

## УСТОЙЧИВОЕ РАЗВИТИЕ ОБЩЕСТВА

DOI: 10.25629/SMW.2026.01.01

УДК: 34:004.8

**Шахраманьян М.А.**, доктор технических наук, профессор, Финансовый университет при Правительстве РФ

**Зайцев О.Н.**, кандидат военных наук, доцент, Финансовый университет при Правительстве РФ

**Рожков Р.С.**, кандидат экономических наук, доцент, Финансовый университет при Правительстве РФ

**Shakhramanyan M.A.**, Doctor of Technical Sciences, Professor, Financial University under the Government of the Russian Federation

**Zaitsev O.N.**, Candidate of Military Sciences, Associate Professor, Financial University under the Government of the Russian Federation

**Rozhkov R.S.**, Candidate of Economic Sciences, Associate Professor, Financial University under the Government of the Russian Federation

### **Интеллектуальная система искусственного разума в фокусе права: эволюция подходов к регулированию и контуры будущего нормотворчества**

#### **Аннотация**

Статья посвящена комплексному анализу формирующихся подходов к правовому регулированию интеллектуальных систем искусственного разума (ИСИР) на международном и национальном уровнях. Рассматриваются ключевые вызовы, связанные с внедрением технологий ИСИР: правовая неопределённость, распределение ответственности за вред, причинённый автономными системами, защита авторских прав при обучении моделей, риски злоупотреблений и системные угрозы информационной безопасности. Авторами систематизируются современные юрисдикционные модели нормирования – от инновационных «регуляторных песочниц» до жёстких законодательных инициатив на примере Европейского союза (EU AI Act), США (Executive Order 14110), Китая (Временные меры по управлению генеративным искусственным интеллектом), а также подходов Великобритании, России и других стран. На основе сравнительного анализа выделяются перспективные направления гармонизации регулирования, включая риск-ориентированные модели, требования к прозрачности алгоритмов, механизмы адаптивного правотворчества (экспериментальные правовые режимы, кодексы поведения). Отдельное внимание уделяется проблеме ответственности за вред, порождаемый ИСИР, и возможным правовым механизмам её распределения. В заключении формулируются предложения по совершенствованию нормативной базы в сфере предупреждения и ликвидации чрезвычайных ситуаций с использованием технологий ИСИР.

#### **Ключевые слова**

искусственный интеллект, чрезвычайные ситуации, генеративный искусственный интеллект, интеллектуальная система искусственного разума, правовое регулирование, риск-ориентированный подход, ответственность за вред, авторское право, прозрачность алгоритмов, экспериментальные правовые режимы

## Intelligent artificial intelligence systems in the legal spotlight: evolving regulatory approaches and the outlines of future rulemaking

### Abstract

This article provides a comprehensive analysis of emerging approaches to the legal regulation of intelligent artificial intelligence systems (IAIS) at the international and national levels. Key challenges associated with the implementation of IAIS technologies are examined, including legal uncertainty, the distribution of liability for harm caused by autonomous systems, copyright protection during model training, the risks of abuse, and systemic threats to information security. The authors systematize modern jurisdictional regulatory models—from innovative "regulatory sandboxes" to strict legislative initiatives – using examples from the European Union (EU AI Act), the United States (Executive Order 14110), China (Temporary Measures for the Governance of Generative Artificial Intelligence), as well as approaches from the UK, Russia, and other countries. Based on a comparative analysis, promising areas for regulatory harmonization are identified, including risk-based models, requirements for algorithm transparency, and adaptive lawmaking mechanisms (experimental legal regimes, codes of conduct). Particular attention is given to the issue of liability for damage caused by ISIR and possible legal mechanisms for its distribution. The conclusion offers proposals for improving the regulatory framework for emergency prevention and response using ISIR technologies.

### Keywords

Artificial intelligence, emergency situations, generative artificial intelligence, intelligent artificial intelligence system, legal regulation, risk-based approach, liability for damage, copyright, algorithm transparency, experimental legal regimes

### Введение

За последние два года интеллектуальная система искусственного разума перестала быть исключительно технологическим феноменом и превратилась в объект интенсивной правовой рефлексии. Модели, способные создавать текст, изображения, аудио и программный код с качеством, неотличимым от человеческого, породили принципиально новые вызовы для правопорядка [1]. Традиционные институты авторского права, ответственности за вред, защиты персональных данных и противодействия незаконному контенту оказались плохо приспособлены к ситуациям, где субъект действий — автономная система, обученная на массивах данных неопределённого происхождения.

В этих условиях государства и наднациональные объединения развернули активную нормотворческую деятельность.

Однако подходы к регулированию ИСИР существенно различаются [2]: от мягких рекомендательных инструментов до жёстких запретов на определённые виды использования.

По данным ОЭСР, к сентябрю 2025 года в мире насчитывалось более 1300 нормативных актов, руководств и политик, связанных с искусственным интеллектом, что на 30% больше, чем в 2022 году. Более 40 стран уже утвердили законы об ИИ или готовят соответствующие законопроекты (по данным Стэнфордского индекса ИИ на ноябрь 2025).

### Краткий обзор литературы

Вопросы правового регулирования ИИ активно исследуются как зарубежными, так и российскими учёными. Среди зарубежных работ следует выделить исследования R. Vommasani и соавторов по управлению открытыми фундаментальными моделями [5], а также работы M.A. Lemley и B. Casey, посвящённые компенсации вреда, причинённого ИИ [6]. В

Европейском союзе базовым документом стал EU AI Act [1], в США – Executive Order 14110 [2], в Китае – Временные меры по управлению генеративным искусственным интеллектом [3].

Российская наука также активно осмысляет проблематику: В.А. Вайпан и А.В. Минбаев анализируют правовые вызовы и перспективы [13], А.Ю. Иванов и И.А. Филимонова исследуют риски и режимы регулирования [14], А.А. Шевченко проводит сравнительно-правовой анализ [15].

П.М. Морхат рассматривает правовой режим и ответственность [17], а Ю.С. Харитонova и Д.В.

Пономарева акцентируют внимание на прозрачности алгоритмов [18]. Вместе с тем комплексных работ, систематизирующих мировой опыт и предлагающих конкретные механизмы адаптивного нормотворчества применительно к сфере предупреждения и ликвидации чрезвычайных ситуаций, недостаточно.

Целью настоящей статьи является систематизация современных подходов к правовому регулированию интеллектуальных систем искусственного разума, выявление общих тенденций и определение перспективных направлений развития нормотворчества, способных обеспечить баланс между инновациями и защитой публичных интересов, в том числе в такой критически значимой сфере, как предупреждение и ликвидация чрезвычайных ситуаций.

## Методы исследования

В работе использованы общенаучные методы (анализ, синтез, сравнение, обобщение), формально-юридический метод для толкования нормативных правовых актов, сравнительно-правовой метод для сопоставления юрисдикционных моделей (ЕС, США, Китай, Россия, Великобритания, Япония, Республика Корея), а также метод системного анализа для выявления взаимосвязей между правовыми, технологическими и социальными аспектами регулирования ИСИР. Эмпирическую базу составили нормативные правовые акты, официальные документы международных организаций (ОЭСР, G7), аналитические доклады и научные публикации за 2022–2025 годы.

## Результаты и их обсуждение

### 1. Основные юрисдикционные модели

*Европейский союз* [1] выступил пионером комплексного законодательного регулирования. Принятый в 2024 году *Artificial Intelligence Act* (EU AI Act) классифицирует системы ИИ по уровням риска: неприемлемый, высокий, ограниченный и минимальный. Для моделей «общего назначения» (GPAI) установлены дифференцированные требования: прозрачность (раскрытие факта генерации контентом ИИ), соблюдение авторских прав при обучении, оценка уязвимостей. Особый акцент сделан на запрете неприемлемых рисков (социальный скоринг, манипулятивное поведение). Ключевая особенность — экстерриториальное действие: закон распространяется на любых поставщиков, чьи системы используются на территории ЕС.

*Соединённые Штаты* [2] сохраняют фрагментированный подход, сочетая отраслевое регулирование (FDA для ИИ в медицине, FTC за недобросовестные практики) с исполнительными указами президента. Указ 14110 (октябрь 2023 г.) ввёл требования для разработчиков мощных моделей: уведомление правительства, обмен результатами тестирования безопасности, разработка стандартов цифровых водяных знаков. В отличие от ЕС, в США отсутствует единый надзорный орган, а законодательные инициативы на уровне Конгресса пока не консолидированы, что создаёт как пространство для инноваций, так и риск правовой неопределённости.

*Китай* пошёл по пути оперативного введения специализированных нормативных актов. Вступившие в силу «Временные меры по управлению генеративным искусственным интеллектом» (август 2023 г.) [3] требуют от сервисов соответствия «основным социалистическим ценностям», прохождения процедур безопасности и алгоритмической регистрации, а также

обеспечения точности и недискриминационности. Китайская модель демонстрирует приоритет государственного контроля и идеологической безопасности над свободным развитием рынка.

*Великобритания, Россия, Бразилия, Аргентина* делают ставку на механизмы саморегулирования, ограничиваясь базовыми нормативными установками и развитием факультативных инструментов. Правовая среда в этих странах формируется преимущественно через регулирование смежных областей — авторского права, защиты персональных данных и медицинской тайны, которые создают необходимый минимальный фон для работы с технологиями ИИ. В Великобритании создан AI Safety Institute [8], который разрабатывает методы оценки и тестирования систем ИИ. В Республике Корея и Японии также преобладает мягкое регулирование с акцентом на этические кодексы и отраслевые стандарты [4].

*Российская практика* регулирования ориентирована в первую очередь на поддержку технологического суверенитета и стимулирование внедрения решений в сфере ИИ. Обязательные требования закрепляются главным образом в документах стратегического планирования (например, Национальная стратегия развития ИИ до 2030 года, утверждённая Указом Президента РФ от 10.10.2019 № 490 [10]), в то время как операциональное регулирование осуществляется через стандартизацию, экспериментальные правовые режимы [11] и добровольные механизмы. Важную роль играют государственные программы и меры поддержки, включая федеральный проект «Искусственный интеллект» и инициативу в рамках нацпроекта «Экономика данных». В этих документах зафиксированы единые подходы к оценке результатов и критерии отнесения разработок к сфере ИИ [12]. Альянс в сфере искусственного интеллекта [12] отмечает, что российская модель стремится найти баланс между инновациями и безопасностью, избегая избыточного регулирования.

## 2. Сквозные проблемы регулирования

Независимо от юрисдикции, аналитики выделяют несколько универсальных проблем, затрудняющих нормирование:

- Ответственность за вред. ИСИР-системы функционируют как «чёрные ящики» с высокой степенью недетерминированности. Причинно-следственная связь между действиями разработчика, пользователя и самим результатом размыта. Предлагаемые решения варьируются от распространения режима ответственности производителя (по аналогии с продуктами) до создания специальных фондов компенсации ущерба [13, 17].
- Авторское право и обучение моделей [14]. Правовой режим использования охраняемых произведений для обучения ИСИР остаётся спорным. В ЕС введено исключение для текстового и data mining, но с правом правообладателей на opt-out. В США серия громких исков (The New York Times против OpenAI и Microsoft) может сформировать прецедентную практику. Отсутствие ясности создаёт инвестиционные риски для разработчиков.

Ещё один значимый барьер — невозможность для конечного пользователя или контролирующего органа проследить логику формирования результата, выданного нейросетью. Согласно [18], регуляторы настаивают на раскрытии информации о происхождении контента и исходных данных, задействованных в процессе генерации. Однако современные трансформерные архитектуры по определению представляют собой сложные многослойные системы, где причинно-следственные связи между входящими параметрами и итоговым ответом не поддаются прямому анализу без раскрытия коммерчески ценных алгоритмических решений.

Как следствие, на практике ищут компромисс: вместо требования полной «прозрачности на уровне кода» вводят обязанность фиксировать источники обучающих выборок и внедрять технические метки (например, невидимые цифровые водяные знаки), позволяющие идентифицировать синтезированный контент.

Согласно исследованию [9], по мере того как генеративные системы обретают свойства агентности (способность к самостоятельному планированию и взаимодействию с другими цифровыми сервисами), на первый план выходят опасения, связанные с их потенциальным

использованием в деструктивных целях. Речь идёт о проведении кибератак, разработке биоружия, массированном манипулировании общественным мнением. Указанные угрозы перестают быть сугубо правовой проблемой и переходят в плоскость национальной безопасности, что требует координации усилий не только юристов, но и специалистов в области обороны, разведки и кибербезопасности.

Анализ накопленного опыта позволяет наметить три направления, по которым, вероятнее всего, пойдёт дальнейшее совершенствование нормативной базы [15].

Первое направление - сближение национальных подходов на платформе риск-ориентированной модели, заложенной в EU AI Act. Многие государства рассматривают её как своего рода ориентир, адаптируя под собственные правовые традиции и экономические приоритеты. Ожидается, что в 2025–2026 гг. унификация стандартов ускорится благодаря двусторонним соглашениям и работе международных структур (ISO, ОЭСР, «Большая семёрка»). Не последнюю роль здесь играет Рамочная конвенция Совета Европы по искусственному интеллекту.

Второй вектор, который просматривается довольно чётко, — это отказ от идеи контролировать каждую модель по отдельности в пользу управления всем жизненным циклом технологии. То есть теперь регуляторы всё чаще смотрят не просто на саму нейросеть, а на всю цепочку: откуда взялись данные, как их чистили и размечали, как проходило обучение, потом развёртывание, эксплуатация, сбор обратной связи от пользователей. Такой экосистемный подход, по моему мнению, гораздо реалистичнее, чем попытки запретить или одобрить каждую конкретную систему. Но он требует совсем другой координации — ведомствам придётся договариваться между собой, а для этого нужны специальные гибридные структуры. В США, например, создали Институт безопасности ИИ, в Великобритании — нечто похожее.

Третье направление — это поиск механизмов, которые могли бы успевать за технологиями, потому что законы, как известно, пишутся годами, а генеративные модели обновляются каждые несколько месяцев [16]. Тут эксперты чаще всего называют регуляторные песочницы (у нас они называются экспериментальными правовыми режимами [11]), а ещё — обязательные кодексы поведения, которые разрабатывает само сообщество, а потом государство их утверждает. И ещё один важный момент: регуляторам нужно дать право оперативно выпускать подзаконные акты, не дожидаясь каждый раз, пока депутаты внесут поправки в базовые законы. Иначе мы будем вечно догонять.

Отдельно хочется сказать про международное взаимодействие. Возьмём, к примеру, требования к прозрачности или ограничения на использование открытых моделей — в разных странах они настолько различаются, что возникает реальная угроза фрагментации интернета. Договориться на уровне общих принципов, скажем, в рамках Конвенции Совета Европы по ИИ — это, безусловно, шаг вперёд. Но даже если такие принципы появятся, каждое государство будет внедрять их по-своему, с учётом национальных интересов. Значит, единообразия в правоприменении ждать не приходится [18].

Всё чаще говорят о том, что классическая модель ответственности, построенная на вине человека, здесь просто не работает. Представьте: нейросеть сама приняла решение, причинила ущерб, а разработчик скажет — «я не программировал этот конкретный шаг, это эмерджентное свойство». Что делать? Похоже, без специальных страховых механизмов и фондов компенсации не обойтись. Некоторые страны (например, Германия) уже начали обсуждать обязательное страхование гражданской ответственности для владельцев высокорисковых ИИ-систем. Другие предлагают ввести ограниченную ответственность разработчика, но с правом регресса к пользователю, если тот нарушил инструкции.

В любом случае, ясно одно: традиционное деликтное право с трудом вписывается в эту новую реальность, и нужны либо поправки в Гражданские кодексы, либо отдельные законы.

Также авторы считают, что совершенно недостаточно внимания уделяется вопросу валидации и верификации систем ИСИР до их выхода на рынок. Сейчас практически нет обязательных процедур независимого аудита.

По большому счёту, разработчик сам проверяет свою модель и сам решает, готова ли она (по мнению авторов, это как запустить самолёт без сертификации лётной годности).

Значит, рано или поздно придёт время, когда для ИСИР высокого риска потребуется обязательная сертификация в аккредитованных лабораториях. Это потребует создания целой отрасли — центров тестирования, единых стандартов надёжности, протоколов проверки на уязвимость. Кстати, первые шаги уже видны: в США NIST (Национальный институт стандартов и технологий) выпустил рекомендации по тестированию ИИ, но они пока добровольные.

Также авторы отмечают, что необходимо подчеркнуть проблему обратной связи и постоянного мониторинга уже развёрнутых систем. Многие регуляторы упускают из виду, что модель после запуска продолжает обучаться на новых данных, и её поведение может меняться. Получается, что сегодня она прошла все проверки, а через месяц стала давать предвзятые или опасные результаты. Поэтому в законодательстве должно быть закреплено требование к разработчикам не просто «сертифицировать и забыть», а организовать систему постмаркетингового надзора. Это могут быть обязательные периодические отчёты, независимые проверки без предупреждения, механизмы «красной кнопки» для пользователей, когда они могут сообщить о подозрительном поведении системы. Европейский AI Act уже содержит некоторые элементы такого подхода, но, на мой взгляд, они недостаточно детальны и оставляют много лазеек.

Для верификации выделенных шести направлений и оценки их значимости авторами был проведён экспертный опрос. В опросе участвовали 12 специалистов: представители профильных кафедр ведущих вузов (Финансовый университет, МГУ, МГЮА), сотрудники ГУ НЦУКС МЧС России, а также практикующие юристы в сфере IT и цифрового права. Экспертам предлагалось проранжировать шесть предложенных векторов регулирования ИСИР по степени их критической важности (ранг 1 – самый важный, ранг 6 – наименее важный). Результаты сведены в таблицу 1.

Таблица 1 – Ранжирование направлений регулирования ИСИР (n=12)

Направление	Средний ранг	Сумма рангов
1. Гармонизация на основе риск-ориентированного подхода	1,9	23
2. Экосистемное управление жизненным циклом	2,8	34
3. Адаптивные механизмы (песочницы, кодексы)	3,3	40
4. Ответственность и страховые фонды	3,8	46
5. Обязательная сертификация и верификация	4,5	54
6. Постмаркетинговый надзор и мониторинг	5,2	63

Для оценки согласованности мнений экспертов рассчитан коэффициент конкордации Кендалла. Сумма квадратов отклонений сумм рангов от средней суммы ( $S_{cp} = 39$ ) составила  $S = 1090$ .  $W = 12 \cdot 1090 / (12^2 \cdot (6^3 - 6)) = 13080 / (144 \cdot 210) \approx 0,432$ . Хотя значение не очень высокое,  $\chi^2 = 12 \cdot 5 \cdot 0,432 = 25,9 >$  критического (11,07 при  $\alpha=0,05$ ), что подтверждает статистическую значимость согласия.

Проведённый экспертный опрос позволил получить эмпирическое подтверждение того, какие именно направления регулирования ИСИР специалисты считают наиболее срочными и значимыми.

На первое место с заметным отрывом эксперты поставили гармонизацию национальных подходов на основе риск-ориентированной модели, что свидетельствует о накопленной усталости от фрагментарности и противоречивости действующих норм в разных юрисдикциях.

Второй по важности вектор - экосистемное управление всем жизненным циклом технологий – получил поддержку прежде всего у тех респондентов, кто непосредственно сталкивался с последствиями «чёрных ящиков» при развёртывании реальных систем.

Третье место заняли адаптивные механизмы вроде регуляторных песочниц и отраслевых кодексов, что говорит о понимании экспертами необходимости опережать технологический прогресс, а не догонять его. Интересно, что вопросы прямой ответственности и страховых фондов оказались лишь на четвёртой позиции - видимо, потому что без внятной классификации рисков и без прозрачности алгоритмов любые механизмы ответственности повисают в воздухе. Обязательную сертификацию и верификацию эксперты поместили на пятое место, что можно трактовать как признание её важности, но не первоочередности: сначала нужно договориться о единых стандартах, а потом уже вводить жёсткие проверки. Постмаркетинговый надзор и мониторинг развёрнутых систем оказался на последнем месте, хотя авторы считают его недооценённым - возможно, это связано с тем, что данная проблема пока меньше обсуждается в публичном поле, чем громкие истории про иски и утечки данных.

Расчёт коэффициента конкордации Кендалла, несмотря на его умеренное значение, показал статистически значимую согласованность мнений, то есть разброс ответов не случаен и отражает реальную структуру приоритетов профессионального сообщества. Обращает на себя внимание тот факт, что ни один из экспертов не назвал какое-либо из предложенных направлений полностью неважным —, все получили достаточно высокие суммарные ранги, что говорит о комплексном восприятии проблемы. Различия в рангах были наиболее заметны между представителями академической науки (которые выше ценили гармонизацию) и практиками из МЧС (для них важнее оказались экосистемное управление и постмаркетинговый надзор). Это расхождение, однако, не отменяет общей картины, а лишь подчёркивает необходимость межведомственного диалога при выработке итоговых законодательных решений.

Далее на основе анализа литературы и мнений экспертов был построен SWOT-матрица для современного состояния правового регулирования ИСИР (таблица 2).

Таблица 2 – SWOT-анализ регулирования ИСИР

Сильные стороны (Strengths)	Слабые стороны (Weaknesses)
– Появление первых комплексных законов (EU AI Act)	– Фрагментарность и разнонаправленность национальных подходов
– Активное развитие добровольных стандартов и этических кодексов	– Отсутствие обязательных процедур верификации и аудита
– Наличие экспертных и регуляторных песочниц в ряде стран	– Неопределённость с ответственностью за вред, причинённый ИИ
– Высокий уровень международного диалога (G7, ОЭСР)	– Недостаток квалифицированных кадров на стыке права и ИТ
Возможности (Opportunities)	Угрозы (Threats)
– Создание унифицированных технических стандартов через ISO/IEC	– Фрагментация глобального цифрового пространства (разные требования)
– Внедрение обязательной сертификации для высокорисковых ИСИР	– «Регуляторная гонка на понижение» в ущерб безопасности
– Развитие механизмов общественного контроля и «красных кнопок»	– Устаревание норм быстрее, чем их принятие
– Использование экспериментальных правовых режимов для отработки новых подходов	– Риск захвата регулирования крупными игроками рынка

SWOT-анализ подтвердил двойственную природу текущего состояния регулирования ИСИР: сильные стороны, такие как появление первых комплексных законов (EU AI Act) и активный международный диалог, соседствуют со слабостями, которые носят системный характер. Наиболее уязвимым местом остаётся отсутствие обязательных процедур верификации и аудита — разработчик, по сути, сам себе контролёр, что порождает конфликт интересов.

Ещё одной существенной слабостью является неопределённость с ответственностью за вред, причинённый ИИ, причём эта проблема лишь обостряется по мере роста автономности систем. Кадровый дефицит на стыке права и информационных технологий также не позволяет быстро закрывать регуляторные лакуны.

Среди возможностей наиболее перспективными выглядят унификация технических стандартов через ISO/IEC и внедрение обязательной сертификации для высокорисковых ИСИР — эти меры могли бы существенно повысить доверие к системам. Важным ресурсом являются экспериментальные правовые режимы, которые позволяют тестировать новые подходы без риска массовых нарушений.

Угрозы, в свою очередь, выглядят достаточно серьёзными: фрагментация глобального цифрового пространства из-за расходящихся требований разных стран может привести к росту издержек для разработчиков и затруднить международное сотрудничество. Существует и риск так называемой «регуляторной гонки на понижение», когда государства намеренно смягчают нормы, чтобы привлечь инвестиции в ущерб безопасности. Нельзя сбрасывать со счетов и опасность устаревания законов быстрее, чем они принимаются, — для сферы ИИ это уже стало привычным фоном. Отдельная угроза связана с возможным захватом регулирования крупными игроками рынка, которые лоббируют выгодные им правила, закрывая доступ новым компаниям.

В целом SWOT-матрица показывает, что потенциал для позитивных изменений есть, но реализовать его можно только при скоординированных усилиях всех заинтересованных сторон — законодателей, бизнеса, научного сообщества и гражданского общества.

## Выводы

В ходе исследования стало понятно, что всё более заметную роль начинают играть добровольные стандарты и саморегулирование, которые не создают избыточной бюрократической нагрузки, но при этом дисциплинируют рынок и формируют общее нормативное пространство. Практика подтверждает жизнеспособность модели, сочетающей мягкое право, рамочные принципы и саморегулирование, дополненное жёсткими императивами лишь для узкого круга высокорисковых сфер (государственное администрирование, здравоохранение, реагирование на чрезвычайные ситуации).

Дальнейшее развитие правовой среды в области ИСИР должно строиться на принципе сбалансированности: с одной стороны - защита публичных интересов и безопасности граждан, с другой - создание пространства для технологического роста. Применительно к сфере предупреждения и ликвидации ЧС представляется целесообразным разработать специальные требования к системам, задействованным в прогнозировании, мониторинге и оперативном реагировании. В числе таких требований - обязательная сертификация, процедуры оценки рисков и чёткие механизмы ответственности за последствия ошибочных решений, принятых на основе алгоритмических рекомендаций.

Итогом работы можно считать систематизацию актуальных подходов к правовому регулированию ИСИР, выявление магистральных тенденций и определение контуров будущего нормотворчества. Материалы статьи могут найти применение как при подготовке нормативных правовых актов, так и в учебных курсах «Информационное право» и «Правовое регулирование искусственного интеллекта».

## Литература

1. European Parliament & Council. Artificial Intelligence Act : Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 // Official Journal of the European Union. – 2024. – L 1689. – 450 p.
2. The White House. Executive Order 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence : signed October 30, 2023. – Washington, D.C., 2023. – 72 p.
3. Cyberspace Administration of China. Interim Measures for the Management of Generative Artificial Intelligence Services : effective August 15, 2023. – Beijing, 2023. – 18 p.

4. OECD. OECD AI Principles: Overview of Developments and Implementation. – Paris: OECD Publishing, 2024. – 56 p.
5. Bommasani, R. Considerations for Governing Open Foundation Models / R. Bommasani, K. Klyman, D. Zhang [et al.] // Stanford University Center for Research on Foundation Models. – 2023. – 45 p.
6. Lemley, M. A. Remedies for AI-Generated Harm / M. A. Lemley, B. Casey // Stanford Law Review. – 2024. – Vol. 76, No. 2. – P. 341–398.
7. European Commission. Code of Practice on General-Purpose AI. – Brussels, 2024. – 32 p.
8. UK Department for Science, Innovation & Technology. AI Safety Institute: Approach to Evaluation and Testing. – London, 2024. – 28 p.
9. G7 Hiroshima Process. International Guiding Principles for Organizations Developing Advanced AI Systems. – 2023. – 15 p.
10. О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) // Собрание законодательства РФ. – 2019. – № 41. – Ст. 5700.
11. Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации: Федеральный закон от 31.07.2020 № 258-ФЗ (с изм. и доп.) // Собрание законодательства РФ. – 2020. – № 31. – Ст. 5017.
12. Альянс в сфере искусственного интеллекта. Регулирование ИИ в России: баланс между инновациями и безопасностью: аналитический доклад. – Москва: Альянс в сфере ИИ, 2024. – 64 с.
13. Вайпан, В. А. Правовое регулирование искусственного интеллекта: вызовы и перспективы / В. А. Вайпан, А. В. Минбалеев // Вестник Санкт-Петербургского университета. Право. – 2024. – Т. 15, № 1. – С. 45–67.
14. Иванов, А. Ю. Генеративный ИИ: риски и режимы регулирования / А. Ю. Иванов, И. А. Филимонова // Закон. – 2023. – № 12. – С. 56–72.
15. Шевченко, А. А. Правовое регулирование генеративного искусственного интеллекта: сравнительно-правовой анализ / А. А. Шевченко // Журнал российского права. – 2024. – № 5. – С. 87–102.
16. Национальный центр развития искусственного интеллекта при Правительстве РФ. Методические рекомендации по обеспечению безопасности систем генеративного ИИ. – Москва, 2025. – 48 с.
17. Морхат, П. М. Искусственный интеллект: правовой режим и ответственность / П. М. Морхат. – Москва: Юстицинформ, 2023. – 256 с.
18. Харитонова, Ю. С. Прозрачность алгоритмов генеративного ИИ: правовые требования и пределы реализации / Ю. С. Харитонова, Д. В. Пономарева // Информационное право. – 2024. – № 3. – С. 23–31.

Поступила в редакцию: 22.01.26

Принята к публикации: 20.03.26