, что поможет предотвратить любые формы дискриминации. Данный вопрос лежит в этическом поле и должен решаться как конкретными странами, так и религиозными, и этническими группами населения. Вполне возможно, что для установления общих этических норм применения ИИ будет достаточно издания соответствующего национального закона, но в других случаях может потребоваться и международно-правовое регулирование, если вопросы будут касаться, например, этики и морали мировых религий.

Очевидно, что вполне вероятна ситуация, когда ИИ будет «придерживаться» определённых политических, религиозных, идеологических взглядов, предпочитать какой-либо пол, нацию, расу, культуру и т.д. Это связано

с тем, что ИИ обучается на определённых разработчиками сегментах доступной информации. Нейронные сети и алгоритмы машинного обучения могут подвергаться влиянию предубеждений и предрассудков и со стороны самих разработчиков, что может привести к умалению прав, оскорблению и неравным возможностям для людей различных социальных групп. Так, например, несмотря на нерешённость этических вопросов, ИИ уже применятся в США для вынесения судебных решений: программа COMPAS вынесла обвинительное заключение по делу Э. Лумиса (дело с отсутствием прямых улик). Подсудимый обжаловал это решение, но Верховный Суд США оставил решение в силе [13]. В Евросоюзе также уделяется колоссальное внимание вопросам этики применения искусственного интеллекта [14].

Всё это может привести к социальным конфликтам, особенно в обществах, сильно отличающихся от тех, в которых создан конкретный продукт ИИ. Поэтому этические стандарты должны быть максимально общими и не зависеть от мнения и убеждений разработчиков ИИ и лиц, осуществляющих непосредственный контроль за использованием этих технологий.

Сами разработчики ИИ будут стремиться не допустить подобных ситуаций, только если они считают это необходимым или заинтересованы в этом. В ситуации международных конфликтов вполне вероятно применение инструментов даже «мирного» ИИ для разрушительного воздействия на противника. Поэтому все технологии ИИ, внедряемые в экономику и общество, должны в обязательном порядке дорабатываться или ограничиваться специалистами применяющего их государства.

Вне всякого сомнения, закон создает предпосылки для активизации исследований в области искусственного интеллекта [15]. Полагаем, что необходимо принятие следующих законов, регулирующих данную сферу общественных отношений:

– о прозрачности алгоритмов. Согласно данному закону, соответствующие алгоритмы и модели роботов, обеспечивающие работу в различных секторах экономики – от торговли до сферы социальных услуг, должны быть доступны для проверки и анализа;

– проверке надлежащего функционирования, в соответствии с которым ИИ должен быть доступен для систематического аудита и контроля для обеспечения его надлежащей работы и соответствия государственным стандартам;

– недопустимости и предотвращении дискриминации, по которому ИИ в процессе функционирования не должен ущемлять права людей на основе расы, пола, возраста, инвалидности, религиозных воззрений, национальности или по иным основаниям;

– справедливом распределении высоких технологий, основанных на ИИ, для всех членов общества, независимо от их социального статуса, финансовых возможностей или других факторов.

Заключение

Применение искусственного интеллекта в социально-экономической сфере предполагает появление новых мощных инструментов, способных

улучшить жизнь всего общества. Однако необходимо учитывать и серьёзные риски, которые несут данные технологии. Безработица, фальсификация с помощью дипфейков, нарушение режима конфиденциальности данных, новые виды мошенничества, отсутствие этического кодекса ИИ и правоприменительной практики, связанной с внедрением и функционированием ИИ в социально-экономической сфере, – всё это вызовы, перед которыми уже сегодня стоит наше общество.

Разработчики защитного программного обеспечения, исполнительные и законодательные органы власти должны стараться сбалансировать потенциальные выгоды ИИ с защитой интересов государства, с одной стороны, прав и законных интересов граждан – с другой. Только в таком случае мы сможем максимально использовать преимущества ИИ в социально-экономической сфере, сталкиваясь с минимумом негативных эффектов.

В настоящей работе мы раскрыли как потенциальные возможности, так и риски использования ИИ. Среди основных рисков можно назвать: потенциальное исчезновение многих профессий, и, соответственно, потерю рабочих мест, уязвимость систем, основанных на ИИ, к хакерским атакам, формирование монополий, возможность дискриминации отдельных граждан и групп людей и т.д. Однако правовое регулирование использования ИИ, несомненно, поможет снизить эти риски и максимизировать преимущества. Для достижения данной цели необходимо принятие ряда законов, создание образовательных программ и программ повышения квалификации, профессиональной переподготовки. Для этой сферы важно также сосредоточиться на вопросах информационной безопасности. В целях общественной и государственной безопасности необходимо предотвратить формирование монополий, использующих передовые ИИ.

Ситуация с внедрением ИИ в жизнь общества уникальна тем, что требует от законодателя широкого сотрудничества с техническими специалистами, научным сообществом, общественностью, бизнесом.

Промедление в развитии ИИ и создании соответствующей правовой базы может привести к отставанию в техническом развитии от других стран, а также к серьёзным проблемам в экономике и обществе [16]. Опасно применять зарубежные продукты ИИ в исходном виде, без проверки и доработки специалистами применяющего их государства. Это значит, что специалисты по безопасности ИИ должны быть в каждой стране, использующей эти технологии. Следует также учиться на зарубежном опыте обеспечения цифровой безопасности и применять работающие процедуры, опять же, после национальной доработки. Опыт других стран позволит значительно ускорить данные процессы.

Список источников

1. Бирюков П.Н. Деятельность США в сфере использования искусственного интеллекта // Вестник ВГУ. Серия: Право. 2019. № 3 (38). С. 324–334.

2. Matjaž P., Mahmut O., Janja H. Social and juristic challenges of artificial intelligence // Nature. 2019. Vol. 5. URL: https://www.nature.com/articles/s41599-019-0278-x

3. Официальный сайт «Оборот.ру». Количество онлайн-касс в России с начала кассовой реформы выросло в 2,5 раза. URL: https://oborot.ru/news/kolichestvo-onlajn-kass-v-rossii-s-nachala-kassovoj-reformy-vyroslo-v-25-raza-i136191.html

4. Степанова О.Н., Асадова С.З. Двигательная активность и нервно-эмоциональная напряжённость труда сотрудников предприятий розничной торговли как ориентиры для проектирования программ корпоративной физкультурно-спортивной работы // Наука. Управление. Образование. РФ. 2023. № 1 (9). С. 37–47.

5. Пономарев Д.А., Королева А.Г., Шамаева И.И. Колесные роботы в сфере доставки // Наука и образование в условиях мировой нестабильности: проблемы, новые этапы развития : материалы II междунар. науч.-практ. конф. Ч. 1. Ростов н/Д : Манускрипт, 2022. С. 262.

6. Блог Яндекса «Ровер – робот-курьер». URL: https://yandex.ru/blog/company/yandeks-rover-robot-dostavschik

7. Красовская Н.Р., Гуляев А.А. Технологии манипуляции сознанием при использовании дипфейков как инструмента информационной войны в политической сфере // Власть. 2020. № 4. С. 94.

8. Атагимова Э.И., Потемкина А.Т., Цопанова И.Г. «Кража личности» как самостоятельное преступление или разновидность мошенничества // Правовая информатика. 2017. № 3. С. 18.

9. Долгочуб Е.А., Поликанин А.Н. Технологии квантовой криптографии // Интерэкспо Гео-Сибирь. 2021. Т. 6. С. 78–83.

10. Шемякина М.А. Анализ использования квантовых технологий в криптографии // Международный журнал гуманитарных и естественных наук. 2019. № 5-4. С. 59–62.

11. Асадуллина А.В., Белоусов В.С. Глобальные тренды в развитии и регулировании технологий искусственного интеллекта // Российский внешнеэкономический вестник. 2023. № 9. С. 86–104.

12. Бреслер М.Г., Сердюк А.В., Сулейманов А.Р. Специфика регулирования IT-индустрии в Китае: история и современность // Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика. 2021. № 4 (38). С. 53–62.

13. Сайт «Хайтек». Алгоритм для вынесения приговоров обвинили в предвзятости. URL: https://hightech.fm/2016/06/28/compas_bias

14. Асадуллина А.В., Белоусов В.С. Регулирование технологий искусственного интеллекта на территории Европейского Союза // Российский внешнеэкономический вестник. 2022. № 8. С. 20–35.

15. Mervis J. U.S. law sets stage for boost to artificial intelligence research // Science. 2021. Vol. 371, № 6525. URL: https://www.science.org/doi/10.1126/science.371.6525.112

16. Neil S. The race to the top among the world's leaders in artificial intelligence // Nature. 2020. URL: https://www.nature.com/articles/d41586-020-03409-8

References

1. Biryukov, P.N. (2019) Deyatel'nost' SShA v sfere ispol'zovaniya iskusstvennogo intellekta [US activities in artificial intelligence]. *Vestnik VGU. Seriya: Pravo*. 3(38). pp. 324–334.

2. Matjaž, P., Mahmut, O. & Janja, H. (2019) Social and juristic challenges of artificial intelli-gence. *Palgrave Commun*. 5(61). DOI: 10.1057/s41599-019-0278-x

3. *Oborot.ru.* (2021) Kolichestvo onlayn-kass v Rossii s nachala kassovoy reformy vyroslo v 2,5 raza [The number of online cash registers in Russia has increased by 2.5 times since the beginning of the cash register reform]. 26th May. [Online] Available from: https://oborot.ru/news/kolichestvo-onlajn-kass-v-rossii-s-nachala-kassovoj-reformy-vyroslo-v-25-raza-i136191.html

4. Stepanova, O.N. & Asadova, S.Z. (2023) Dvigatel'naya aktivnost' i nervno-emotsional'naya napryazhennost' truda sotrudnikov predpriyatiy roznichnoy torgovli kak

orientiry dlya proektirovaniya programm korporativnoy fizkul'turno-sportivnoy raboty [Physical activity and neuro-emotional stress of employees of retail enterprises as guidelines for designing corporate physical education and sports programs]. *Nauka. Upravlenie. Obrazovanie*. 1(9). pp. 37–47.

5. Ponomarev, D.A., Koroleva, A.G. & Shamaeva, I.I. (2022) Kolesnye roboty v sfere dostavki [Wheeled robots in delivery]. *Nauka i obrazovanie v usloviyakh mirovoy nestabil'nosti: problemy, novye etapy razvitiya* [Science and Education Under Global Instability: Problems, New Stages of Development]. Proc. of the Second International Conference. Rostov on Don: Manuskript. p. 262.

6. Yandex blog "Rover – a robot courier." [Online] Available from: https://yandex.ru/blog/company/yandeks-rover-robot-dostavschik

7. Krasovskaya, N.R. & Gulyaev, A.A. (2020) Tekhnologii manipulyatsii soznaniem pri ispol'zovanii dipfeykov kak instrumenta informatsionnoy voyny v politicheskoy sfere [Technologies of consciousness manipulation when using deepfakes as a tool of information warfare in the political sphere]. *Vlast'*. 4. p. 94.

8. Atagimova, E.I., Potemkina, A.T. & Tsopanova, I.G. (2017) "Krazha lichnosti" kak samostoyatel'noe prestuplenie ili raznovidnost' moshennichestva ["Identity theft" as an independent crime or a type of fraud]. *Pravovaya informatika*. 3. p. 18.

9. Dolgochub, E.A. & Polikanin, A.N. (2021) Tekhnologii kvantovoy kriptografii [Quantum cryptography technologies]. *Interekspo Geo-Sibir'*. 6. pp. 78–83.

10. Shemyakina, M.A. (2019) Analiz ispol'zovaniya kvantovykh tekhnologiy v kriptografii [An analysis of the use of quantum technologies in cryptography]. *Mezhdunarodnyy zhurnal gumanitarnykh i estestvennykh nauk*. 5–4. pp. 59–62.

11. Asadullina, A.V. & Belousov, V.S. (2023) Global'nye trendy v razvitii i regulirovanii tekhnologiy iskusstvennogo intellekta [Global trends in the development and regulation of artificial intelligence technologies]. *Rossiyskiy vneshneekonomicheskiy vestnik*. 9. pp. 86–104.

12. Bresler, M.G., Serdyuk, A.V. & Suleymanov, A.R. (2021) Spetsifika regulirovaniya IT-industrii v Kitae: istoriya i sovremennost' [Specificity of regulation of the IT industry in China: history and modernity]. *Vestnik UGNTU. Nauka, obrazovanie, ekonomika. Seriya: Ekonomika*. 4(38). pp. 53–62.

13. Avelsnik, N. (2016) *Algoritm dlya vyneseniya prigovorov obvinili v predvzyatosti* [Sentencing algorithm accused of bias]. [Online] Available from: https://hightech.fm/2016/06/28/compas_bias

14. Asadullina, A.V. & Belousov, V.S. (2022) Regulirovanie tekhnologiy iskusstvennogo intellekta na territorii Evropeyskogo Soyuza [Regulation of artificial intelligence technologies in the European Union]. *Rossiyskiy vneshneekonomicheskiy vestnik*. 8. pp. 20–35.

15. Mervis, J. (2021) U.S. law sets stage for boost to artificial intelligence research. *Science*. 371 (6525). pp. 112–113. DOI: 10.1126/science.371.6525.112

16. Savage, N. (2020) The race to the top among the world's leaders in artificial intelligence. *Nature Index*. 9th December. [Online] Available from: https://www.nature.com/articles/d41586-020-03409-8

Информация об авторе:

Киселев А.С. – кандидат юридических наук, старший научный сотрудник Центра исследований и экспертиз, доцент кафедры международного и публичного права юридического факультета Финансового университета при Правительстве Российской Федерации (Москва, Россия). E-mail: alskiselev@fa.ru; SPIN-код: 3570-8911; Author ID: 819975; ORCID: 0000-0002-5044-4721; WoS Researcher ID: ABX-2279-2022.

Автор заявляет об отсутствии конфликта интересов.

Information about the author:

A.S. Kiselev, Candidate of Law, Senior Researcher at the Center for Research and Expertise, Associate Professor of the Department of International and Public Law at the Faculty of Law of the Financial University under the Government of the Russian Federation (Moscow, Russian Federation). E-mail: alskiselev@fa.ru; SPIN-код: 3570-8911; AuthorID: 819975; ORCID: 0000-0002-5044-4721; WoS ResearcherID: ABX-2279-2022.

The author declares no conflicts of interests.

Статья поступила в редакцию 10.09.2024;
одобрена после рецензирования 27.12.2024; принята к публикации 19.03.2025.

The article was submitted 10.09.2024;
approved after reviewing 27.12.2024; accepted for publication 19.03.2025.