

Дата поступления рукописи в редакцию: 05.10.2026 г.

DOI: 10.24412/2076-1503-2026-10-415-422

Дата принятия рукописи в печать: 29.10.2026 г.

ОЛЕЙНИКОВ Олег Владимирович,
кандидат юридических наук, доцент
кафедры бизнес-процесса и экономической безопасности
НАН ЧОУ ВО «Академия маркетинга и социально-
информационных технологий - ИМСИТ»,
Краснодар, Россия,
e-mail: oleynikovnvr@mail.ru

ПЕТРУШИН Константин Игоревич,
студент 2 курса магистратуры,
направление подготовки 40.04.01 «Юриспруденция»
НАН ЧОУ ВО «Академия маркетинга и социально-
информационных технологий - ИМСИТ»,
Краснодар, Россия,
e-mail: petrushin.k@gmail.ru

АГАДЖАНИЯ Давид Арутюнович,
студент 2 курса,
направление подготовки 09.03.01
«Информатика и вычислительная техника»
НАН ЧОУ ВО «Академия маркетинга и социально-
информационных технологий - ИМСИТ»,
Краснодар, Россия,
e-mail: mail@law-books.ru

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЧЕЛОВЕЧЕСКОГО КОНТРОЛЯ НАД ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ В РОССИИ И ПУТИ ИХ РЕШЕНИЯ

Аннотация. В настоящем исследовании анализируются существующие правовые механизмы, призванные обеспечить эффективный человеческий контроль над функционированием систем искусственного интеллекта (ИИ). Особое внимание уделяется эволюции регуляторного подхода: от формальной концепции «человек в контуре», предполагающей лишь номинальное присутствие оператора, к более строгому стандарту «содержательного человеческого контроля». Последний требует, чтобы субъект не просто механически подтверждал действия алгоритма, но и обладал реальным пониманием логики работы ИИ, а также фактической возможностью своевременно вмешаться в его работу. В ходе исследования выявлены системные пробелы в действующем законодательстве, среди которых: отсутствие легального закрепления понятия человеческого контроля, явный технологический перекося в обязанностях разработчиков, делегирование стандартов маркировки синтетического контента на усмотрение частных соглашений, а также отсутствие специализированного режима юридической ответственности. На основе проведенного анализа авторами предложен комплекс конкретных мер, направленных на совершенствование нормативно-правовой базы.

Ключевые слова: искусственный интеллект, человек в контуре, содержательный человеческий контроль, большие фундаментальные модели, деликтная ответственность, маркировка синтетического контента.

Для цитирования: Олейников О. В., Петрушин К. И., Агаджанян Д. А. Проблемы правового регулирования человеческого контроля над искусственным интеллектом в России и пути их решения // Образование и право. 2026. № 10. С. 415–422.

OLEYNIKOV Oleg Vladimirovich,
Candidate of Legal Sciences, Associate Professor
Department of Business Processes and Economic Security
Academy of Marketing and Social-Information
Technologies (IMSIT),
Krasnodar, Russia

PETRUSHIN Konstantin Igorevich,
2nd-year Master's student,
Field of study: 40.04.01 "Jurisprudence"
Academy of Marketing and Social-Information
Technologies (IMSIT),
Krasnodar, Russia

AGADZHANYAN David Arutyunovich,
2nd-year student,
Field of study: 09.03.01
"Informatics and Computer Engineering"
Academy of Marketing and Social-Information
Technologies (IMSIT),
Krasnodar, Russia

ISSUES REGARDING THE LEGAL REGULATION OF HUMAN CONTROL OVER ARTIFICIAL INTELLIGENCE IN RUSSIA AND WAYS TO ADDRESS THEM

Annotation. This study analyzes existing legal mechanisms designed to ensure effective human control over the functioning of artificial intelligence (AI) systems. Particular attention is paid to the evolution of the regulatory approach: from the formal "human-in-the-loop" concept—which implies only a nominal presence of an operator—to the more rigorous standard of "meaningful human control." The latter requires that an individual not merely provide a mechanical confirmation of an algorithm's actions, but also possess a genuine understanding of the AI's operational logic, as well as the practical ability to intervene in its functioning in a timely manner. The study identifies systemic gaps in current legislation, including the lack of a formal legal definition for "human control," a pronounced technological bias in the obligations imposed on developers, the delegation of standards for labeling synthetic content to private agreements, and the absence of a specialized legal liability regime. Based on this analysis, the authors propose a set of concrete measures aimed at improving the regulatory framework.

Key words: artificial intelligence, human-in-the-loop, meaningful human control, large foundational models, tort liability, labeling of synthetic content.

For citation: Oleynikov O. V., Petrushin K. I., Agadzhanian D. A. Issues regarding the legal regulation of human control over artificial intelligence in Russia and ways to address them. *Education and law*. 2026;(10):415–422. (In Russ.).

К 2026 году технологии искусственного интеллекта трансформировались из экспериментальных разработок в неотъемлемый элемент критической информационной и производственной инфраструктуры. Особую правовую обеспокоенность вызывает стремительное развитие агентных систем ИИ – автономных программных комплексов, способных выполнять многоуровневые задачи без необходимости постоянного прямого вмешательства человека. В этой связи возникает острый правовой парадокс: законодательство им-

перативно требует сохранения человеческого контроля над ИИ, однако архитектура современных глубоких нейросетей зачастую делает осмысленное вмешательство либо технически нереализуемым, либо когнитивно бессмысленным для оператора.

Принятие Федерального закона от 26 июля 2026 г. № 243-ФЗ «О поддержке развития технологий искусственного интеллекта в Российской Федерации» (далее – Федеральный закон № 243-ФЗ) стало знаковым этапом в формировании

отечественного регулирования данной сферы [9]. Указанный акт вводит категорию больших фундаментальных моделей (БФМ), регламентирует требования к суверенным и национальным моделям, а также закрепляет обязанности разработчиков и механизмы маркировки контента. Тем не менее, закон оставляет без детальной проработки фундаментальный вопрос: каким образом гарантировать содержательный, а не декларативный, человеческий контроль над системами ИИ?

Целью данной работы является выявление пробелов в существующих механизмах человеческого надзора, комплексный анализ положений Федерального закона № 243-ФЗ и формулирование предложений по их нормативному совершенствованию.

Концепция содержательного человеческого контроля (Meaningful Human Control, МНС) над ИИ предполагает, что человек должен сохранять дееспособность и фактическую возможность оценивать обстановку, осознавать последствия принимаемых решений и нести за них персональную ответственность в процессе взаимодействия с интеллектуальными системами [1]. Ключевой тезис заключается в том, что человек не должен превращаться в формальную «галочку» или «резиную печать» в цепочке автоматизированного принятия решений. Данная концепция базируется на трех столпах:

Осознанное принятие решений. Оператор обязан анализировать контекст, этические дилеммы и реальные риски, а не слепо подтверждать выводы, сгенерированные ИИ.

Персонификация ответственности. Даже в условиях высокой автономности системы, бремя ответственности за итоговое решение остается за человеком, особенно при функционировании ИИ в социально значимых и критических сферах.

Сохранение контроля в нештатных ситуациях. Принцип не подразумевает, что оператор должен непрерывно мониторить каждый шаг алгоритма. Он предполагает наличие надежных технических и организационных механизмов, позволяющих перехватить управление, если система допустила сбой или вошла в противоречивое состояние.

Иными словами, простого физического присутствия человека за пультом управления недостаточно. Оператор должен понимать логику работы системы и обладать реальными рычагами для своевременного вмешательства. Если сотрудник лишь нажимает кнопку «Подтвердить», не имея инструментов для верификации алгоритмической логики, мы имеем дело не с контролем, а с его опасной имитацией.

Подходы к обеспечению человеческого кон-

троля над ИИ в различных правовых системах (ЕС, США, Китай и Россия) существенно различаются по степени императивности и детализации.

Европейский союз в статье 14 Регламента об искусственном интеллекте (EU AI Act, 2024) детально регламентирует архитектуру надзора за системами высокого риска. Документ содержит прямое предписание: система должна проектироваться таким образом, чтобы физическое лицо имело практическую и техническую возможность контролировать её функционирование, а при необходимости — оперативно вмешаться и остановить процесс. Если надзор существует исключительно на бумаге, не подкрепляясь реальными инструментами вмешательства, это квалифицируется как нарушение регламента [4].

В США базовым документом выступает «Система управления рисками с использованием искусственного интеллекта» (NIST AI RMF, 2023), которая пока носит рекомендательный характер. Однако на уровне отдельных штатов внедряются жесткие регуляторные требования. Так, в Нью-Йорке в соответствии с Законом об автоматизированных инструментах принятия решений в сфере занятости (Local Law 144) работодатели обязаны проводить независимый аудит алгоритмов, применяемых при найме персонала, на предмет выявления дискриминации кандидатов по защищаемым признакам: расе, этнической принадлежности или полу [5].

В Китае «Временные меры по управлению службами генеративного искусственного интеллекта» (2023) возлагают на поставщиков услуг прямую ответственность за весь сгенерированный контент. Для минимизации рисков документ предписывает внедрение строгих технических и организационных барьеров: компании обязаны разрабатывать четкие регламенты маркировки синтетического контента, проводить регулярную оценку качества, осуществлять выборочные проверки и контролировать исполнение внутренних правил [6].

В России же Федеральный закон № 243-ФЗ пока ограничивается декларацией принципа «уважения автономии и свободы воли человека» (п. 4 ст. 4), не формулируя конкретных императивных требований к механизмам осуществления такого контроля [9].

Таблица 1. Требования к человеческому контролю в разных юрисдикциях

Предпосылки для выстраивания человеческого контроля заложены в положениях Федерального закона № 243-ФЗ, который дифференцирует большие фундаментальные модели ИИ на суверенные и национальные (ст. 6). Оба данных статуса предполагают, что разработчиком выступает

российское юридическое лицо, а обработка данных осуществляется на территории РФ. Статус суверенной модели дополнительно требует обеспечения полной технической воспроизводимости всего цикла разработки. Национальная модель обязывает, чтобы её ключевые характеристики определялись исключительно российским юридическим лицом.

Критерий	Россия	Китай	США	ЕС
Обязательность HTML	Декларируется как принцип	Обязательна для публичного контента	Рекомендательно; обязательна в отдельных штатах	Строго для высокого риска
Стандарт компетентности	Отсутствует	Проверка ценностей	Оценка рисков	«Правильное понимание»
Ответственность	Общий деликтный режим	Административная и уголовная	Договорная; деликтная	Презумпция вины поставщика
Маркировка	Платформы >500 тыс. пользователей	Обязательна	Фрагментарно	Обязательна

С позиции человеческого контроля это формирует важную правовую предпосылку: субъект контроля становится четко идентифицируемым. Российское юридическое лицо может быть привлечено к ответственности в рамках российской юрисдикции и обязано предоставлять необходимую документацию регуляторам. Более того, интерфейс и техническая документация должны быть представлены на русском языке, что является базовым условием для понимания оператором логики работы системы [13].

Однако данное регулирование имеет существенное ограничение. Закон четко определяет, кто осуществляет контроль, но не отвечает на вопросы, как именно и в каком объеме он должен осуществляться. Сам факт того, что разработчиком является отечественная компания, не гарантирует наличия внутри неё эффективных механизмов надзора. Российская организация вполне может эксплуатировать оператора по принципу «резиновой печати» — сотрудника, который лишь формально, без анализа, подтверждает решения алгоритма [14].

Статья 8 Федерального закона № 243-ФЗ закрепляет три основные обязанности разработчика:

- принятие организационных и технических мер по обеспечению безопасности модели;
- определение правил эксплуатации модели;
- ведение технической документации.

Все перечисленные обязанности ориентированы преимущественно на техническую безопасность, а не на проектирование эффективных механизмов человеческого надзора. Закон не обязывает разработчика доказывать, что его си-

стема «поддается эффективному человеческому пониманию», и не требует внедрения интерфейсов объяснимости (Explainable AI, XAI). Иными словами, человеческий контроль рассматривается законодателем как второстепенный придаток технической безопасности, а не как самостоятельное и равнозначное требование. Это вступает в противоречие с теорией МНС, согласно которой контроль должен быть заложен в архитектуру системы на этапе проектирования, а не добавляться постфактум.

Статья 9 Федерального закона № 243-ФЗ регламентирует механизм маркировки контента, созданного с помощью ИИ. Платформы с суточной аудиторией более 500 тысяч пользователей обязаны предоставлять пользователям функционал для размещения предупреждений о применении ИИ. Однако часть 2 статьи 9 устанавливает, что «формат, содержание и порядок размещения информационного предупреждения определяются соглашением между лицом, применяющим большую фундаментальную модель, и лицом, предоставляющим возможность её применения». Это означает, что стандарты маркировки делегируются на уровень рыночных соглашений, а не регулируются императивной нормой права. С точки зрения человеческого контроля это является нормативным дефектом: маркировка служит предварительным условием для получения надзирающим субъектом релевантной информации. Если стандарты определяются частными соглашениями, маркировка на различных платформах станет несопоставимой. В результате модератор или конечный пользователь не сможет сформировать целостную и достоверную картину. Кроме того, отсутствие единого законодательного стандарта создает высокие риски манипулятивного использования маркировки в целях введения потребителей в заблуждение.

Часть 2 статьи 10 Федерального закона № 243-ФЗ устанавливает широкое исключение из ответственности за использование объектов авторского права для обучения моделей. Если произведение является общедоступным и не защищено техническими средствами защиты, его допускается использовать для обучения без согласия правообладателя. С позиции человеческого контроля это также выступает структурным дефектом: правообладатель полностью исключается из процесса контроля над решением об использовании его интеллектуальной собственности. Он лишен возможности как запретить такое использование, так и получить информацию о нем [2; 3].

Статья 11 Федерального закона № 243-ФЗ содержит лишь отсылочную норму: «за нарушение настоящего Федерального закона... участники от-

ношений... несут ответственность в соответствии с законодательством Российской Федерации». Это означает, что при причинении вреда большой фундаментальной моделью ответственность будет регулироваться общими нормами ГК РФ (в частности, ст. 1064). Однако применимость этих общих деликтных норм к автономным системам ИИ сама по себе является острой и до конца не решенной доктринальной проблемой. Возникает классический «разрыв ответственности» (liability gap): вред причинен, но привлечь к ответственности конкретное виновное лицо крайне сложно, поскольку общие нормы или правила об ответственности за источник повышенной опасности (ст. 1079 ГК РФ) плохо адаптированы к самостоятельным, непредсказуемым действиям нейросетей, не обладающих правосубъектностью.

Ранее проведенные эмпирические исследования демонстрируют, что операторы склонны к «эффекту автоматизации» — слепому доверию алгоритмическим решениям. В правоприменительной практике органов по защите данных ЕС (например, в решениях итальянского регулятора Garante и нидерландского AP в 2024–2025 гг.) формальное наличие человека, лишь механически нажимавшего кнопку «Подтвердить», не было признано действительным человеческим контролем. Это повлекло за собой наложение крупных штрафов за нарушение статьи 22 Общего регламента по защите данных (GDPR) [7].

При этом внедрение полноценного МНС (включая интерфейсы ХАИ, специализированное обучение персонала и ведение детальных журналов) неизбежно увеличивает операционные расходы компаний. Чрезмерно жесткое регулирование без гибких механизмов может привести к отказу бизнеса от внедрения ИИ или к «регуляторному арбитражу» — переносу разработок и серверов в юрисдикции с более либеральными правилами [15].

Для перехода от формального присутствия человека к содержательному контролю предлагается реализовать следующий комплекс мер:

1. Закрепить легальное определение содержательного контроля и дополнить Федеральный закон № 243-ФЗ положением о том, что человеческий контроль признается надлежащим только при одновременном соблюдении условий:

- система прошла сертификацию на соответствие международным или национальным стандартам управления рисками ИИ (например, ISO/IEC 42001:2023 и ISO/IEC 23894:2023) [10; 11];
- интерфейс системы обеспечивает объяснимость принимаемых решений в формате, доступном для понимания конкретным оператором;
- оператор обладает необходимой професси-

ональной компетенцией и выделенным временем для анализа и вмешательства.

2. Внедрить градуированную модель надзора, дифференцируя требования в зависимости от уровня потенциального риска (в увязке с положениями Национальной стратегии развития ИИ [12]):

Таблица 2.

Разработать и внедрить профессиональные стандарты для операторов высокорисковых систем, включая обязательные регулярные тренировки на симуляторах – по аналогии с системой управления ресурсами экипажа (Crew Resource Management) в авиации [8].

Дифференцировать режим ответственности и дополнить ст. 11 Федерального закона № 243-ФЗ специальными положениями:

Уровень риска	Режим надзора	Требования
Экстремально высокий (медицина, правосудие)	НПТЛ (предварительное одобрение)	Система не может выполнить решение без явного одобрения человека
Средне-высокий (финансы, критическая инфраструктура)	НОТЛ (мониторинг + право вето)	Наблюдатель может отслеживать и отменять решение в реальном времени
Общий	Постфактумный аудит	Журналы работы системы доступны для проверки

- презумпция вины оператора, если система предоставила понятное объяснение своего решения, но оператор его проигнорировал;

- строгая (безвиновная) ответственность разработчика, если система функционировала как «чёрный ящик» и не предоставила оператору технических средств для выявления ошибки;

- императивное правило, согласно которому ссылка на «наличие человека в контуре» не освобождает от ответственности, если был обеспечен лишь формальный, фиктивный надзор.

Ввести обязательную трассируемость действий и вменить в обязанность операторам высокорисковых систем ведение защищенных от несанкционированной модификации журналов, фиксирующих входные данные, объяснение, сгенерированное ИИ, и конкретное действие оператора.

Восполнить правовой пробел в исключении для обучающих данных и включить в ст. 10 Федерального закона № 243-ФЗ право правообладателя на информацию: разработчик обязан уведомлять о факте включения произведения в обучающие массивы через организации коллективного управления правами или посредством публичного реестра.

Установить единый законодательный стандарт маркировки и дополнить ст. 9 Федерального

закона № 243-ФЗ императивными требованиями к формату и содержанию информационного предупреждения, исключив возможность передачи этих вопросов на усмотрение частного соглашения сторон.

Экономически стимулировать внедрение МНС. Для компенсации возросших операционных расходов целесообразно предусмотреть меры государственной поддержки (налоговые льготы, приоритет при осуществлении государственных закупок) для компаний, добровольно сертифицирующих свои системы на соответствие стандартам содержательного человеческого контроля.

Федеральный закон № 243-ФЗ заложил важную институциональную основу для российского регулирования сферы искусственного интеллекта. Разграничение суверенных и национальных моделей отражает обоснованное стремление государства к обеспечению технологического суверенитета. Однако с точки зрения правовых механизмов человеческого контроля данный закон пока остается рамочным актом, сфокусированным преимущественно на квалификации разработчика и вопросах технической безопасности. Переход к стандарту содержательного человеческого контроля требует фундаментальной смены правовой парадигмы: право должно оценивать не сам факт физического наличия человека в процессе, а его верифицируемую способность понять логику алгоритма и при необходимости отменить его решение. Реализация предложенных мер позволит устранить опасный «разрыв ответственности», обеспечить надежную защиту прав граждан и создать предсказуемые, прозрачные условия для добросовестных разработчиков технологий ИИ.

Список литературы:

- [1] Булавинова, М. П. «Значимый человеческий контроль» как основа для этического и правового регулирования применения автономных систем / М. П. Булавинова // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 8: Науковедение. Реферативный журнал. – 2020. – № 4. – С. 14-29.
- [2] Коряка, Д. А. Интеллектуальные права на объекты, созданные с использованием искусственного интеллекта: сравнительный анализ российского и зарубежных подходов к регистрации и охране / Д. А. Коряка, О. В. Олейников // Экономические и социальные проблемы регионального развития в современных условиях : Сборник научных трудов 2-й Международной научно-практической конференции. В 2-х томах, Курск, 06 февраля 2026 года. – Курск: ЗАО "Университетская книга", 2026. – С. 393-402.
- [3] Карецкий, А. О. Правовой статус результатов интеллектуальной деятельности, созданных искусственным интеллектом: проблемы и перспективы / А. О. Карецкий, О. В. Олейников // Экономические и социальные проблемы регионального развития в современных условиях : Сборник научных трудов 2-й Международной научно-практической конференции. В 2-х томах, Курск, 06 февраля 2026 года. Том 2. – Курск: ЗАО "Университетская книга", 2026. – С. 376-381.
- [4] Регламент ЕС 2024/1689 Закон об искусственном интеллекте // Официальный журнал Европейского союза. – 2024. – L 168/1.
- [5] Система управления рисками в области искусственного интеллекта (AI RMF 1.0). // Национальный институт стандартов и технологий (NIST) США. – 2023.
- [6] Временные меры по управлению службами искусственного интеллекта в Китае (CAC, MIIT, MPS, NRTA, 10 июля 2023 г.). // Центр глобальной IT кооперации. URL: <https://cgitc.ru/upload/iblock/a6e/3z053f61c763gcvx2bt2qiu6qbgvh87m.pdf?ysclid=muv2yz518725590961> (дата обращения: 18.07.2026).
- [7] Положение об использовании искусственного интеллекта в автоматизированных процессах подбора персонала. – Постановление Итальянского управления по защите данных (Garante). № 150 от 2024 года.
- [8] Руководство ИКАО по обучению, основанному на фактических данных (Дос 9995) и управлению ресурсами экипажа (Дос 9868) / Международная организация гражданской авиации (ИКАО). – 11-е изд., 2023.
- [9] Федеральный закон от 26.07.2026 № 243-ФЗ «О поддержке развития технологий искусственного интеллекта в Российской Федерации» // Официальный интернет-портал правовой информации <http://pravo.gov.ru>. – 2026. – 26 июля.
- [10] ISO/IEC 42001:2023. Информационные технологии – Искусственный интеллект — Система управления. – 2023. // Росстандарт. URL: <https://rst.gov.ru:8443/file-service/file/load/1742995304141?ysclid=mvksdmqgjx904157401> (дата обращения: 18.07.2026).
- [11] ISO/IEC 23894:2023. Информационные технологии – Искусственный интеллект — Руководство по управлению рисками. – 2023. // Росстандарт. URL: <https://rst.gov.ru:8443/file-service/file/load/1682519677927?ysclid=mvksdsev6o523234720> (дата обращения: 18.07.2026).
- [12] Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Офи-

циальный интернет-портал правовой информации <http://www.pravo.gov.ru>. – 2019. – 11 октября.

[13] Паршин, Д. С. Влияние искусственного интеллекта на кибербезопасность: новые возможности и угрозы / Д. С. Паршин, Т. Г. Маглинова // Юность и Знания - Гарантия Успеха - 2025 : Сборник научных статей 12-й Международной молодежной научной конференции. В 4-х томах, Курск, 25–26 сентября 2025 года. – Курск: ЗАО "Университетская книга", 2025. – С. 234–236.

[14] Мадатова, О. В. Правовые основы ключевых отраслей права: учебное пособие / О. В. Мадатова, С. Ю. Субачев, О. Я. Мадатов. – Краснодар: АНО НИИ ЭПИТ, 2025. – 235 с.

[15] Бондаренко, И. А. Искусственный интеллект и проблема финансовой устойчивости / И. А. Бондаренко, Р. О. Яковцева // Экономический рост как основа устойчивого развития России : Сборник статей IX-ой Всероссийской научно-практической конференции, Курск, 04–05 декабря 2025 года. – Курск: ЗАО "Университетская книга", 2025. – С. 72–76.

References:

[1] Bulavinova, M. P. "Meaningful Human Control" as a Basis for the Ethical and Legal Regulation of the Use of Autonomous Systems / M. P. Bulavinova // Social Sciences and Humanities. Domestic and Foreign Literature. Series 8: Science Studies. Abstract Journal. – 2020. – No. 4. – pp. 14–29.

[2] Koryaka, D. A. Intellectual Property Rights to Objects Created Using Artificial Intelligence: A Comparative Analysis of Russian and Foreign Approaches to Registration and Protection / D. A. Koryaka, O. V. Oleynikov // Economic and Social Problems of Regional Development in Contemporary Conditions: Proceedings of the 2nd International Scientific and Practical Conference. In 2 volumes, Kursk, February 6, 2026. – Kursk: ZAO "Universitetskaya Kniga", 2026. – pp. 393–402.

[3] Karetsky, A. O. Legal Status of the Results of Intellectual Activity Created by Artificial Intelligence: Problems and Prospects / A. O. Karetsky, O. V. Oleynikov // Economic and Social Problems of Regional Development in Contemporary Conditions: Proceedings of the 2nd International Scientific and Practical Conference. In 2 volumes, Kursk, February 6, 2026. Volume 2. – Kursk: ZAO "Universitetskaya Kniga", 2026. – pp. 376–381.

[4] EU Regulation 2024/1689: Artificial Intelligence Act // Official Journal of the European Union. – 2024. – L 168/1.

[5] Artificial Intelligence Risk Management Framework (AI RMF 1.0). // National Institute of Standards and Technology (NIST), USA. – 2023.

[6] Interim Measures for the Management of Artificial Intelligence Services in China (CAC, MIIT, MPS, NRTA, July 10, 2023). // Center for Global IT Cooperation. URL: <https://cgitc.ru/upload/iblock/a6e/3z053f61c763gcvx2bt2qiu6qbgvvh87m.pdf?ysclid=muv2yz518725590961> (accessed: July 18, 2026).

[7] Regulation on the Use of Artificial Intelligence in Automated Recruitment Processes. – Resolution of the Italian Data Protection Authority (Garante) No. 150 of 2024.

[8] ICAO Guidance on Evidence-Based Training (Doc 9995) and Crew Resource Management (Doc 9868) / International Civil Aviation Organization (ICAO). – 11th ed., 2023.

[9] Federal Law No. 243-FZ of July 26, 2026, "On Supporting the Development of Artificial Intelligence Technologies in the Russian Federation." // Official Internet Portal of Legal Information: <http://pravo.gov.ru>. – 2026. – July 26.

[10] ISO/IEC 42001:2023. Information Technology — Artificial Intelligence — Management System. – 2023. // Rosstandart. URL: <https://rst.gov.ru:8443/file-service/file/load/1742995304141?ysclid=mvksmqgjx904157401> (accessed: July 18, 2026).

[11] ISO/IEC 23894:2023. Information technology — Artificial intelligence — Guidance on risk management. – 2023. // Rosstandart. URL: <https://rst.gov.ru:8443/file-service/file/load/1682519677927?ysclid=mvksdsev6o523234720> (accessed: July 18, 2026).

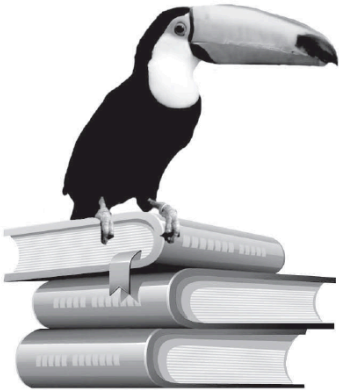
[12] Decree of the President of the Russian Federation No. 490 dated October 10, 2019 (as amended on February 15, 2024) "On the Development of Artificial Intelligence in the Russian Federation" (including the "National Strategy for the Development of Artificial Intelligence for the Period up to 2030") // Official Internet Portal of Legal Information <http://www.pravo.gov.ru>. – 2019. – October 11.

[13] Parshin, D. S. The Impact of Artificial Intelligence on Cybersecurity: New Opportunities and Threats / D. S. Parshin, T. G. Maglinova // Youth and Knowledge — A Guarantee of Success — 2025: Collection of Scientific Articles from the 12th International Youth Scientific Conference. In 4 volumes, Kursk, September 25–26, 2025. – Kursk: ZAO "Universitetskaya Kniga", 2025. – pp. 234–236.

[14] Madatova, O. V. Legal Foundations of Key Branches of Law: A Textbook / O. V. Madatova, S. Yu. Subachev, O. Ya. Madatov. – Krasnodar: АНО НИИ ЭПИТ, 2025. – 235 p.

[15] Bondarenko, I. A. Artificial Intelligence and the Problem of Financial Stability / I. A. Bondarenko, R. O. Yakovtseva // Economic Growth as a Basis for the Sustainable Development of Russia: Collection of Articles from the 9th All-Russian Scientific and Practical Conference, Kursk, December 4–5, 2025.

– Kursk: ZAO "Universitetskaya Kniga", 2025. – pp. 72–76.



ЮРКОМПАНИ

www.law-books.ru

Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.