Правовое обеспечение безопасности информационного пространства Российской Федерации в сфере искусственного интеллекта

Полина Владимировна ЕРЕСЬКО,
доцент кафедры информационного права и цифровых технологий Саратовской государственной юридической академии (СГЮА),
кандидат педагогических наук, доцент
pv.eresko@yandex.ru
410056, Россия, г. Саратов, ул. Чернышевского, д. 104, стр. 3

Аннотация. *С одной стороны, одним из приоритетных направлений государственной политики в соответствии с Национальной стратегией развития искусственного интеллекта на период до 2030 года становится ускоренная разработка ИИ, с другой — возникают различные проблемы, в том числе правового регулирования сферы ИИ в целях обеспечения безопасности информационного пространства Российской Федерации.*
Методология: использование совокупности диалектического, формального и системного методов исследования развития и внедрения технологий ИИ для определения основных направлений правового регулирования в сфере ИИ и выявления проблем, связанных с правовым обеспечением безопасности информационного пространства Российской Федерации.
Результаты: проанализированы подходы к регулированию ИИ в Российской Федерации и в мировой практике; рассмотрены имеющиеся правовые проблемы в области развития и использования ИИ; выявлено, что внедрение технологий ИИ приводит к нарушениям безопасности информационного пространства Российской Федерации. Результатом исследования явилось обоснование необходимости создания единой нормативно-правовой базы в сфере ИИ для обеспечения безопасности информационного пространства Российской Федерации, которая может быть достигнута путем совершенствования законодательной базы в сфере ИИ, а также минимизации выделенных правовых рисков, сопряженных с практикой разработки и внедрения технологий ИИ.
Ключевые слова: *информационная безопасность, безопасность информационного пространства, искусственный интеллект, правовое регулирование искусственного интеллекта, правовые проблемы, правовые риски*

DOI: 10.17803/2311-5998.2024.122.10.069-076

Polina V. ERESKO,
Associate Professor of the Department of information law and digital technologies of the Saratov State Law Academy (SSLA), Cand. Sci. (Pedagogy), Associate Professor
pv.eresko@yandex.ru
104/3, ul. Chernyshevsky, Saratov, Russia, 410056

Legal Support of the Security of the Information Space of the Russian Federation in the Field of Artificial Intelligence

Abstract. *On the one hand, one of the priority areas of state policy in accordance with the National Development Strategy is the accelerated development of artificial intelligence (AI), on the other hand, various problems arise, including legal regulation of the field of AI in order to ensure the security of the information space of the Russian Federation.*
Methodology: Using a set of dialectical, formal and systemic methods to study the development and implementation of AI technologies to determine the main directions of legal regulation in the field of AI and identify problems associated with legal support for the security of the information space of the Russian Federation.
Results. Approaches to regulation of AI in the Russian Federation and in world practice are analyzed; The existing legal problems in the field of development and use of AI are considered. It has been revealed that the introduction of AI technologies leads to violations of the security of the information space of the Russian Federation. The result of the study was the substantiation of the need to create a unified regulatory framework in the field of AI to ensure the security of the information space of the Russian Federation, which can be achieved by improving the legislative framework in the field of AI, as well as minimizing the identified legal risks associated with the practice of developing and implementing AI technologies.
Keywords: *information security, security of the information space, artificial intelligence, legal regulation of artificial intelligence, legal problems, legal risks*

Искусственный интеллект развивается стремительными темпами в мировом масштабе в качестве передовой технологии. Влияние технологий искусственного интеллекта на современное информационное общество неоспоримо, а в будущем легко предположить проникновение этих технологий во все большее количество процессов.

ИИ основан на алгоритмах различного вида, состоит из множества нейронов, обменивающихся информацией и образующих нейронные сети. ИИ при помощи математических моделей имитирует работу человеческого мозга и обладает такими свойствами, как анализ, синтез, обучение, управление, принятие решений, воспроизведение и генерирование звуков, выполнение тех или иных действий, которые раньше были присущи человеку как субъекту. ИИ постоянно обучается,

осуществляет поиск решений без заранее заданного алгоритма, совершенствуется и адаптируется к новым обстоятельствам.

Указом Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы»[1] искусственный интеллект выделен в качестве одного из основных направлений развития российских информационных и коммуникационных технологий.

В 2022 г. Минэкономразвития России совместно с учеными Национального исследовательского университета «Высшая школа экономики», компаниями — лидерами отрасли и экспертными организациями определили вектор развития высокотехнологичных направлений в «Белой книге»[2]: ИИ, интернет вещей; перспективные космические системы и др. При этом ИИ входит в первые десять передовых технологий.

Развитие технологий ИИ, а в будущем — занятие лидирующих позиций в мире в сфере ИИ становится одной из приоритетных задач в области государственной политики нашей страны, что подтверждается принятой Национальной стратегией развития искусственного интеллекта на период до 2030 года, утвержденной Указом Президента РФ 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации»[3].

Согласно Национальной стратегии развития ИИ (в ред. Указа Президента РФ от 15.02.2024 № 124)[4], ИИ определяется как «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их».

К технологиям ИИ официально относят: компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта. Правовое регулирование ИИ выделено в качестве ключевого фактора развития ИИ на территории нашей страны.

Цифровая трансформация различных областей общественной деятельности технологиями ИИ неизбежно влечет за собой для общества, граждан и государства правовые риски. Необходимо учитывать особенности развития и внедрения технологий ИИ в структуры управления, области экономики, транспорта, промышленности, медицины, образования и т.д. для обеспечения безопасности информационного пространства.

Вопросы правового обеспечения безопасности информационного пространства нашей страны в условиях цифровой трансформации, соответствующие

[1] СЗ РФ. 2017. № 20. Ст. 2901.

[2] «Белая книга» высоких технологий в России и за рубежом // URL: https://ict.moscow/static/pdf/files/belaya_kniga_2022.pdf (дата обращения: 05.10.2024).

[3] СЗ РФ. 2019. № 41. Ст. 5700.

[4] СЗ РФ. 2024. № 8. Ст. 1102.

правовые проблемы рассматривались в трудах Т. А. Поляковой[5], Н. Н. Ковалевой[6], А. В. Минбалеева[7], В. Н. Лопатина[8], А. А. Козыревой, Р. В. Надтоки[9] и др.

Создание, разработка и внедрение технологий ИИ в мировую практику несет с собой массу неразрешенных правовых проблем и характеризуется частичным регулированием в правовом поле. По Индексу ИИ Стэнфордского университета по состоянию на 2022 г.[10] Россия занимала второе лидирующее место после США по количеству нормативных правовых актов в сфере ИИ, принятых в 25 странах за пять лет (2016—2021). В США было принято на 2022 г. 13 законопроектов, в России — 6, в других странах — 5 и меньше, а в некоторых странах законопроектов не имелось. Индекс ИИ Стэнфордского университета по состоянию на 2023 г.[11] за 2016—2022 гг. показал, что Россия занимает пятое место вместо второго (как в предыдущем исследовании) в мировом сообществе, уступая США, Португалии, Испании и Италии (см. рисунок).

В качестве одного из основных принципов развития и использования ИИ указан принцип безопасности. ИИ не должен причинять вред гражданам и юридическим лицам, в том числе недопустимо злонамеренно, умышленно использовать ИИ для достижения своих целей. Для предотвращения возникновения негативных последствий использования ИИ необходимо предпринимать меры по предупреждению и минимизации рисков.

В случае сбалансированного законодательства в сфере ИИ, основанного на соблюдении этических норм при внедрении технологий ИИ, с учетом обеспечения безопасности информационного пространства, Россия будет иметь высокие шансы на опережение западных исследований в сфере ИИ. Как следствие этого прогнозируются экономический и технологический рост за счет собственных и

---

[5] *Полякова Т. А., Бойченко И. С.*, *Троян Н. А.* Информационно-правовое обеспечение информационной безопасности в транспортной сфере в условиях цифрового развития // Транспортное право и безопасность. 2021. № 3 (39). С. 146—155.

[6] *Ковалева Н. Н.* Роль информационной безопасности в процессе организации эффективного управления регионами // Информационная безопасность регионов. 2011. № 2 (9). С. 72—75.

[7] *Минбалеев А. В., Сторожакова Е. Э.* Проблемы правовой охраны персональных данных в процессе использования нейронных сетей // Вестник Университета имени О.Е. Кутафина (МГЮА). 2023. № 2 (102). С. 71—79.

[8] *Лопатин В. Н.* Проблемы информационной безопасности и риски интеллектуальной собственности в цифровой экономике // Информационное право. 2017. № 2. С. 8—16.

[9] *Козырева А. А., Надтока Р. В.* Правовые подходы к минимизации рисков, связанных с применением технологий искусственного интеллекта // Социально-политические науки. 2021. Т. 11. № 3. С. 74—79.

[10] The AI Index Report 2022 — Artificial Intelligence Index Report 2022 // Stenford Univeresity Human-Centered Artificial Intelligence. URL: https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-ai-index-report_master.pdf (дата обращения: 05.10.2024).

[11] The AI Index Report 2023 — Artificial Intelligence Index Report 2022 // Stenford Univeresity Human-Centered Artificial Intelligence. URL: https://arxiv.org/ftp/arxiv/papers/2310/2310.03715.pdf (дата обращения: 05.10.2024).

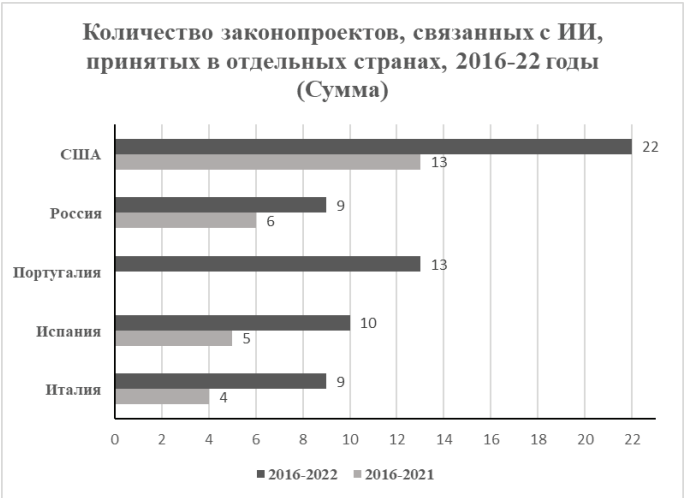

Диаграмма изменения количества законопроектов, связанных с ИИ, принятых в отдельных странах, 2016—2022 гг.

иностранных инвестиций, создание условий для улучшения уровня жизни населения нашей страны.

Проанализировав развитие, внедрение и использование технологий ИИ, можно выделить следующие правовые риски обеспечения безопасности информационного пространства Российской Федерации в сфере ИИ.

1. Проблемы кибербезопасности, относящиеся к защите информации операторов и пользователей автоматизированных информационных систем (АИС) (логин; пароль; информация, содержащаяся в системе и т.п.). При перехвате такого рода информации технологиями ИИ мошенники могут представляться другим физическим или юридическим лицом и совершать от этого лица неправомерные действия с различными коммерческими целями.

Информация АИС может являться конфиденциальной, секретной и не быть общедоступной. Распространение такого рода информации запрещено. Но у технологий ИИ нет морального аспекта, злоумышленники могут воспользоваться ими для получения ценной информации, возможно, информации, относящейся к государственной тайне. Применить технологии ИИ может любой пользователь сети Интернет как из России, так и из-за границы. В настоящее время норм права, относящихся к сфере использования ИИ в противоправных целях, в УК РФ не имеется. Необходимо правовое регулирование технологий ИИ в мировом сообществе и в России для создания и использования законным образом данных технологий, а также привлечения к ответственности для определения меры наказания в случае противоправного использования.

2. Проблемы конфиденциальности персональных данных. Происходит нарушение приватности, личной жизни и интересов человека. Современные облачные АИС собирают, получают, хранят и обрабатывают большие массивы персональных и государственных данных, не имеющих статус общедоступных. Если АИС не обладают достаточным уровнем защиты, то использование технологий ИИ увеличивает риски взлома АИС и утечки конфиденциальных данных.

Для предотвращения утечки данных пользователей беспилотного такси и обеспечения режима персональных данных статьей 7 Федерального закона от 24.04.2020 № 123-ФЗ[12] была изменена ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Изменения касались обработки персональных данных, полученных в результате обезличивания персональных данных, которая осуществляется в целях повышения эффективности государственного или муниципального управления.

При этом Федеральный закон от 24.04.2020 № 123-ФЗ не допускает хранения персональных данных, полученных в результате обезличивания, за пределами Москвы. Поточечно имеется правовое регулирование этой проблемы, но пока отсутствует системный подход, необходимо совершенствование законодательства в области персональных данных.

3. Проблема создания технологиями ИИ фейков и дипфейков. Это проблема искажения данных или создания фальсифицированных данных, практически не отличимых от реальности. Фейками могут быть версии картин общеизвестных гениальных художников, фотографий, лекарств и т.п., созданные технологиями ИИ. Под дипфейком понимают поддельный медиаконтент (аудио, изображение или видео). ИИ анализирует данные серверов, хранящих информацию пользователей сети Интернет.

Предметом анализа может служить как объективная информация — факты, так и субъективная информация — неактуальная, устаревшая, высказывание отдельного человека. При случайном попадании неверной информации для анализа ИИ может сгенерировать неверные, ошибочные результаты, которые могут отрицательно отразиться на политическом, психологическом здоровье наших граждан, находящихся в так называемом «смешанном» пространстве. Мировые новости могут быть представлены с использованием технологий ИИ в искаженном свете, являться информационным оружием. С каждым годом усложняется техническая возможность разоблачения дезинформации в связи с усложнением алгоритмов ИИ. Недостаточно проработана правовая база по определению и доказательству таких противоправных действий в сфере ИИ и определения наказания за подрыв национальной безопасности.

4. Проблема хакерских атак с использованием технологий ИИ на АИС различных государственных структур и организаций. Они осуществляются с целью нарушения структуры данных и потоков информации, нарушения работы АИС, получения несанкционированного доступа к информации систем.

5. Проблема определения авторства в генерированных ИИ текстах, изображениях, видео. Технологии ИИ используют данные сети Интернет для формирования текстов, запрашиваемых любым пользователем. Тем самым нарушается авторское право, не имеется ссылок на используемые ИИ тексты научных работ и новостей, картины. Проблема относится к ChatGPT, Midjourney, Kandinsky и

[12] Федеральный закон от 24.04.2020 № 123-ФЗ1 «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона “О персональных данных”» // СПС «КонсультантПлюс».

другим технологиям ИИ, постоянно создаваемым и с интересом используемым пользователями. Нет общих критериев и разработанных правовых международных норм, касающихся этой части сферы ИИ.

Для решения проблем безопасности информационного пространства страны при создании и использовании технологий ИИ нужно использовать комплекс мер, направленных на обеспечение информационной и технологической безопасности. Комплекс мер обязательно должен содержать:

— контроль удаленного доступа, в том числе с использованием ИИ, такого как компьютерное зрение и др.;
— меры по защите исходного кода программы от умышленного копирования, искажения или удаления;
— меры по защите инфраструктуры.

Без использования технологий ИИ в будущем не обойдется ни одна сфера деятельности человека, в том числе космические исследования. В контексте стремительно развивающейся сферы искусственного интеллекта во всем мире важная роль отводится обеспечению национальной безопасности.

Для искусственного интеллекта нет никаких границ, в связи с чем возникают явные и скрытые угрозы нарушения безопасности информационного пространства Российской Федерации, минимизировать которые возможно формированием единой нормативно-правовой базы в сфере ИИ путем разработки новых нормативных правовых актов, совершенствования имеющихся нормативных правовых актов, введения новых норм в сфере ИИ.

Решение правовых проблем безопасности информационного пространства Российской Федерации в процессе развития, разработки и использования технологий искусственного интеллекта позволит достичь ключевых показателей Национальной стратегии развития искусственного интеллекта и удержать лидирующие позиции России в правовом регулировании искусственного интеллекта в мире.

БИБЛИОГРАФИЯ

1. *Ковалева Н. Н.* Роль информационной безопасности в процессе организации эффективного управления регионами // Информационная безопасность регионов. — 2011. — № 2 (9). — С. 72—75.
2. *Козырева А. А.*, *Надтока Р. В.* Правовые подходы к минимизации рисков, связанных с применением технологий искусственного интеллекта // Социально-политические науки. — 2021. — Т. 11. — № 3. — С. 74—79.
3. *Лопатин В. Н.* Проблемы информационной безопасности и риски интеллектуальной собственности в цифровой экономике // Информационное право. — 2017. — № 2. — С. 8—16.
4. *Минбалеев А. В.*, *Сторожакова Е. Э.* Проблемы правовой охраны персональных данных в процессе использования нейронных сетей // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2023. — № 2 (102). — С. 71—79.
5. *Полякова Т. А.*, *Бойченко И. С.*, *Троян Н. А.* Информационно-правовое обеспечение информационной безопасности в транспортной сфере в условиях

цифрового развития // Транспортное право и безопасность. — 2021. — № 3 (39). — С. 146—155.
6. The AI Index Report 2022 — Artificial Intelligence Index Report 2022 // Stenford Univeresity Human-Centered Artificial Intelligence. — URL: https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-ai-index-report_master.pdf (дата обращения: 05.10.2024).
7. The AI Index Report 2023 — Artificial Intelligence Index Report 2022 // Stenford Univeresity Human-Centered Artificial Intelligence/. — URL: https://arxiv.org/ftp/arxiv/papers/2310/2310.03715.pdf (дата обращения: 05.10.2024).