УДК 342.7 + 004.8

Белова Дарья Ивановна магистрант

1 курс, Владивостокский государственный университет

Россия, г. Владивосток

ГРАЖДАНСКО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РОССИИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОЕКТА ФЕДЕРАЛЬНОГО ЗАКОНА И ЕВРОПЕЙСКОГО AI ACT

Аннотация: *Статья посвящена сравнительному анализу двух ключевых нормативных актов в сфере регулирования искусственного интеллекта: проекта Федерального закона Российской Федерации «Об основах государственного регулирования сфер применения технологий искусственного интеллекта» и Европейского регламента AI Act. Проведено исследование философских основ, подходов к классификации систем ИИ, механизмов ответственности, регулирования интеллектуальной собственности и других аспектов гражданско-правового регулирования. Выявлены фундаментальные различия в подходах, обусловленные разными стратегическими целями: защитой фундаментальных прав человека в ЕС и достижением технологического суверенитета в РФ. Показаны потенциальные точки сближения и конфликта правовых режимов, а также практические последствия для международного сотрудничества в сфере ИИ.*

Ключевые слова: *искусственный интеллект, гражданско-правовое регулирование, AI Act, законодательство о ИИ, сравнительный анализ, цифровые технологии.*

Annotation*. The article is devoted to a comparative analysis of two key regulatory acts in the field of artificial intelligence regulation: the draft Federal Law of the Russian Federation "On the Fundamentals of State Regulation of the Spheres of Application of Artificial Intelligence Technologies" and the European AI Act. The study examines the philosophical foundations, approaches to the classification of AI systems, liability mechanisms, intellectual property regulation and other aspects of*

civil law regulation. Fundamental differences in approaches determined by different strategic goals are revealed: the protection of fundamental human rights in the EU and the achievement of technological sovereignty in the Russian Federation. Potential points of convergence and conflict of legal regimes are shown, as well as practical consequences for international cooperation in the field of AI.

***Keywords**: artificial intelligence, civil law regulation, AI Act, AI legislation, comparative analysis, digital technologies.*

Введение

Стремительное развитие технологий искусственного интеллекта (далее – ИИ) в последние годы поставило перед правовыми системами беспрецедентные вызовы. Как справедливо отмечает Иванов С.В., «стремительное развитие технологий искусственного интеллекта ставит перед современным публичным правом беспрецедентные вызовы» [1, с. 26]. Особую актуальность приобретает задача разработки сбалансированного правового регулирования, которое, с одной стороны, не затормозило бы инновации, а с другой обеспечило бы защиту прав и законных интересов граждан, а также национальную безопасность [2, с. 126].

В мировой практике к настоящему моменту сложилось несколько моделей правового регулирования ИИ. Согласно классификации, предложенной в научной литературе, выделяют три базовые модели: риск-ориентированная горизонтальная (Европейский Союз, Южная Корея), секторально-фрагментированная (США, Израиль) и вертикально-контрольная (Китай) [1, с. 26]. Каждая из этих моделей отражает специфические правовые традиции и политические приоритеты соответствующих государств.

Наиболее значимым событием в сфере правового регулирования ИИ стало принятие Европейским Союзом Регламента 2024/1689 (AI Act), вступившего в силу 1 августа 2024 г. [4]. Данный документ «знаменует формирование первого в мире комплексного правового режима ИИ, основанного на риск-ориентированном подходе» [1, с. 26]. Параллельно с этим

Российская Федерация, опираясь на Национальную стратегию развития искусственного интеллекта до 2030 года [2, с. 126], разработала проект федерального закона «Об основах государственного регулирования сфер применения технологий искусственного интеллекта» (опубликован для общественного обсуждения 19 марта 2026 г.), который представляет собой национальный ответ на глобальные вызовы [5].

Настоящая статья направлена на всесторонний сравнительный анализ указанных нормативных актов. В отличие от имеющихся публикаций, акцент в работе сделан на гражданско-правовые аспекты регулирования: вопросы ответственности, интеллектуальной собственности, правового статуса субъектов. Цель исследования не просто описать различия, но и выявить их причины: расхождение в философских основаниях и стратегических целях европейского и российского подходов.

Основная часть

1. Философские основания и целевые установки регулирования

Фундаментальное различие между двумя анализируемыми актами коренится в их базовых философских предпосылках. Европейский AI Act в качестве основной цели декларирует «улучшение функционирования внутреннего рынка и содействие внедрению ориентированного на человека и заслуживающего доверия ИИ при обеспечении высокого уровня защиты здоровья, безопасности и фундаментальных прав» (п. 1 ст. 1 AI Act). Как подчеркивается в доктрине, это «риск-ориентированная горизонтальная модель», в основе которой лежит принцип пропорциональности: «интенсивность регулятивного воздействия возрастает по мере увеличения потенциального вреда от применения соответствующей технологии» [1, с. 26]. Европейский законодатель видит свою миссию в предотвращении ущерба правам человека еще до того, как такой ущерб будет причинен.

Российский Законопроект, напротив, в ст. 1 провозглашает «создание правовых условий для ускоренного развития и внедрения технологий ИИ, обеспечение безопасности личности, общества и государства, а также

достижение государственного технологического суверенитета». Примечательной особенностью является впервые введенное в явном виде требование соответствия технологий «традиционным российским духовно-нравственным ценностям» (п. 6 ст. 4 Законопроекта). Как отмечает Макаров Т.И., «государство и юридические организации интегрируют ИИ в свою деятельность, что неизбежно оказывает влияние на повседневную жизнь граждан», однако в России акцент сделан на обеспечение национальной конкурентоспособности и безопасности [2, с. 126].

Сравнительный анализ показывает, что европейский подход может быть охарактеризован как «превентивно-защитный», тогда как российский, как «суверенно-стимулирующий». Европа стремится установить «правила игры», которые бы защитили человека от произвола алгоритмов. Россия же использует правовой инструментарий для достижения технологической независимости, что особенно актуально в условиях внешних ограничений. По справедливому замечанию Астапенко П.Н., «российский подход можно определить как путь «малых, но точных шагов»: законодатель не стремится к всеобъемлющему регулированию ИИ, процесс осуществляется постепенно, путем формулирования рамочных принципов и положений» [3, с. 48–49].

2. Сфера действия и экстерриториальность

Вопрос о территориальных пределах действия нормативных актов приобретает особое значение в контексте ИИ, поскольку цифровые технологии не признают государственных границ. AI Act демонстрирует принцип «полной экстерриториальности». Согласно п. 1 ст. 2, он применяется к провайдерам, размещающим на рынке или вводящим в эксплуатацию системы ИИ в Союзе, «независимо от места их учреждения», а также к провайдерам и пользователям из третьих стран, если «результат, произведённый системой ИИ, используется в ЕС». Этот подход, как указывается в литературе, «формирует правовой режим, выходящий за пределы территориальной юрисдикции государств – членов ЕС» [6, с. 180].

Фактически любой разработчик в мире, желающий работать с европейским рынком, вынужден соблюдать европейские правила.

Российский Законопроект также содержит элементы экстерриториальности, но в значительно более ограниченном объеме. Согласно п. 3 «г» ст. 10 владелец сервиса ИИ обязан выполнять требования закона, если к сервису «в течение суток обращается более 500 тысяч пользователей сети «Интернет», находящихся на территории РФ». Кроме того, ст. 7 вводится приоритет для субъектов, контролируемых РФ. Таким образом, российский подход более «территориально-резидентный»: он ориентирован на регулирование деятельности на территории страны, а не на распространение своих правил на весь мир. Это соответствует общей стратегии обеспечения «суверенного ИИ», о которой пишет Астапенко [3, с. 48].

3. Классификация систем ИИ: риск против происхождения

Наиболее показательным является различие в подходах к классификации систем ИИ. Данное различие отражает глубинное расхождение в ценностных ориентирах.

Европейский AI Act использует четкую четырёхуровневую классификацию по степени риска для прав и свобод человека. Как отмечается в научной литературе, «европейские законодатели предлагают разделить нейросети на три уровня риска: недопустимый (unacceptable), высокий (high) и низкий или минимальный (low or minimal)» [7, с. 280]. В итоговой версии AI Act выделены четыре категории.

- Недопустимый риск охватывает системы, которые прямо запрещены. Согласно ст. 5 AI Act, запрещено 8 категорий практик. Иванов С.В. конкретизирует: «Статья 5 AI Act запрещает 8 категорий практик, включая социальный скоринг государственными органами, предиктивную полицию исключительно на основе профилирования личности и биометрическую идентификацию в реальном времени в публичных местах с ограниченными

исключениями» [1, с. 26–27]. Это абсолютные запреты, не зависящие от конкретных обстоятельств.

- Высокий риск – системы, подлежащие строгим требованиям (ст. 6 и Приложение III AI Act). Сюда относятся системы, используемые в критически важных сферах: биометрическая идентификация, управление критической инфраструктурой, образование, занятость, доступ к услугам, правоприменение, миграционный контроль, правосудие [7, с. 281].

- Ограниченный риск предполагает лишь требования прозрачности (ст. 50 AI Act): пользователь должен знать, что взаимодействует с ИИ.

- Минимальный риск (например, спам-фильтры) не регулируется [7, с. 282].

Российский Законопроект предлагает принципиально иную классификацию, по критериям «происхождения» и «уровня доверия». Ст. 3, 7 и 8 вводят следующие понятия:

- «Доверенные модели ИИ» – включённые в реестр, обрабатывающие данные исключительно на территории РФ, соответствующие требованиям безопасности ФСТЭК/ФСБ. Такие модели обязательны к применению в государственных информационных системах и на объектах критической информационной инфраструктуры (КИИ) (ст. 8).

- «Суверенные» и «национальные модели» – все этапы разработки и обучения осуществлены на территории РФ гражданами РФ или российскими юридическими лицами, находящимися под российским контролем (более 50% голосующих акций или долей) (ст. 7).

Таким образом, европейский регулятор спрашивает: «Что делает система? Какой риск она несёт для человека?». Российский законодатель задаёт иные вопросы: «Кто и где создал систему? Под чьим контролем она находится? Может ли ей доверять государство?». Европейская модель представляет собой управление рисками, российская – управление доверием через контроль происхождения.

Предполагается, что российский подход имеет определённые преимущества в контексте обеспечения национальной безопасности и технологического суверенитета, однако он менее гибок для регулирования стремительно развивающихся технологий. Классификация по происхождению быстро устаревает (сегодняшние «национальные модели» могут завтра использовать зарубежные компоненты), тогда как оценка рисков является более универсальным и долгосрочным инструментом.

4. Субъектный состав и распределение обязанностей

Правовое регулирование ИИ неизбежно предполагает определение круга субъектов, на которых возлагаются юридические обязанности. Оба анализируемых акта исходят из того, что сам ИИ не является субъектом права, он остаётся объектом, а ответственность несут люди и организации [3, с. 50].

AI Act в ст. 3 выделяет следующих операторов: провайдер (provider), пользователь (deployer), импортёр, дистрибьютор, уполномоченный представитель. Обязанности провайдера высокорисковых систем закреплены в ст. 16 и включают: создание системы менеджмента качества (ст. 17), ведение технической документации (ст. 11), логирование событий (ст. 12), постмаркетинговый мониторинг (ст. 72). Эта система детально проработана и ориентирована на непрерывный контроль соответствия.

Российский Законопроект в ст. 6 называет четырёх основных субъектов: разработчик модели, оператор системы, владелец сервиса и пользователь, а также органы государственной власти. Обязанности закреплены в ст. 10:

- Разработчик обязан обеспечить безопасность модели, исключить дискриминацию, документировать архитектуру, моделировать риски.

- Оператор обязан включить в документацию руководство по безопасной эксплуатации, тестировать систему, приостанавливать эксплуатацию при угрозе вреда, назначать ответственных лиц.

- Владелец сервиса обязан определить правила доступа, информировать пользователей о взаимодействии с ИИ, внедрять механизмы ограничения создания противоправного контента.

- Пользователь обязан соблюдать правила доступа и не обходить механизмы безопасности.

Интересно, что Законопроект РФ не использует термин «deployer» в том же смысле, что AI Act, а вместо этого вводит отдельную фигуру «пользователя сервиса». Это сужает сферу ответственности конечного потребителя, что, по нашему мнению, является разумным шагом, поскольку рядовой пользователь не обладает возможностями для оценки рисков ИИ-системы. В отличие от этого, AI Act возлагает значительный объём обязанностей на пользователя-развёртывающего (deployer), что может быть чрезмерным бременем для малого и среднего бизнеса.

5. Юридическая ответственность за вред, причинённый ИИ

Вопрос ответственности за вред, причинённый ИИ, является одним из наиболее дискуссионных как в доктрине, так и в законодательной практике. Так как отсутствие единой основы в понимании сущности искусственного интеллекта порождает правовую неопределённость, что напрямую влияет на механизмы ответственности.

AI Act устанавливает преимущественно административно-штрафную модель ответственности (глава XII). В Ст. 99 предусмотрено беспрецедентно высокие санкции: «Санкции достигают 35 млн евро или 7% мирового оборота, самые высокие штрафы в праве Европейского Союза» [1, с. 26]. Конкретно:

- за использование запрещённых практик (ст. 5) – до 35 млн евро или 7% годового оборота;

- за нарушение требований к высокорисковым системам – до 15 млн евро или 3% оборота;

- за предоставление неверной информации – до 7,5 млн евро или 1% оборота.

При этом сам AI Act не регулирует гражданско-правовую ответственность за вред, оставляя её действие проекту Директивы об ответственности в сфере ИИ (Proposed AI Liability Directive). Штрафы

налагаются публичными органами, а компенсация вреда потерпевшим осуществляется в рамках отдельных исков.

Российский Законопроект в ст. 11 предлагает иную гражданско-правовую модель:

Ответственность наступает соразмерно степени вины каждого субъекта (п. 1). Установлена презумпция вины разработчика, оператора и владельца: они несут ответственность, если «заведомо знали или должны были знать о возможности получения такого результата» (п. 2). Освобождение от ответственности возможно при наличии обстоятельств непреодолимой силы, умысла потерпевшего, а также если субъект предпринял «исчерпывающие меры» для предотвращения нарушения и соблюдал все требования законодательства (п. 3). Пользователь несёт ответственность только за умышленные действия или несоблюдение условий использования (п. 4).

Сравнение двух моделей позволяет сделать следующие выводы. Европейская модель представляет собой внешний контроль со стороны государства (надзорные органы налагают штрафы). Российская модель – внутреннее распределение рисков между участниками гражданского оборота с широкими возможностями судебной дискреции. Европейский подход обеспечивает большую определённость и предсказуемость (фиксированные штрафы), но может быть чрезмерно жёстким. Российский подход более гибок, однако содержит оценочные понятия («должен был знать», «исчерпывающие меры»), что создаёт правовую неопределённость и риск злоупотреблений. Представляется, что для России более предпочтительной была бы комбинированная модель: административные штрафы за грубые нарушения (по аналогии с AI Act) в дополнение к гражданско-правовой ответственности.

6. Интеллектуальная собственность и правовой режим обучения моделей

Наиболее существенное расхождение между двумя актами наблюдается в регулировании использования охраняемых произведений для обучения моделей ИИ. Это расхождение имеет не только теоретическое, но и огромное

практическое значение, поскольку именно данные, на которых обучаются модели, составляют основу их эффективности.

AI Act в п. 1 ст. 53 требует от провайдеров моделей общего назначения внедрить политику соблюдения авторского права, в частности, «выявлять и соблюдать оговорку об отказе от прав (opt-out) в соответствии с п. 3 ст. 4 Директивы (EU) 2019/790». Иными словами, правообладатель может явно запретить использование своих произведений для text and data mining. Это так называемая «модель opt-out»: использовать можно, если правообладатель не возражает, но его возражение имеет обязательную силу.

Российский Законопроект в п. 5 ст. 13 устанавливает прямо противоположный принцип. Согласно его положению, «не является нарушением авторских и (или) патентных прав извлечение информации из охраняемых объектов (включая компьютерную обработку, сравнение, классификацию, анализ закономерностей) для формирования наборов данных и/или обучения ИИ при условии, что у разработчика был правомерный экземпляр такого произведения либо объект был доведён до всеобщего сведения и доступен для анализа». Иными словами, российский законодатель выбирает «модель opt-in»? Нет, правильнее сказать модель «свободного использования» для целей обучения ИИ, если доступ к произведению был правомерным.

Как отмечает Макаров Т.И., «критерием для квалификации, что является творческой и (или) коммерческой деятельностью в этом контексте, является публичность, если произведение или информация каким-либо образом приобретают публичное распространение, то автор данных материалов должен быть идентифицирован» [2, с. 129]. Однако для целей обучения ИИ Законопроект делает исключение.

Сравнительный анализ показывает: европейский режим защищает права авторов (они могут запретить использование), российский, стимулирует разработчиков ИИ (им не нужно запрашивать разрешение). Европейский подход может затормозить развитие больших языковых моделей из-за

необходимости отслеживать opt-out каждого правообладателя. Российский подход создаёт благоприятные условия для отечественных разработчиков, но вступает в противоречие с международным авторским правом. Если российская модель будет обучаться на данных, полученных из европейских источников, такое обучение может быть признано нарушением Директивы 2019/790, что создаст правовые риски для экспорта российских ИИ-продуктов в ЕС.

Полагаем, что российский законодатель сделал осознанный выбор в пользу ускоренного развития национальной ИИ-индустрии, пожертвовав интересами отдельных правообладателей. Однако в долгосрочной перспективе необходимо выработать механизмы справедливого вознаграждения авторов, чьи произведения используются для обучения, например, через систему отчислений (роялти) или специальный налог.

7. Защита прав пользователей и право на отказ от искусственного интеллекта

Вопрос о том, насколько гражданин может контролировать взаимодействие с ИИ, является ключевым с точки зрения защиты прав человека в цифровую эпоху.

AI Act в ст. 50 устанавливает требования прозрачности: информирование о взаимодействии с ИИ (если это не очевидно), маркировка синтезированного контента (deepfake), раскрытие использования систем распознавания эмоций и биометрической классификации. Однако право на отказ от использования ИИ в AI Act прямо не предусмотрено.

Российский Законопроект в ст. 9 закрепляет уникальную норму: право гражданина на отказ от использования ИИ в предусмотренных Правительством РФ случаях. П. 3 гласит: «лицо, оказывающее услуги, обязано обеспечить возможность получения услуги в форме и порядке, не предусматривающем автономное использование технологий искусственного интеллекта». Кроме того, Проект закрепляет право на обжалование решений,

принятых с использованием ИИ (п. 4 ст. 9), и право на компенсацию вреда от неправомерного использования ИИ (п. 5 ст. 9).

Данное положение представляется одной из самых сильных сторон российского законопроекта. Оно имплементирует принцип «human in the loop» (человек в контуре принятия решений) и предоставляет гражданам защиту от полной автоматизации, особенно в социально значимых сферах (медицина, социальное обеспечение, государственные услуги). Европейский подход, при всей его строгости, не даёт гражданину права требовать человеческого рассмотрения, он лишь обязывает информировать о наличии ИИ. Российский подход идёт дальше: гражданин может потребовать, чтобы решение принял человек.

8. Регулирование фундаментальных (больших) моделей

Большие генеративные модели (ChatGPT, GigaChat и аналоги) представляют собой особую категорию ИИ, требующую специфического регулирования из-за их универсальности и масштаба.

AI Act посвящает целую главу (Глава V) моделям общего назначения (GPAI). Выделяются модели с системным риском (ст. 51), для которых установлены дополнительные обязательства: оценка модели, тестирование на уязвимости, снижение системных рисков, кибербезопасность (ст. 55). Все провайдеры GPAI обязаны предоставлять техническую документацию, сводку об обучающих данных и соблюдать авторские права (ст. 53). Как отмечается в литературе, «AI Act является уникальным и прорывным, он может быть сравнен по изложению материала с кодифицированным законодательством» [7, с. 282].

Российский Законопроект в ст. 7 вводит понятие «большие фундаментальные модели», но их регулирование строится исключительно на критериях локализации. Требования: все стадии разработки и обучения на территории РФ, силами российских лиц, под российским контролем. По сути, это инструмент технологического протекционизма, а не управления рисками, связанными с мощностью модели. Европейский подход обращает внимание на

вычислительную мощность (более 10^{25} FLOPs) и системный риск, то есть на объективные характеристики модели. Российский подход – на происхождение.

Полагаем, что регулирование больших моделей только по критерию происхождения недостаточно. Модель, созданная в России, но обладающая разрушительным потенциалом, может быть не менее опасной, чем зарубежная. Необходимо дополнить российский подход элементами риск-ориентированной оценки: установить пороговые значения по вычислительной мощности, объёму параметров и сфере применения, при достижении которых модель подлежит особому контролю (независимо от её «суверенности»).

Заключение

Проведённый сравнительный анализ позволяет сделать ряд обобщений и выводов, имеющих значение как для правовой доктрины, так и для законотворческой практики.

1. Формирование двух разнонаправленных моделей. Европейский AI Act и российский проект федерального закона представляют собой две принципиально разные парадигмы правового регулирования ИИ. Первая, риск-ориентированная, превентивная, с фокусом на защиту прав человека. Вторая, суверенно-ориентированная, стимулирующая, с фокусом на достижение технологической независимости. Как справедливо отмечает Астапенко П.Н., «ни одна страна не наделяет ИИ самостоятельной правосубъектностью. Вместо этого вырабатываются механизмы закрепления ответственности за человеком» [3, с. 52]. Однако пути выработки этих механизмов расходятся.

2. Ключевые точки расхождения. Наиболее существенные различия выявлены по следующим позициям: 1) основание классификации: риск нарушения прав человека (ЕС) или происхождение и уровень доверия к разработчику (РФ); 2) механизм ответственности: административные штрафы (ЕС) или гражданско-правовая ответственность с презумпцией вины (РФ); 3) режим интеллектуальной собственности: opt-out правообладателей (ЕС) или

свободное использование для обучения (РФ); 4) право на отказ от ИИ: отсутствует (ЕС) или закреплено (РФ).

3. Точки сходства. Несмотря на различия, оба акта признают необходимость: 1) прозрачности взаимодействия с ИИ (информирование пользователей); 2) человеческого надзора за критически важными системами; 3) запрета на манипулятивные и эксплуатирующие практики (хотя в российском проекте этот запрет сформулирован более общо, «эксплуатация уязвимостей человека» в ст. 3).

4. Рекомендации по совершенствованию российского законопроекта. Исходя из проведённого анализа, предлагается:

- Дополнить классификацию систем ИИ риск-ориентированными критериями (помимо критериев происхождения), особенно для моделей, применяемых в здравоохранении, правосудии и критической инфраструктуре.

- Уточнить оценочные понятия в ст. 11 («должен был знать», «исчерпывающие меры») через принятие подзаконных актов или разъяснений Верховного Суда РФ.

- Сохранить право на отказ от ИИ (ст. 9 Законопроекта) как уникальную и прогрессивную норму, но уточнить перечень случаев, когда такой отказ допустим.

- При сохранении либерального режима использования произведений для обучения (ст. 13) предусмотреть механизм последующего вознаграждения авторов, чьи работы внесли значительный вклад в формирование обучающих наборов данных.

5. Направления будущих исследований. Представляется необходимым дальнейшее изучение вопросов международно-правовой гармонизации регулирования ИИ. Как справедливо отмечает Иванов С.В., «для российской науки публичного права актуальны: сравнительный анализ моделей регулирования с учётом конституционно-правовых традиций; исследование механизмов защиты прав граждан от алгоритмических решений; разработка концепции ответственности за вред от ИИ в публичном секторе;

адаптация международных принципов (ОЭСР, ЮНЕСКО, Совета Европы) к национальной правовой системе» [1, с. 29]. Кроме того, требует отдельного анализа вопрос о правосубъектности ИИ: пока ни одна юрисдикция не пошла по пути признания ИИ субъектом права, однако дискуссии об «ограниченной правосубъектности» ведутся, и они заслуживают внимания [3, с. 50].

В завершение следует подчеркнуть: российский проект федерального закона представляет собой важный шаг вперёд, но не окончательный этап. Законодательство об ИИ должно быть динамичным, способным адаптироваться к стремительному технологическому развитию. Как полагают некоторые исследователи, «только риск-ориентированного подхода недостаточно для эффективного регулирования ИИ, необходима комбинация различных подходов» [8, с. 133]. Российский законопроект, при всех его достоинствах, нуждается в дополнении риск-ориентированными элементами, чтобы обеспечить баланс между суверенитетом и безопасностью человека.

Использованные источники:

1. Иванов С. В. Институт искусственного интеллекта в зарубежных системах публичного права / С. В. Иванов // Закон и власть – 2026. – № 1 – С. 26–30.

2. Макаров Т. И. Искусственный интеллект в российском законодательстве: предметы регулирования, права, обязанности и ответственность субъектов / Т. И. Макаров// Публично-правовые (государственно-правовые) науки – 2026. – № 111. – С. 125–134.

3. Астапенко П. Н. Сравнительный анализ правового регулирования искусственного интеллекта в России, Китае, США и Европейском союзе / П. Н. Астапенко // Закон и право – 2025. – № 6. – С. 47–54.

4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 // An official website of the European Union [Электронный ресурс]. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата обращения: 21.04.2026).

5. «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации»: Проект Федерального закона от 19.03.2026 ID: 166424 [Электронный ресурс]. URL: https://regulation.gov.ru/projects/166424/ (дата обращения: 21.04.2026).

6. Нурмагомедов Д. А. Анализ опыта правового регулирования использования технологий искусственного интеллекта в зарубежных странах / Д. А. Нурмагомедов // Государственная служба и кадры – 2026. – № 1. – С. 178–181.

7. Николаев Н. А., Касаткина Н. А., Гельдибаев М. Х. AI Act Еврокомиссии как первый регламент об использовании нейросетей / Н. А. Николаев, Н.А. Касаткина, М. Х. Гельдибаев // Закон и право – 2024. – № 8. – С. 279–283.

8. Pantsever K. A., Oztas B. AI regulation: Challenges, the EU AI Act and Turkey's approach / K. A. Pantsever, B. Ozta// Vestnik of Saint Petersburg University. International Relations – 2024. – Vol. 17. – Issue 2. – P. 131–142.