

Научная статья

УДК 338.24; 004.8; 351.82

DOI: 10.47475/1994-2796-2026-512-6-221-232

КОНЦЕПЦИЯ САМОРЕГУЛИРУЕМОЙ ОРГАНИЗАЦИИ В СФЕРЕ ИИ КАК ФАКТОР РАЗВИТИЯ НАЦИОНАЛЬНОЙ ЭКОНОМИКИ

**Кирилл Михайлович Елин¹✉, Наталья Витальевна Усова²,
Михаил Павлович Логинов³**

¹ Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Уральский институт управления, Екатеринбург, Россия, kirill0420@rambler.ru, 0009-0007-4521-380X

² Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Уральский институт управления; Уральский государственный экономический университет; Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, Екатеринбург, Россия, nata-ekb-777@yandex.ru, 0000-0002-7575-6078

³ Уральский государственный экономический университет, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина; Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Уральский институт управления, Екатеринбург, Россия, port-all@mail.ru, 0000-0003-0831-3004

Аннотация. Повышение эффективности национальной экономики напрямую сопряжено с внедрением и активным использованием цифровых технологий, одной из которых является искусственный интеллект (далее — ИИ). Авторами представлены результаты исследования пробелов в регулировании решений, принимаемых системами ИИ, а также механизм минимизации рисков, сопутствующих применению технологий ИИ. Проведен анализ российских и зарубежных исследований в области регулирования ИИ, определены общие аспекты, выявлены пробелы в части отсутствия установленной ответственности за его действия. Представлена систематизация ключевых проблем и вызовов, связанных с внедрением ИИ. Основным результатом исследования является разработанная концепция деятельности саморегулируемой организации (далее — СРО) в сфере действия ИИ, определяющая ее цели, задачи, участников и предмет деятельности. На основе анализа данных об инцидентах и опыта СРО в финансовой сфере выявлены преимущества предлагаемого подхода, а по результатам сравнительного анализа обоснована важность внедрения института СРО в части способности существенно повысить эффективность и адресность регулирования ИИ в России. Авторами предложено создание пилотных отраслевых СРО с последующей возможностью их интеграции в систему трансграничного сотрудничества. В заключении делается вывод о необходимости и практической ценности внедрения механизмов саморегулирования как гибкого инструмента, дополняющего государственное регулирование и способствующего ответственному развитию ИИ-технологий.

Ключевые слова: саморегулируемая организация, искусственный интеллект, ответственность, регулирование, безопасность, цифровые технологии, управление

Для цитирования: Елин К. М., Усова Н. В., Логинов М. П. Концепция саморегулируемой организации в сфере ИИ как фактор развития национальной экономики // Вестник Челябинского государственного университета. 2026. № 6 (512). С. 221–232. DOI: 10.47475/1994-2796-2026-512-6-221-232.

Original article

THE CONCEPT OF A SELF-REGULATORY ORGANIZATION IN THE FIELD OF AI AS A FACTOR IN THE DEVELOPMENT OF THE NATIONAL ECONOMY**Kirill M. Yelin^{1✉}, Natalya V. Usova², Mikhail P. Loginov³**¹ Russian Presidential Academy of National Economy and Public Administration, the Ural Institute of Management, Yekaterinburg, Russia, kirill0420@rambler.ru, 0009-0007-4521-380X² Russian Presidential Academy of National Economy and Public Administration, the Ural Institute of Management; Ural State University of Economics; Ural Federal University, Yekaterinburg, Russia, nata-ekb-777@yandex.ru, 0000-0002-7575-6078³ Ural State University of Economics, Ural Federal University, Russian Presidential Academy of National Economy and Public Administration, the Ural Institute of Management, Yekaterinburg, Russia, port-all@mail.ru, 0000-0003-0831-3004

Abstract. Improving the efficiency of the national economy is directly related to the introduction and active use of digital technologies, one of which is artificial intelligence (hereinafter — AI). The authors present the results of a study of gaps in the regulation of decisions made by AI systems, as well as a mechanism for minimizing the risks associated with the use of AI technologies. An analysis of Russian and foreign research in the field of AI regulation has been carried out, general aspects have been identified, and gaps have been identified in terms of the lack of established responsibility for its actions. A systematization of the key problems and challenges associated with the introduction of AI is presented. The main result of the research is the developed concept of a self-regulatory organization (hereinafter — SRO) in the field of AI, defining its goals, objectives, participants and the subject of its activities. Based on the analysis of incident data and the experience of SRO in the financial sector, the advantages of the proposed approach have been identified, and based on the results of a comparative analysis, the importance of introducing the SRO institute in terms of its ability to significantly increase the effectiveness and targeting of AI regulation in Russia has been substantiated. The authors proposed the creation of pilot sectoral SROs with the subsequent possibility of their integration into the system of cross-border cooperation. In conclusion, it is concluded that it is necessary and practical to introduce self-regulation mechanisms as a flexible tool that complements government regulation and promotes responsible development of AI technologies.

Keywords: self-regulating organization, artificial intelligence, responsibility, regulation, security, digital technologies, management

For citation: Yelin KM, Usova NV, Loginov MP. The Concept of a Self-Regulatory Organization in the Field of AI as a Factor in the Development of the National Economy. *Bulletin of Chelyabinsk State University*. 2026;(6(512):221-232. (In Russ.). DOI: 10.47475/1994-2796-2026-512-6-221-232.

Введение

Экономика России и мир в целом переживают этап масштабной технологической трансформации, обусловленной развитием таких инноваций, как Big Data, технологии трехмерной печати, беспилотные аппараты, виртуальная и дополненная реальность, нейросети и ИИ.

Цифровые технологии и ИИ-решения существенным образом трансформируют сложившиеся экономические структуры и рыночные механизмы на всех уровнях социально-экономических систем. Для индивида они выступают инструментом повышения скорости и качества принятия решений за счет оперативного доступа к информации. На уровне предприятий ИИ, помимо аналогичного повышения эффективности управленческих решений, способствует улучшению качества продукции, взаимодействия с потребителями, оптимизации производственных затрат и повышению эффективности логистических процессов [1].

Кроме того, эффекты использования ИИ в предприятиях могут в долгосрочной перспективе способствовать автоматизации труда и снижению операционных расходов, созданию новых рабочих мест, повышению производительности экономик, изменениям в профессиональных структурах, повышению уровня инновационности предприятий [2].

По мере развития формирование технологий ИИ в образ полноценного экономического агента, взаимодействующего с человеком и активно участвующего в социально-экономических процессах, видоизменяет не только микро-, но и макроэкономические связи.

При этом регуляторное воздействие применения технологий ИИ сталкивается с тремя ключевыми вызовами, что влияет на конкурентоспособность и потенциал национальной экономики: — темпы нормотворческой работы отстают от скорости развития технологий;

— глобальный характер ИИ создает пробелы в национальном законодательстве при трансграничном использовании алгоритмов;

— регулятор зачастую не обладает необходимыми компетенциями для оценки рисков внедрения ИИ-решений.

Цель исследования — предложить и обосновать организационно-экономический механизм отношений между операторами ИИ и пользователями, направленный на обеспечение контроля применения технологий ИИ.

В качестве задач исследования следует:

1) охарактеризовать степень теоретической работанности исследуемой проблемы;

2) провести анализ действующих регуляторных механизмов, применяемых в сфере ИИ;

3) предложить организационно-экономический механизм, обеспечивающий контроль использования технологий ИИ операторами и защиту прав и свобод пользователей.

Последовательное решение поставленных задач позволит сформулировать направления повышения эффективности и обеспечения качественной составляющей как применения технологий ИИ, так и получения результата деятельности с использованием данных технологических решений.

Теоретический обзор

В условиях формирования цифровой модели национальной экономики всё большую востребованность приобретают инновационные цифровые технологии, наблюдается популяризация цифровых платформ и экосистем.

Согласно позиции М. Н. Конякина, обеспечение безопасности, социальной справедливости и устойчивой экономики напрямую зависит от выстраивания системы регулирования ИИ [3].

В свою очередь отмечается необходимость развития комплексного регулирования разработки и применения ИИ как особого нового явления, объединяющего в себе технические, этические и правовые аспекты [4].

Несмотря на возможные трудности, развитие регулирования ИИ в социально-экономических системах повлечет ряд положительных последствий. Эффективное регулирование способно повысить общественное доверие к технологиям и обеспечить правовую определенность для разработчиков, стимулируя инвестиции в инновации на уровне национальной экономики и ее отраслей.

Зарубежными авторами также отмечается, что акцентировать внимание при решении данной проблемы стоит на осознании высоких темпов

развития отрасли, учете сложностей технологий ИИ и верной классификации рисков, а также верном определении ответственных лиц [5].

Участие государства с точки зрения регулирования крайне важно для того, чтобы ИИ внедрялся ответственно, минимизируя негативные побочные эффекты и риски, одновременно максимизируя выгоды от технологических инноваций [6].

В процессе рассмотрения инновационных рисков Л. И. Кулакова выделяет специфические риски, связанные с применением ИИ, а именно риски «плохих данных», «недостатка прозрачности», «чрезмерной зависимости», «непреднамеренной предвзятости», «наивности и преественности», а также «неправильного выбора» [7].

В работе А. А. Сычева отмечается, что технологии ИИ фактически являются лишь инструментом, тогда как его действия и ответственность за их совершение справедливо относятся к группе лиц, состоящих из разработчиков, субъектов регулирования и контроля, пользователей и иных [8].

Как отмечает Н. В. Филина, ИИ должен быть интегрирован в правовое поле, тогда как ответственность за результаты действий технологии необходимо возлагать на связанных с ним физических и юридических лиц [9].

Таким образом, проведенный анализ работ российских и зарубежных ученых демонстрирует, что фундаментальной проблемой развития ИИ остается отсутствие четких правовых параметров ответственности за решения технологий, что порождает непрозрачность алгоритмов, уязвимость данных, дискриминацию и социальное неравенство. Всё это свидетельствует о необходимости законодательного закрепления справедливой ответственности прежде всего перед человеком.

Материалы и методы

Учитывая достаточную инновационность самих технологий ИИ, а также фрагментарность научных исследований, что подтверждается представленным обзором доступной авторам литературы, необходимо дополнить существующий инструментарий, используемый для регулирования применения технологий ИИ, в процессе производства, распределения, обмена и потребления.

Использование ИИ сопряжено с рядом проблем, ключевыми из которых являются следующие:

— наблюдается недостаточность норм права и стандартов регулирования действий ИИ, что приводит к неопределенности относительно того, кто несет ответственность за последствия

применения технологий ИИ, а также определения авторства на произведения, созданные ИИ;

– учитывая сложность моделей ИИ, становится затруднительным пояснить причины принятия того либо иного решения. Также к этическому аспекту относится как возможность воспроизведения предвзятых точек зрения, заложенных при обучении ИИ, так и усиление риска утечки персональных данных в связи с использованием их в больших объемах;

– ИИ становится объектом кибератак для обмана моделей и кражи персональных данных, что связано с ростом востребованности. Также возможна неверная интерпретация запросов пользователей, что приводит к нежелательным последствиям;

– рост социальной напряженности в обществе, что выражается в трансформации рынка труда и, соответственно, потере рабочих мест в связи с автоматизацией ряда процессов и сокращением некоторых профессий. Некорректное же применение технологий ИИ способно усугубить проблему социального неравенства и сформировать предпосылки новых социальных проблем либо сами проблемы;

– с учетом того, что небольшие компании и исследователи располагают достаточно низким уровнем доступности значительных вычислительных мощностей и большого объема качественных данных, мощные модели ИИ для них становятся недоступны и, как следствие, снижается эффективность работы комплекса ИИ-систем в целом, а также возрастает зависимость от вычислительных мощностей и качества используемых данных.

Технологии ИИ становятся одним из ключевых инструментов и трансформируют архитектуру технологических процессов экономических систем, что сопряжено не только с возможностями, которые открываются участникам экономических систем, но и с вызовами, связанными с использованием ИИ (рис. 1).

Так, ключевыми вызовами внедрения ИИ являются дискриминация алгоритмов, ведущая к несправедливым решениям по косвенным признакам, а также недостоверность данных, вызванная ошибками обучения или манипуляциями. Одним из важнейших вызовов являются потенциальные кибератаки с использованием фальсифицированных с помощью ИИ персональных данных [10]. Следующим вызовом выступают этические дилеммы, связанные с авторством контента и дезинформацией. Дополнением ко всему является



Рис. 1. Вызовы внедрения технологий ИИ в национальную экономику

Fig. 1. Challenges of introducing AI technologies into the national economy

Источник: разработано авторами.

риск монополизации технологий крупными корпорациями, что может существенно ограничить развитие рынка и доступ малого бизнеса к инновациям.

Результаты

Широкая область применения цифровых технологий и инструментов ИИ в актуальном векторе развития общества, а именно вопросах ответственности за результаты деятельности по использованию таких решений, фактически не закреплена нормативно.

Неконтролируемость процесса использования технологий ИИ приводит к нарушению прав и свобод граждан, созданию угроз преднамеренного и непреднамеренного характера, в том числе как со стороны разработчиков, создающих соответствующее ПО, так и разработчиков, обучающих ИИ.

Например, негативным аспектом является возможная потеря контроля над ИИ со стороны человека, а создание и/или распространение фейковых новостей может послужить причиной военных действий, запуска непопулярных политических процессов, а также иных неблагоприятных последствий. Так, в 2021 г. согласно информационной базе инцидентов, связанных с цифровыми системами данных и ИИ было зарегистрировано 126 инцидентов, 72 из которых связаны с вопросами надежности алгоритмов и технологий. Вместе с тем 29 случаев из данных 72 связаны с трагическими для пользователей последствиями [11].

На рис. 2 приведена статистика по количеству инцидентов, связанных с технологиями ИИ

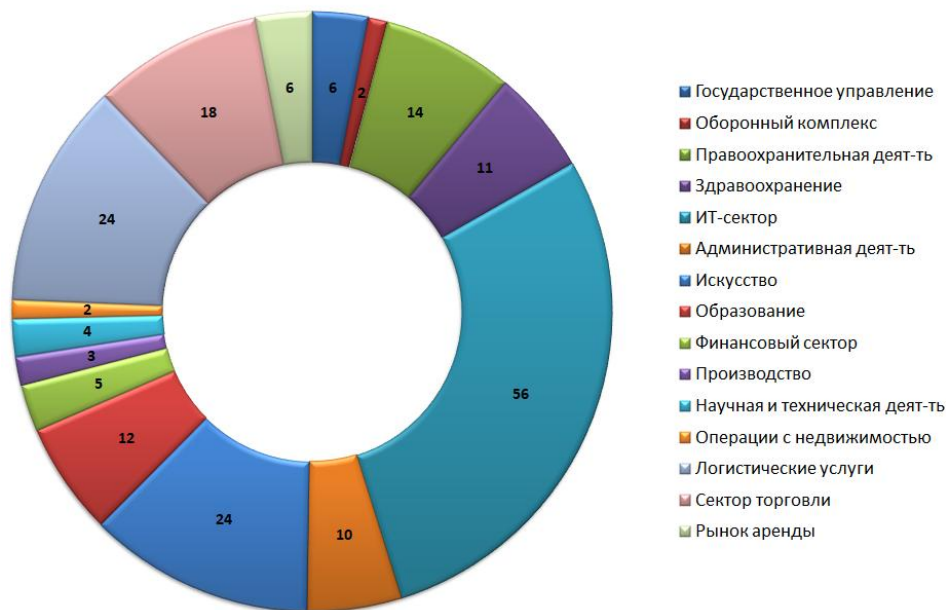


Рис. 2. Статистика инцидентов с ИИ по ключевым сферам деятельности мирового сообщества
Fig. 2. Statistics of AI incidents in key areas of activity of the global community

Источник: составлено авторами на основе Базы данных инцидентов ИИ¹.

¹ Artificial intelligence database. URL: <https://incidentdatabase.ai/summaries/spatial/> (дата обращения: 17.11.2025).

по ключевым сферам деятельности мирового сообщества.

Отметим, что на 01.09.2025 г. зафиксированы инциденты в работе интегрированных ИИ-систем. В представленной совокупности также присутствуют такие критически важные сферы, как оборонный комплекс, государственное (муниципальное) управление, здравоохранение и иные. Фактор наличия инцидентов в данных областях подтверждает важность вопроса определения ответственности и полномочий по регулированию результатов деятельности технологий, поскольку процессы, происходящие внутри данных систем и сфер общества напрямую влияют на его целостность и безопасность. Вместе с тем, помимо представленных на диаграмме данных, среди общего числа зафиксированных случаев на частное использование приходится 1 002 случая. Тем не менее данная практика хотя и не включена в определенные сферы общества, может повлечь за собой последствия, негативно влияющие и на них.

Таким образом, учитывая активный рост востребованности технологий, справедливо отметить, что членство в СРО для всех операторов ИИ (организаций, индивидуальных предпринимателей и самозанятых в сфере ИИ) является обязательным.

Исторические параллели: опыт СРО в финансовом секторе

Прежде чем более детально охарактеризовать авторское видение СРО в сфере ИИ, необходимо рассмотреть практику создания и функционирования СРО в финансовой сфере.

По состоянию на июль 2025 г. в финансовой сфере функционируют 16 СРО, среди которых «Всероссийский союз страховщиков», «Ассоциация форекс-дилеров», «Национальная ассоциация участников фондового рынка» и иные. Опыт их деятельности показал, что институт саморегулирования не только снижает нагрузку на государство, но и создает механизмы досудебного урегулирования споров, и, соответственно, повышается прозрачность конкретной сферы деятельности.

Учитывая, что система финансов является одним из ключевых компонентов национальной экономики, положительный опыт действия СРО в данной сфере имеет потенциал к развитию модели саморегулирования до уровня экономики страны с целью объединения всех участников экономических отношений, использующих ИИ-решения в операционной деятельности.

На рис. 3 представлена система действия СРО в сфере ИИ, включающая в себя основной состав участников данной СРО, механизмы взаимодействия с основными сторонами области деятельности, а также функционал.

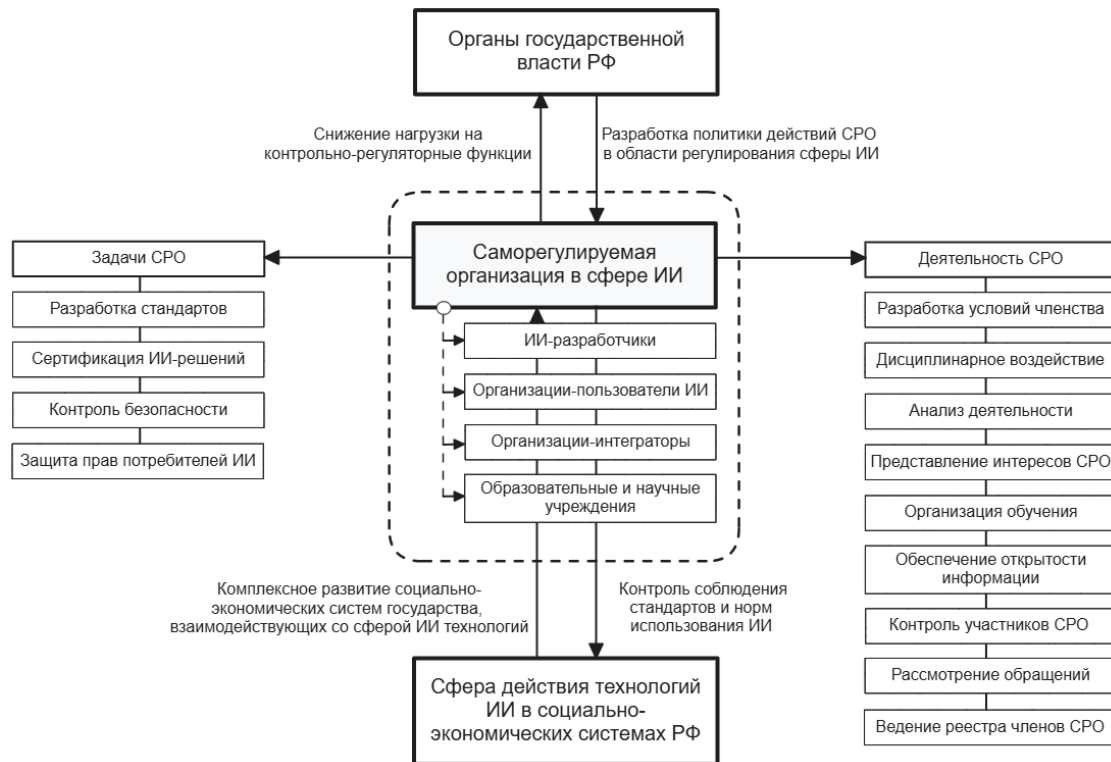


Рис. 3. Схема деятельности СРО в сфере ИИ

Fig. 3. The scheme of activity of a self-regulatory organization in the field of AI

Источник: разработано авторами

Таким образом, концептуально СРО в сфере ИИ включает в себя четыре группы участников с четким закреплением обязанностей каждой из них.

Первая группа представлена разработчиками ИИ-систем, которые в свою очередь обязаны соблюдать стандарты безопасности, контролировать данные для обучения и устранять выявленные пробелы в моделях. Вторую группу составляют предприниматели (организации, ИП, самозанятые), активно внедряющие ИИ в операционную деятельность. Данные представители станут основным источником статистических данных, а их высокая вовлеченность к 2030 г. окажет значительное экономическое влияние [12]. Вместе с тем использование ИИ предпринимателями с точки зрения ученых является важнейшим фактором для сохранения уровня экономической эффективности [13]. В третью группу входят компании-интеграторы, которые благодаря пониманию специфики решений могут контролировать этичность и безопасность внедрения ИИ у заказчиков. Четвертая группа представлена образовательными и научными организациями, осуществляющими подготовку квалифицированных кадров в соответствии с нормативами СРО и проведение исследований для совершенствования регламентов разработки и использования ИИ.

При взаимодействии с государством возможна господдержка в виде налоговых льгот для сертифицированных компаний, ИП и самозанятых; разработки совместных стандартов с целью гармонизации требований СРО и норм права; контроля за сферой ИИ путем наличия у государства права отзыва аккредитации СРО в случае выявления нарушений с ее стороны.

Для регулирования деятельности СРО в сфере ИИ предлагается по аналогии с Федеральным законом от 13.07.2015 № 223-ФЗ «О саморегулируемых организациях в сфере финансового рынка»¹, ввести Федеральный закон «О саморегулируемых организациях в сфере ИИ», коррелирующий с Федеральным законом от 01.12.2007 № 315-ФЗ «О саморегулируемых организациях»².

Правовую же основу деятельности СРО предлагается дополнить принципами, закрепленными в Указе Президента РФ № 490 «О развитии искусственного интеллекта в Российской Федера-

¹ О саморегулируемых организациях в сфере финансового рынка: Федеральный закон от 13.07.2015 г. № 223-ФЗ. URL: <https://base.garant.ru/71129194/> (дата обращения: 20.11.2025).

² О саморегулируемых организациях: Федеральный закон от 01.12.2007 № 315-ФЗ. URL: <https://base.garant.ru/12157433/> (дата обращения: 20.11.2025).

ции»¹, среди которых обеспечение защищенности и безопасности, разграничение ответственности пользователей и разработчиков, а также недопущение возложения ответственности за решения на ИИ-инструменты вместо физических или юридических лиц.

Среди непосредственных функций СРО также следует выделить следующие:

- разработка этических кодексов, правил и стандартов работы для всех участников (стандартов оказания услуг, этики использования ИИ, а также конфликта интересов);
- рассмотрение жалоб на членов организации и представление их в суде;
- обучение и повышение квалификации членов СРО;
- обеспечение имущественной ответственности участников за причинённый вред путем внесения страховых взносов;
- сертификация продуктов знаком «Безопасный ИИ».

Также необходимо обратить внимание на то, что все операторы ИИ должны быть членами данной СРО, а для физического лица должен действовать уведомительный порядок.

В свою очередь СРО страхует ответственность и в случае наступления страхового случая несет ответственность своим страховым фондом.

Потенциально страхование ответственности операторов ИИ должно осуществляться в следующем размере:

- для операторов ИИ с количеством зарегистрированных клиентов до 1 млн пользователей и объемом сделок в месяц до 500 млн руб. объем страховой суммы в год составляет 10 млн руб.;
- до 10 млн пользователей и объемом сделок до 1 млрд руб. страховая сумма составляет 20 млн руб. в год;
- более 10 млн пользователей и объемом сделок более 1 млрд руб. страховая сумма составляет в год 50 млн руб., любые сделки слияния и поглощения для таких операторов ИИ осуществляются только с согласия антимонопольной службы России.

Для повышения эффективности функционирования рынка ИИ целесообразно формирование двух реестров, где первый — реестр добросовестного использования ИИ, а второй — реестр недо-

бросовестного использования ИИ. Для повышения же качества ИИ-услуг возможно введение сертификации оказываемых услуг с использованием ИИ, а также обязательство хозяйствующих субъектов получать маркировку «Безопасный ИИ».

В целом деятельность СРО в сфере ИИ будет направлена на защиту ноу-хау, разработку правил и критериев этичного использования ИИ, страхование ответственности, регулирование деятельности операторов ИИ и ее лицензирование.

Так, на СРО операторов ИИ возлагается ряд регуляторных функций, среди которых допуск на рынок, контроль качества, ведение реестров, страхование, сбор отчетности и разрешение споров. Для этих целей должны быть созданы реестры рекомендуемых сервисов, а также инструменты формализации отчетности, защиты и стимулирования операторов ИИ.

Маркировка «Безопасный ИИ» как инструмент доверия

Для снижения рисков национальной экономики и защиты пользователей ИИ предлагается внедрение добровольной сертификации «Безопасный ИИ», что подтвердит надежность и справедливость алгоритмов. Для государства знак выступит инструментом снижения регуляторной нагрузки и прозрачного контроля, для бизнеса — конкурентным преимуществом, а граждан — гарантией безопасности и защиты от дискриминации.

Критериями же присвоения знака выступают: прозрачность алгоритмов (объяснимость решений), защита данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»², устойчивость к взломам и отсутствие дискриминации (регулярный аудит предвзятости, анализ данных и мониторинг в демографических группах).

На основании вышеизложенного процедура прохождения ИИ-системой сертификации и присвоения статуса «Безопасный ИИ» должна представлять собой алгоритм действий, представленный на рис. 4.

Также Уставом СРО необходимо закрепить положение о порядке реагирования на информацию об инцидентах и ошибках алгоритмов, поступающую от пользователей ИИ-систем. Так, по аналогии с положениями ст. 10 Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской

¹ О развитии искусственного интеллекта в Российской Федерации: Указ Президента Российской Федерации от 10.10.2019 № 490. URL: <https://www.garant.ru/products/ipo/prime/doc/72738946/> (дата обращения: 20.11.2025).

² О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ. URL: <https://base.garant.ru/12148567/> (дата обращения: 23.11.2025).

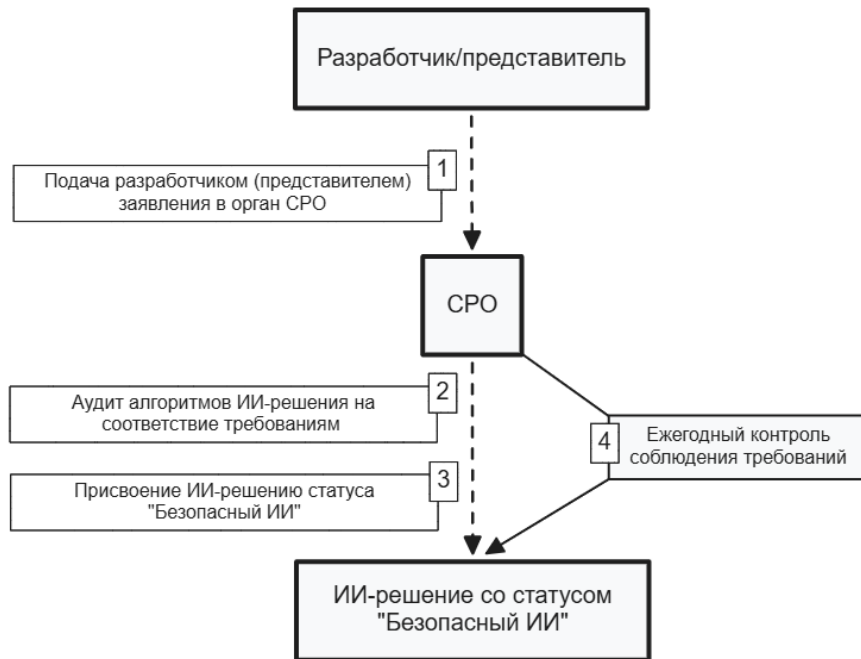


Рис. 4. Процедура сертификации ИИ-решения
 Fig. 4. The procedure for certification of an AI solution

Источник: разработано авторами

Федерации»¹ представителями СРО могут быть проведены внеплановые контрольные мероприятия в отношении предмета обращения. По результатам проверки в случае выявления нарушений определенной ИИ-системой установленных регламентов организации-представителю направляется уведомление об отзыве статуса «Безопасный ИИ» и исключении из реестра добросовестного использования ИИ. В данном случае ИИ-решение подлежит включению в реестр недобросовестного использования ИИ с приложением информации и документов о соответствующих решениях, принятых СРО по результатам контрольных действий.

Характер и сам факт создания и развития такого субъекта, как СРО в сфере ИИ, должны повлечь существенные положительные изменения в данной технологической области. В табл. 1 представлено сравнение фактического и перспективного положения в сфере регулирования ИИ в России.

Проведенное сравнение наглядно демонстрирует, что создание СРО в сфере ИИ является не просто альтернативным инструментом, а качественно новым, прогрессивным решением в разработке и моделировании эффективной системы регулирования.

¹ О порядке рассмотрения обращений граждан Российской Федерации: Федеральный закон от 02.05.2006 № 59-ФЗ. URL: <https://base.garant.ru/12146661/> (дата обращения: 23.11.2025).

Так, потенциал СРО заключается в формировании целостной системы стандартов, направленной на минимизацию актуальных рисков, а также в обеспечении экспертного контроля взамен исключительно государственного надзора. Привлечение же специалистов с профильными компетенциями позволиткратно повысить качество проверок и обоснованность постпроверочных решений.

Обсуждение

Внедрение института СРО в сфере ИИ, а также введение маркировки «Безопасный ИИ» позволят обеспечить гибкость и адаптивность регулирования и тем самым свободу инновационного развития, снизить риски для участников рынка и защитить общественные интересы, создать устойчивую экосистему доверия и поддерживать конкурентную среду на рынке, а также повысить инвестиционный потенциал экономики страны.

Реализация данной модели потребует активного участия не только государства в части формирования регуляторного базиса формирования и функционирования института СРО в сфере ИИ, но и предпринимательского сообщества. Как было отмечено ранее, достаточно много сфер деятельности уже используют технологии ИИ и важно в первую очередь разработать четкие механизмы функционирования СРО, а затем постепенно расширять сферы охвата СРО.

Сравнение фактического и перспективного положения в сфере регулирования ИИ в России
Comparison of the actual and prospective situation in the field of AI regulation in Russia

№	Критерий сравнения	Текущая ситуация (факт)	Ожидаемый результат
1	Гибкость нормативно-го регулирования	Недостаточная проработка нормативной базы в части контроля, регулирования и ответственности за результаты решений, принимаемых ИИ	Разработка и внедрение гибких отраслевых стандартов, оперативно актуализируемых для покрытия существующих пробелов
2	Механизм контроля	Контроль в узком формате со стороны ряда государственных структур без конкретного разделения полномочий	Всесторонний контроль ключевых субъектов сферы ИИ, их продуктов и действий в соответствии с регламентами
3	Качество ИИ-решений	Большая часть доступных и открытых ИИ-продуктов предоставляет некачественные решения на основе непроверенной информации	Обязательная сертификация с последующим регулярным предоставлением отчетов с целью подтверждения качества ИИ-продукта
4	Безопасность информации и защита данных	Отсутствие единых обязательных стандартов кибербезопасности для ИИ-систем. Фрагментированный подход	Обязательные для всех участников СРО единые стандарты кибербезопасности. Система аудита и сертификации
5	Разрешение спорных ситуаций	Спорные ситуации решаются в судебном порядке. Процессы длительные и не всегда справедливые	Оперативное реагирование на обращения; разрешение споров посредством участия в процессе экспертов-членов СРО
6	Этический аспект	Отсутствие единых и обязательных правил, требований, стандартов	Алгоритмы проверены на предмет нарушения норм этики, отсутствия дискриминации

Источник: разработано авторами.

Авторами предлагается в перспективе создать пилотные СРО в сфере ИИ с возможностью тиражирования положительного опыта в дальнейшем; внедрить предлагаемую маркировку «Безопасный ИИ» как добровольный стандарт; разработать механизм взаимодействия с государственными органами.

В свою очередь создание эффективной системы саморегулирования в сфере ИИ сопряжено с рядом сложностей, таких как разнородность участников и их интересов, стремительная смена технологических парадигм, глобальный характер ИИ-решений, а также необходимость баланса между инновационной свободой и государственным регулированием. Предложенный формат специализированной СРО потенциально способен обеспечить контроль за развитием технологий ИИ и выступить качественным организационно-экономическим механизмом взаимодействия всех участников сектора. При этом оценка эффективности данного решения возможна путем сравнения результатов пилотного проекта СРО с действующими в настоящее время инструментами регулирования и конт-

роля за разработкой и внедрением ИИ-технологий.

Данный формат, объединяющий всех участников процесса наряду с активными пользователями конечных ИИ-решений, также позволит существенно сократить статистику регистрируемых инцидентов в данной области, тем самым ограждая социально-экономическую систему страны от низкокачественных и вредоносных систем, обеспечивая безопасное пользование и последующее устойчивое развитие отрасли.

Заключение

Так, настоящее исследование подтверждает, что центральной проблемой в сфере правового регулирования ИИ является не столько отсутствие нормативных актов, сколько дефицит конкретных механизмов, распределяющих ответственность за решения, сгенерированные автономными системами. Существующие правовые конструкции, ориентированные на действие или бездействие ответственного субъекта в лице человека, демонстрируют свою ограниченность при причинении вреда или принятии значимого решения

инициировано алгоритмом, чья структура действий может являться недостаточно прозрачной, в том числе для его разработчиков. Проведенный анализ ключевых рисков — от алгоритмической дискриминации и унаследованных социальных предубеждений до стратегических киберугроз и зависимости от технологических монополий — указывает на системный характер вызовов. Данные вызовы не могут быть эффективно нивелированы исключительно императивными нормами государственного права, которые по своей природе недостаточно адаптивны и зачастую излишне формальны для технологической среды, характеризующейся динамичным развитием.

Разработанная в рамках статьи схема деятельности СРО в сфере ИИ предлагает определенный институт. В свою очередь, такая организация может взять на себя функции по созданию сертификационных процедур, аккумулярованию луч-

ших практик, досудебному разрешению споров и формированию компенсационных фондов, что создаст реальные стимулы для ответственного поведения компаний.

Следовательно, исследованием определена необходимость регулирования комплексной деятельности, связанной со сферой ИИ, посредством гибких форм. Создание пилотных СРО в приоритетных секторах станет следующим логическим шагом. Успешный опыт организаций данного формата впоследствии может составить основу как национального законодательства, так и стать ядром для построения трансграничных систем доверия и кооперации в области контроля над ИИ. Таким образом, предложенная модель представляет собой практико-ориентированный путь к управлению рисками ИИ, сочетающий адаптивность отрасли и достижение ключевых общественных целей.

Список источников

1. Wan Y., Tao H., Zhao Y., Huang L. The Economic Impact of Artificial Intelligence as a General Purpose Technology and Its Innovations in Economic Research // *International Journal of Computer Science and Information Technology*. 2025. № 1 (5). P. 26–28. DOI: 10.62051/ijcsit.v5n1.03.
2. Kasperska E. M., Stefanczyk J., Dabrowski P. J., Zaloga W. The Consequences of Implementing Artificial Intelligence Technology in the Digital Economy from the Perspective of Generation Z // *European Research Studies Journal*. 2024. № 3. P. 1039–1057. DOI: 10.35808/ersj/3764.
3. Конякин М. Н. О формировании системы правового регулирования искусственного интеллекта // *Бизнес. Образование. Право*. 2024. № 3 (68). С. 267–272. DOI: 10.25683/VOLBI.2024.68.1086.
4. Кондрашов П. Е., Петрунин Ю. Ю., Попова С. С. Регулирование разработки и применения искусственного интеллекта: проблемы и направления развития // *Вестник Московского университета. Серия 21: Управление (государство и общество)*. 2025. № 1. С. 3–19. DOI: 10.55959/MSU2073-2643-22-2025-1-3-19. EDN: YNLBUI.
5. Alfiani F. R. N., Santiago F. The important role of artificial intelligence regulation in protecting public interest // *Journal of Social Science*. 2024. № 7 (3). P. 432–439. DOI: 10.57185/joss.v3i7.339.
6. Goswami R., Singh S., Tomar A. The role of government in regulating AI for economic benefit // *ShodhKosh: Journal of Visual and Performing Arts*. 2024. № 5(1). P. 2025–2038. DOI: 10.29121/shodhkosh.v5.i1.2024.1659
7. Кулакова Л. И. Инновационные риски применения искусственного интеллекта в предпринимательских структурах // *Вестник Академии знаний*. 2022. № 50 (3). С. 180–185.
8. Сычев А. А. В поисках надежности: трансформация доверия в эпоху цифровых технологий // *Мониторинг общественного мнения: экономические и социальные перемены*. 2024. № 5. С. 37–59. DOI: 10.14515/monitoring.2024.5.2595.
9. Филина Н. В., Гудков Ю. А., Сенин И. Н. Юридическая ответственность искусственного интеллекта: теоретические модели и практические решения // *Журнал прикладных исследований*. 2025. № 7. С. 193–198. DOI: 10.47576/2949-1878.2025.7.7.025.
10. Мосечкин И. Н. Дипфейк-технологии и биометрические данные: направления уголовно-правового регулирования // *Вестник Санкт-Петербургского университета. Право*. 2025. № 1(16). С. 95–110. DOI: 10.21638/spbu14.2025.107.
11. Yili H., Jiayi L., Li X., Jie M., Yueyao W., Laura J. F., Xinwei D. Statistical perspectives on reliability of artificial intelligence systems // *Quality Engineering*. 2023. № 1 (35). P. 56–78. DOI: 10.48550/arXiv.2111.05391.
12. Fossen F., McLemore T., Sorgner A. Artificial Intelligence and Entrepreneurship // *Foundations and Trends in Entrepreneurship*. 2024. № 20 (8). P. 781–904. DOI: 10.1561/03000000130.

13. Bassey R. G., Brownson G. D., Efi A. Artificial Intelligence (AI) power and entrepreneurial success // *British Journal of Management and Marketing Studies*. 2025. № 8 (1). P. 49–66. DOI: 10.52589/BJMMS CFWU44NZ.

References

1. Wan Y, Tao H, Zhao Y, Huang L. The Economic Impact of Artificial Intelligence as a General Purpose Technology and Its Innovations in Economic Research. *International Journal of Computer Science and Information Technology*. 2025;1(5):26-28. DOI: 10.62051/ijcsit.v5n1.03
2. Kacperska EM, Stefanczyk J, Dabrowski PJ, Zaloga W. The Consequences of Implementing Artificial Intelligence Technology in the Digital Economy from the Perspective of Generation Z. *European Research Studies Journal*. 2024;(3):1039-1057. DOI: 10.35808/ersj/3764.
3. Konyakin MN. On the formation of a system of legal regulation of artificial intelligence. *Biznes. Obrazovanie. Pravo = Business. Education. Law*. 2024;(3(68):267-272. DOI: 10.25683/VOLBI.2024.68.1086. (In Russ.).
4. Kondrashov PE, Petrushin YY, Popova SS. Regulation of the development and application of artificial intelligence: problems and directions of development. *Vestnik Moskovskogo universiteta. Seriya 21: Upravlenie (gosudarstvo i obshchestvo) = Bulletin of the Moscow University. Episode 21: Governance (State and Society)*. 2025;(1):3-19. DOI: 10.55959/MSU2073-2643-22-2025-1-3-19. (In Russ.).
5. Alfiani FRN, Santiago F. The important role of artificial intelligence regulation in protecting public interest. *Journal of Social Science*. 2024;(7(3):432-439. DOI: 10.57185/joss.v3i7.339.
6. Goswami R, Singh S, Tomar A. The Role of Government in Regulating AI for Economic Benefit. *Shodh-Kosh: Journal of Visual and Performing Arts*. 2024;5(1):2025-2038. DOI: 10.29121/shodhkosh.v5.i1.2024.1659.
7. Kulakova LI. Innovative risks of using artificial intelligence in business structures. *Vestnik Akademii znaniy = Bulletin of the Academy of Knowledge*. 2022;(50(3):180-185. (In Russ.).
8. Sychev AA. In search of reliability: the transformation of trust in the era of digital technologies. *Monitoring obshchestvennogo mneniya: ekonomicheskie i sotsial'nye peremeny = Public opinion monitoring: economic and social changes*. 2024;(5):37-59. DOI: 10.14515/monitoring.2024.5.2595. (In Russ.).
9. Filina NV, Gudkov YA, Senin IN. Legal responsibility of artificial intelligence: theoretical models and practical solutions. *Zhurnal prikladnykh issledovaniy = Journal of applied research*. 2025;(7):193-198. DOI: 10.47576/2949-1878.2025.7.7.025. (In Russ.).
10. Mosechkin IN. Deepfake technologies and biometric data: areas of criminal law regulation. *Vestnik Sankt-Peterburgskogo universiteta. Pravo = Bulletin of St. Petersburg University. Law*. 2025;(1(16):95-110. DOI: 10.21638/spbu14.2025.107. (In Russ.).
11. Yili H, Jiayi L, Li X, Jie M, Yueyao W, Laura JF, Xinwei D. Statistical perspectives on reliability of artificial intelligence systems. *Quality Engineering*. 2023;(1(35):56-78. DOI: 10.48550/arXiv.2111.05391.
12. Fossen F, McLemore T, Sorgner A. Artificial Intelligence and Entrepreneurship. *Foundations and Trends in Entrepreneurship*. 2024;(20(8):781-904. DOI:10.1561/03000000130.
13. Bassey RG, Brownson GD, Efi A. Artificial Intelligence (AI) Power and Entrepreneurial Success. *British Journal of Management and Marketing Studies*. 2025;(8(1):49-66. DOI:10.52589/BJMMS CFWU44NZ.

Информация об авторах

К. М. Елин — аспирант Центра социально-экономических исследований.

Н. В. Усова — доктор экономических наук, доцент, профессор кафедры экономической теории; профессор кафедры маркетинга и международного менеджмента; профессор кафедры международного менеджмента и маркетинга.

М. П. Логинов — доктор экономических наук, доцент, профессор кафедры финансов, денежного обращения и кредита; профессор кафедры менеджмента; профессор кафедры экономической теории.

Information about the authors

K. M. Yelin — Postgraduate Student at the Center for Socio-Economic Research.

N. V. Usova — Doctor of Economics, Associate Professor, Professor of the Department of Economic Theory; Professor of the Department of Marketing and International Management; Professor of the Department of International Management and Marketing.

M. P. Loginov — Doctor of Economics, Associate Professor, Professor of the Department of Finance, Money Circulation and Credit; Professor of the Department of Management; Professor of the Department of Economic Theory.

Статья поступила в редакцию 24.12.2025; одобрена после рецензирования 23.03.2026; принята к публикации 15.06.2026.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.

Авторы заявляют об отсутствии конфликта интересов.

The article was submitted 24.12.2025; approved after reviewing 23.03.2026; accepted for publication 15.06.2026.

Contribution of the authors: the authors contributed equally to this article.

The authors declare no conflicts of interests.