УДК 34.01

ПРАВОВЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАЩИТЕ ИНФОРМАЦИИ

Legal issues of using artificial intelligence in information protection

К. Быценко, студент
Юридический институт
Белгородского государственного национального исследовательского университета
(Белгород, улица Победы, 85)

Научный руководитель: Н. В. Бородаенко,
старший преподаватель кафедры
административного права и процесса

Аннотация

Статья посвящена анализу правовых проблем, возникающих при использовании искусственного интеллекта (далее - ИИ) в сфере защиты информации и персональных данных. Автор отмечает, что действующее законодательство зачастую не учитывает особенностей систем искусственного интеллекта – их автономности, непрозрачности работы и трансграничного характера. В результате возникают риски, как для субъектов персональных данных, так и для операторов, эксплуатирующих подобные технологии. Автор предлагает принять отдельные нормативные акты и внести изменения в существующие законы, направленные на определение понятия ИИ, установление требований к безопасности таких систем, а также внедрение принципов прозрачности и подотчетности. В качестве перспективных направлений отмечаются развитие саморегулирования и создание этических стандартов работы с ИИ.

Ключевые слова: искусственный интеллект, защита информации, персональные данные, информационная безопасность, правовое регулирование, прозрачность, ответственность, цифровые технологии, законодательство, саморегулирование.

Summary

This article analyzes the legal issues arising from the use of artificial intelligence (hereinafter referred to as AI) in the field of information and personal data protection. The author notes that current legislation often fails to take into account the specific features of AI systems—their autonomy, opaque operation, and cross-border nature. This creates risks for both data subjects and operators using such technologies. The author proposes adopting separate regulations and amending existing laws aimed at defining the concept of AI, establishing security requirements for such systems, and implementing principles of transparency and accountability. The development of self-regulation and the creation of ethical standards for working with AI are noted as promising areas.

Keywords: artificial intelligence, information protection, personal data, information security, legal regulation, transparency, responsibility, digital technologies, legislation, self-regulation.

Понятие искусственного интеллекта закреплено в единственном нормативном правовом акте РФ: национальной стратегии развития искусственного интеллекта на период до 2030 года, утвержденной указом Президента РФ от 10 октября 2019 года № 490 «О развитии искусствен-

ного интеллекта в Российской Федерации», согласно П. П. 5 которого искусственный интеллект – это «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» [1].

Согласимся с И. И. Литвиным, что проблема правовой охраны персональных обрабатываемых с использованием технологий ИИ, формируется и решается в Российской Федерации несколько лет [2, с. 113]. Главным вопросом остается соблюдение баланса между требованиями по защите персональных данных и необходимостью их использования для обучения систем ИИ для цели выполнения задачи повышения доступности и качества данных [3, с. 92].

В контексте рассматриваемого вопроса отметим, что ключевой проблемой использования ИИ в сфере защиты персональных данных является отсутствие законодательства, регламентирующего данный процесс. Кроме того, с нашей точки зрения, несмотря на наличие отдельных актов, законодатель по-прежнему недостаточно четко отвечает на вопрос о правовом статусе ИИ, порядке его сертификации и контроля, а также механизмах раскрытия логики решений, принятых посредством данных систем. Фактически, в отрыве от подзаконных актов многие нормы остаются декларативными и не приспособлены для практической реализации. При этом уровень угроз, связанных с ошибками или злоупотреблениями со стороны ИИ-систем, только возрастает. Так, на сегодняшний день действует только Указ Президента РФ от 10 октября 2019 года № 490 «О развитии искусственного интеллекта в Российской федерации», а также федеральный закон от 24 апреля 2020 года №123-ФЗ «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» [4]. Однако данные нормативные правовые акты не содержат конкретных норм, регламентирующих порядок использования ИИ, а также установления ответственности за нарушение законодательства о персональных данных, совершенных с помощью ИИ или в силу допущения им технической ошибки, которая привела к сбою [5].

Для решения проблемы отсутствия в России законодательства, регламентирующего порядок использования искусственного интеллекта (ИИ) в сфере защиты персональных данных, необходим комплексный правовой подход, включающий разработку и внедрение новых нормативных актов, а также внесение изменений в существующие законы о персональных данных и информационной безопасности.

Во-первых, целесообразно принять отдельный федеральный закон или внести существенные дополнения в действующий федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных», в котором должно быть четко определено понятие искусственного интеллекта применительно к обработке персональных данных [6]. Необходимо установить специальные требования к системам ИИ, используемым в этой сфере: это может быть обязательная сертификация таких систем, оценка их соответствия стандартам безопасности, а также введение механизмов аудита и мониторинга функционирования ИИ.

Во-вторых, на законодательном уровне следует закрепить принципы прозрачности и подотчетности при использовании ИИ в обработке и защите персональных данных. Применение ИИ должно предполагать возможность объяснения решений, принимаемых системой, и предоставление субъекту персональных данных доступа к информации о логике и критериях обработки его данных. Кроме того, важно прописать обязанности оператора персональных данных

по обеспечению контроля за действиями ИИ, а также по своевременному предотвращению и ликвидации последствий ошибок или сбоев в функционировании таких систем.

В-третьих, если обратиться к зарубежному опыту, то, например, в Европейском союзе, где законодательство традиционно считается одним из самых развитых в сфере использования искусственного интеллекта, специального нормативного правового акта пока нет. Законодательные органы лишь начинают вырабатывать эффективные правила. Например, в последние годы был принят Общий регламент защиты персональных данных [7], а также предложен специальный закон о регулировании искусственного интеллекта – Европейский Акт об искусственном интеллекте (European AI Act) [8]. Анализируя данные нормативные правовые акты, отметим, что Общий регламент защиты персональных данных, действующий в странах Европейского союза, устанавливает строгие правила обработки персональных данных, в том числе с использованием искусственного интеллекта. Важным положением GDPR является обязанность организации обеспечить прозрачность обработки данных, необходимость получения информированного согласия у субъектов персональных данных, а также гарантия возможности для человека узнать и оспорить решения, принятые автоматически с помощью алгоритмов ИИ.

Что касается Европейского акта, то данный закон, вступивший в силу с 1 августа 2024 года, представляет собой первую попытку комплексно регулировать применение искусственного интеллекта в ЕС. Документ устанавливает классификацию ИИ по уровням риска, предъявляет более строгие требования к системам, которые могут затрагивать права и свободы человека, например, в области биометрической идентификации, оценки кредитоспособности или принятия решений, влияющих на судьбу граждан. В отношении персональных данных в Европейском Акте содержит положения о необходимости обеспечить контроль, прозрачность, а также возможность объяснения решений ИИ. Таким образом, оба нормативных правовых акта направлены на то, чтобы повысить защиту прав граждан при использовании искусственного интеллекта, особенно когда речь идет о персональных данных.

Таким образом, правовое решение проблемы заключается в создании целостной системы регулирования на законодательном уровне с обязательной детализацией требований к ИИ в сфере обработки персональных данных, обеспечении прозрачности функционирования таких технологий и ответственности операторов, а также формировании правовых и технических инструментов для надзора и защиты интересов субъектов персональных данных.

В целом можно заключить, что развитие и внедрение искусственного интеллекта в сферу защиты информации сопровождается существенными правовыми вызовами, которые современное российское законодательство пока не в полной мере способно решить. Особенности ИИ – автономность, сложность алгоритмов и недостаточная прозрачность принимаемых решений – обостряют вопросы определения ответственности и эффективности традиционных механизмов защиты персональных данных. Анализ российского и зарубежного опыта показывает необходимость создания детальной и гибкой системы регулирования, способной учитывать как технические, так и этические аспекты использования ИИ. По нашему мнению, дальнейшее совершенствование законодательства должно быть направлено на формирование четких требований к ИИ-системам, усиление принципов прозрачности и подотчетности, а также защиту прав субъектов персональных данных в условиях стремительного технологического прогресса.

Библиографический список

1. Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации» // Собрание законодательства РФ. 2019. № 41. Ст. 5700.
2. *Литвин И. И.* Особенности сбора, обработки и защиты персональных данных искусственным интеллектом // Вестник Уральского юридического института МВД России. 2021. № 4. С. 112-118.
3. *Ищейнов В. Я.* Применение искусственного интеллекта в информационной безопасности // Делопроизводство. 2024. № 2. С. 90-93.
4. Федеральный закон от 24.04.2020 № 123-ФЗ «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» // Собрание законодательства РФ. 2020. № 17. Ст. 2701.
5. *Базалеева В. Р., Карпухина Д. А., Бородаенко Н. В.* Использование искусственного интеллекта в юридической сфере // Международный журнал гуманитарных и естественных наук. 2024. № 5-1 (92). URL: https://cyberleninka.ru/article/n/ispolzovanie-iskusstvennogo-intellekta-v-yuridicheskoy-sfere (дата обращения: 02.06.2025).
6. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024) «О персональных данных» // Собрание законодательства РФ. 2006. № 31. Ст. 3451.
7. Общий регламент защиты персональных данных Европейского союза. URL: https://gdpr-text.com/ru/ (дата обращения: 17.05.2025).
8. EU Artificial Intelligence Act. URL: https://artificialintelligenceact.eu/ (дата обращения: 17.05.2025).