УДК 342

**© Анастасия Николаевна Орлова**
кандидат юридических наук,
доцент кафедры юриспруденции Муромского института (филиала) федерального государственного бюджетного образовательного учреждения высшего образования «Владимирский государственный университет имени А. Г. и Н. Г. Столетовых»,
г. Муром
oid@mivlgu.ru

**Anastasia N. Orlova**
Candidate of Law, Associate Professor of the Department of Jurisprudence of the Murom Institute (branch) of the Federal State Budgetary Educational Institution of Higher Education «Vladimir State University named after Alexander Grigorievich and Nikolay Grigorievich Stoletov»,
Murom

**© Артём Алексеевич Демидов**
студент 4-го курса
Муромского института (филиала) федерального государственного бюджетного образовательного учреждения высшего образования «Владимирский государственный университет имени А. Г. и Н. Г. Столетовых»,
г. Муром

**Artem A. Demidov**
4th year student
of the Murom Institute (branch) of the Federal State Budgetary Educational Institution of Higher Education «Vladimir State University named after Alexander Grigorievich and Nikolay Grigorievich Stoletov»,
Murom

# ПРАВОВЫЕ ОГРАНИЧЕНИЯ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

## Legal restrictions on the development of artificial intelligence

*Аннотация. Статья посвящена актуальным проблемам правового регулирования искусственного интеллекта (далее – ИИ) в контексте его стремительного развития и повсеместного внедрения. Распространение ИИ порождает значительные правовые риски, требующие комплексного законодательного реагирования. На основе проведенного исследования сформулированы выводы о необходимости скорейшего развития единого законодательства, четкого определения ответственности, обеспечения баланса между инновациями и защитой прав граждан, а также усиления контроля за обработкой данных.*

*Annotation. The article is devoted to topical issues of legal regulation of artificial intelligence (hereinafter – AI) in the context of its rapid development and widespread implementation. The spread of AI generates significant legal risks that require a comprehensive legislative response. Based on the conducted research, conclusions have been formulated on the need for the rapid development of unified legislation, a clear definition of responsibility, ensuring a balance between innovation and the protection of citizens' rights, as well as strengthening control over data processing.*

*Ключевые слова: искусственный интеллект, персональные данные, защита, прозрачность, технологии, законодательство, контроль.*

*Keywords: artificial intelligence, personal data, protection, transparency, technology, legislation, control.*

Искусственный интеллект – это направление науки, которое занимается разработкой компьютерных систем, способных выполнять задачи, свойственные человеческому интеллекту. К ним относятся анализ данных, распознавание образов, обработка текстов и запросов, обучение на потоках данных и принятие решений.

За последние несколько лет развитие технологий искусственного интеллекта достигло беспрецедентных высот, системы искусственного интеллекта стали неотъемлемой частью нашей жизни: домашняя Яндекс-станция с голосовым помощником, способная напомнить о важном мероприятии, подобрать музыку исходя из предпочтений или построить диалог, тем самым заменив живое общение с людьми. В поездке на работу используем навигатор с встроенным ИИ, который анализирует загруженность дорог, погоду, историю ваших поездок и за считанные секунды выстраивает оптимальный маршрут. Листая ленту в социальных сетях, вы могли замечать, что приложение будто бы знает, что именно вам интересно в данным момент. Это тоже работа ИИ, который анализирует предыдущие понравившиеся посты или видео, время просмотра и авторов, что позволяет подстраивать предлагаемый контент под вкус потребителя.

Стоит отметить, что системы искусственного интеллекта участвуют не только в жизни обычных граждан. В частности, с 2024 года Министерство финансов Российской Федерации совместно со Сбербанком запустили пилотный проект по использованию искусственного интеллекта в бюджетном процессе [4], технология помогает в сопоставлении кодов бюджетной классификации (обозначают статьи доходов и расходов казны) и привязанных к ним результатов.

Также ИИ используется в медицине при анализе МРТ, КТ, рентгенов, УЗИ, а также помогает готовить заключения. В промышленности ИИ занят прогнозированием поломок, оптимизацией ремонтов, а, к примеру, на трассе М-11 уже ездят беспилотные тягачи.

Несомненно, развитие систем искусственного интеллекта делает жизнь проще, искусственный интеллект ежедневно собирает огромное количество информации, создавая риски как для граждан, так и для государств в целом, поэтому в целях обеспечения безопасности требуется тщательное правовое регулирование его использования и дальнейшего развития.

Анализ текущего состояния правового регулирования выявляет ряд существенных проблем. Прежде всего, это отсутствие единой и чёткой законодательной базы, способной эффективно регулировать все аспекты развития ИИ. Особую сложность представляет проблема определения субъекта ответственности за действия, совершаемые ИИ-системами.

К примеру, врач доверился диагнозу, который пациенту поставил искусственный интеллект, а пациент умер из-за неправильно поставленного диагноза. Кто же будет виноват в такой ситуации? Разработчик системы, которая

вынесла неверный диагноз? Руководство больницы как владелец системы? Или врач, слепо верящий в достоверность работы ИИ?

В частности, эта проблема сложна и потому, что ИИ – это не просто программа. Он учится на данных, принимает решения самостоятельно, и часто нельзя точно объяснить, почему он поступил именно так (это называют «чёрным ящиком»). Поэтому классическая схема ответственности («кто сделал – тот и виноват») здесь не работает. Также и сам искусственный интеллект, вынесший диагноз, не может нести ответственность, ведь субъектом права он не является.

Также немаловажной проблемой является защита данных. С одной стороны, искусственный интеллект становится умнее и точнее только тогда, когда обучается на объёмных, разнообразных и качественных данных, включая личную информацию – медицинские записи, голос, изображения, поведенческие паттерны. С другой – использование таких данных без должной защиты угрожает приватности, автономии и безопасности людей.

К примеру, чтобы ИИ мог, например, диагностировать болезни, ему нужны реальные медицинские снимки и истории болезни; понимать речь – тысячи часов аудиозаписей с разными акцентами и языками; распознавать лица – фотографии людей в разных условиях; предсказывать поведение – данные о действиях пользователей. Без этих данных ИИ будет недоученным, предвзятым или неработоспособным.

Люди часто не знают, что их данные используются для обучения ИИ, или дают согласие «вслепую», не понимая масштабов. Всё это угрожает конфиденциальности, поскольку данные могут утечь, быть проданы или использованы не по назначению, например, для манипуляций, слежки или дискриминации. Персональные данные могут быть скомпрометированы: даже если имя скрыто, по поведению, голосу или местоположению человека часто можно идентифицировать. К примеру, сейчас мошенники с помощью искусственного интеллекта, получив доступ к аккаунту в социальной сети и взяв оттуда несколько голосовых сообщений, могут сгенерировать голосовое сообщение с просьбой «перевести на карту денег в долг» или любой другой информацией, полностью подделав голос человека.

Мировая практика демонстрирует разнообразие подходов к регулированию искусственного интеллекта.

В Евросоюзе в 2024 году был принят первый в мире всеобъемлющий закон об ИИ – AI Act. Его особенность заключается в разделении ИИ-систем на три уровня риска:

1) запрещённые (скрытая слежка за людьми, социальный скоринг, манипуляция сознанием и подобные) – их разработка и использование полностью запрещены;

2) высокорисковые (они включают в себя ИИ-системы в здравоохранении, образовании, судах, полиции, транспорте) – их использование разрешено, однако требует чёткой регламентации алгоритмов деятельности, оценки безопасности их использования, контроля со стороны работников, а также необходимость их регистрации в едином реестре;

3) ИИ-системы ограниченного или минимального риска (чат-боты, рекомендации и др.) – их использование разрешено, однако требуется пометка, что контент сгенерирован ИИ или об использовании ИИ.

Интересен тот факт, что ответственность за нарушение закона разделена между поставщиком (provider) – компанией, которая разрабатывает или продвигает ИИ-систему под своим именем, и пользователем (deployer) – организацией, которая использует ИИ (например, больница, банк, полиция).

В Китае в 2023 году было принято «Положение об администрировании глубокого синтеза», которое запрещает распространять фейковые новости с помощью искусственного интеллекта, содержит обязанность предупреждать в случае генерации видео или изображения с помощью ИИ об этом, а также необходимо получать согласие на использование изображения или голоса человека. Сервисы, использующие ИИ-рекомендации, обязаны раскрывать алгоритм их работы. Также Китай делает упор на государственную безопасность, запрещая создавать контент, который может её подрывать и обязывая регистрировать ИИ-системы в соответствующем реестре [1].

В США отсутствует единый закон о регулировании искусственного интеллекта, однако с 2023 года действует указ президента, определяющий основные начала деятельности ИИ. В частности, закрепляется принцип прозрачности, справедливости и безопасности использования ИИ. Также в США используется секторный подход к регулированию искусственного интеллекта, предполагающий, что каждое федеральное ведомство контролирует и регулирует использование ИИ-систем в своей деятельности.

В России пока отсутствует единый закон об ИИ, однако регулирование развивается на основе национальной стратегии и отраслевых норм. Указом Президента РФ от 10.10.2019 № 490 утверждена «Национальная стратегия развития искусственного интеллекта до 2030 года» [2], которая задаёт курс на технологическое лидерство, развитие компетенций и внедрение ИИ в ключевые сферы – здравоохранение, образование, транспорт, промышленность и госуправление. Правовое регулирование строится не на запретах, а на постепенном формировании стандартов, реестров и этических принципов. В отдельных сферах уже действуют нормативные требования: например, Минздрав устанавливает правила для ИИ-систем в медицине, а Центральный банк РФ – для использования ИИ в банках и финансовых сервисах. Особое внимание уделяется защите персональных данных: использование ИИ на «Госуслугах», в полиции или здравоохранении должно соответствовать Федеральному закону № 152-ФЗ [1]. Ведётся работа над созданием реестра высокорисковых ИИ-систем, подлежащих обязательной оценке и контролю. Разработчики и операторы таких систем могут быть обязаны проходить независимую сертификацию и этическую экспертизу. Госдума рассматривает законопроекты, направленные на регулирование генеративного ИИ, включая обязанность маркировать синтетический контент и запрет на распространение дезинформации. Акцент делается на государственной безопасности и суверенитете технологий, в том числе на развитие отечественных моделей и платформ. Главная цель российского подхода – обеспечить технологическую

независимость, безопасность и контроль, не тормозя при этом внедрение инноваций.

Проведённое исследование демонстрирует, что развитие искусственного интеллекта достигло беспрецедентных высот и стало неотъемлемой частью современной жизни, охватывая как повседневные задачи граждан, так и профессиональную деятельность в различных сферах – от медицины до государственного управления.

Анализ показал наличие существенных проблем в правовом регулировании ИИ, среди которых особенно выделяются отсутствие единой законодательной базы и сложность определения субъекта ответственности за действия ИИ-систем. Особую тревогу вызывает вопрос защиты персональных данных при обучении искусственного интеллекта, поскольку системы требуют доступа к обширной информации, включая личные данные граждан, что создаёт риски для приватности и безопасности.

Мировая практика демонстрирует различные подходы к регулированию ИИ: от жёсткого законодательного регулирования в ЕС до гибкого секторального подхода в США и акцента на государственной безопасности в Китае. Российская модель регулирования находится в стадии формирования, опираясь на Национальную стратегию развития искусственного интеллекта, которая направлена на обеспечение технологической независимости и безопасности при одновременном развитии отечественных технологий. Проведённое исследование позволяет сделать ряд важных выводов относительно правового регулирования искусственного интеллекта в современном мире:

1) необходимо ускорить разработку единого законодательства в сфере ИИ;

2) требуется чёткое определение ответственности за действия ИИ-систем;

3) важно обеспечить баланс между развитием технологий и защитой прав граждан;

4) необходимо усилить контроль за защитой персональных данных при обучении ИИ.

Таким образом, правовое регулирование искусственного интеллекта требует комплексного подхода, учитывающего как технологические возможности, так и социальные риски. Только сбалансированное законодательство способно обеспечить безопасное и эффективное развитие технологий ИИ в интересах общества.

## Список литературы

1. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ : ред. от 01.09.2025 // Собр. законодательства Рос. Федерации. – 2006. – № 31, ч. 1, ст. 3451.

2. О развитии искусственного интеллекта в Российской Федерации : Указ Президента РФ от 10.10.2019 № 490 : ред. от 15.02.2024 // Собр. законодательства Рос. Федерации. – 2019. – № 41, ст. 5700.

3. Афанасьева Е. Н., Коротнев Р. И., Сунь Юйпэн. Правовое регулирование технологии глубокого синтеза в контексте искусственного интеллектуальных систем: на примере Китая и России // Baikal Research Journal. – 2023. – № 3.

4. Минфин впервые использовал ИИ в подготовке бюджета // Известия : [сайт]. URL: https://iz.ru/1777646/2024-10-21/minfin-vpervye-ispolzoval-ii-v-podgotovke-biudzheta (дата обращения: 12.10.2025).