**ИНСТИТУТ НАУЧНОЙ ИНФОРМАЦИИ ПО ОБЩЕСТВЕННЫМ НАУКАМ
РОССИЙСКОЙ АКАДЕМИИ НАУК
(ИНИОН РАН)**

**СОЦИАЛЬНЫЕ
И
ГУМАНИТАРНЫЕ НАУКИ**

ОТЕЧЕСТВЕННАЯ И ЗАРУБЕЖНАЯ
ЛИТЕРАТУРА

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЖУРНАЛ

СЕРИЯ 4

ГОСУДАРСТВО
И
ПРАВО

2025 – 3

Издается с 1974 года
Выходит 4 раза в год
Индекс серии 2.4

Учредитель
Институт научной информации по общественным наукам
Российской академии наук

Включен в перечень журналов ВАК и Российский индекс научного цитирования (РИНЦ)

DOI: 10.31249/iajpravo/2025.03.00

ISSN 2219-861X

Регистрационное свидетельство ПИ № ФС 77-80872 от 21.04.2021

СОДЕРЖАНИЕ

ТЕМА НОМЕРА
ПРАВОВОЕ РЕГУЛИРОВАНИЕ БЕЗОПАСНОГО И НАДЕЖНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

НОВЫЕ КНИГИ НА ПОЛКАХ ФУНДАМЕНТАЛЬНОЙ БИБЛИОТЕКИ ИНИОН РАН

CONTENTS

ISSUE THEME
LEGAL REGULATION OF SAFE AND RELIABLE ARTIFICIAL INTELLIGENCE

NEW BOOKS ON THE SHELVES OF THE FUNDAMENTAL LIBRARY INION RAN

ТЕМА НОМЕРА
ПРАВОВОЕ РЕГУЛИРОВАНИЕ БЕЗОПАСНОГО И НАДЕЖНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

УДК 34.096 DOI: 10.31249/iajpravo/2025.03.01

КОДАНЕВА С.И.[1] ТРАНСФОРМИРУЮЩЕЕ ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ГОСУДАРСТВО И ОБЩЕСТВО: ПРАВОВЫЕ ВЫЗОВЫ И ПУТИ ИХ ПРЕОДОЛЕНИЯ (Статья)

Аннотация. В статье анализируются новые правоотношения, возникающие в связи с массовым распространением генеративного искусственного интеллекта. Показано, что алгоритмы оказывают преобразующие воздействие на все сферы жизни общества и приводят к появлению новых бизнес-процессов, способов взаимодействия государства с гражданами и моделей социального управления. Однако рождаются новые технологические и социальные риски. Предложены подходы к формированию правового регулирования использования искусственного интеллекта.

Ключевые слова: цифровое право; верховенство права; экспериментальные правовые режимы; генеративный искусственный интеллект; цифровое государство; глубокие подделки.

KODANEVA S.I. The Transformative Impact of Artificial Intelligence on the State and Society: Legal Challenges and Ways to Overcome Them (Article)

Abstract. The article analyzes new legal relations arising in connection with the massive spread of generative artificial intelligence. It is shown that algorithms have a transformative effect on all spheres of

[1] *Коданева Светлана Игоревна*, ведущий научный сотрудник отдела правоведения ИНИОН РАН, кандидат юридических наук, доцент.

society and lead to the emergence of new business processes, ways of government interaction with citizens and models of social management. However, new technological and social risks are also emerging. Approaches to the formation of legal regulation of the use of artificial intelligence are proposed.

Keywords: digital law; rule of law; experimental legal regimes; generative artificial intelligence; digital state; deep forgeries.

Для цитирования: Коданева С.И. Трансформирующее влияние искусственного интеллекта на государство и общество: правовые вызовы и пути их преодоления (Статья) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2025. – № 3. – С. 7–22. – DOI: 10.31249/iajpravo/2025.03.01

Введение

В современном обществе искусственный интеллект (далее – ИИ) воспринимается как прорывная технология, преобразующая практически все сферы жизни. Однако, прежде чем превратиться из теоретической концепции в один из самых используемых инструментов цифровой экономики, ИИ прошел довольно долгий путь. Появление концепции ИИ принято связывать с Дартмутской конференцией 1956 г., когда А. Тьюринг, Д. Маккарти и М. Мински сформулировали идею о машинном обучении. Однако для ее реализации требовались большие вычислительные мощности и технологии, которыми человечество еще не обладало. В результате в 1970-е и 1980-е годы наступили «зимы искусственного интеллекта» – периоды сокращения интереса к ИИ и, соответственно, финансирования. Технологические прорывы 1990-х и 2000-х годов оживили концепцию ИИ благодаря усовершенствованным алгоритмам, увеличению мощности вычислительных машин и распространению больших объемов данных. Методы машинного обучения, в частности нейронные сети, получили широкое распространение, позволив системам ИИ распознавать закономерности и совершенствоваться на основе опыта. В этот период (примерно с 1990 по 2010 г.) было создано несколько полезных приложений ИИ, которые принято называть «слабым ИИ», основанном на принципе «белого ящика», когда алгоритм сформирован программистом и может решать только «узкие», «конкретные» задачи. В 2010-х годах началась эра «глубокого обучения», в основе которой лежало использование нейросетей, работающих по принципу «черного ящика». Однако ИИ по-прежнему остается «слабым», поскольку он

не может выполнять общие рассуждения, но предназначен для решения конкретных задач. Еще одной неразрешимой задачей оставалось распознавание человеческой речи, или «обработка естественного языка». Ожидалось, что эта способность у ИИ появится только к 2030-м годам. Однако, неожиданно для всех, в 2022 г. OpenAI выпустила ChatGPT, основанный на генеративном ИИ (GenAI), который стал по-настоящему революционным достижением, поскольку оно сделало ИИ способным создавать оригинальный контент – от текста и изображений до музыки и программного кода – путем изучения шаблонов из обширных наборов данных. В отличие от традиционного ИИ, который фокусируется на анализе и прогнозировании, генеративный ИИ производит новые, согласованные результаты, имитирующие творческие способности человека[1].

Возникновение крупных языковых моделей (LLM), таких как ChatGPT, генераторов изображений или DALL·E и MidJourney и инструментов для генерации кода, например GitHub Copilot, преобразило различные отрасли – от маркетинга до здравоохранения. Так, ChatGPT пишет статьи, сценарии и маркетинговые материалы, MidJourney создает логотипы и рекламные объявления, музыкальный автомат OpenAI – оригинальные музыкальные партитуры. The Economist использует GenAI для составления финансовых отчетов, Insilico – разрабатывает молекулярные структуры, Khanmigo от Khan Academy – индивидуальные планы уроков, Zalando позволяет осуществлять виртуальную примерку одежды и т.д.

Таким образом, появление GenAI вплотную приблизило человечество к созданию «общего», или «сильного» ИИ, который сможет логично рассуждать и одновременно решать множество разноплановых задач, т.е. вести себя подобно человеку. Это предоставит новые возможности для развития всех сфер экономики и государственного управления, но также и породит новые риски и вызовы, требующие выработки принципиально новых подходов к правовому регулированию.

Трансформация общества под влиянием искусственного интеллекта

Как было показано выше, ИИ преобразует отрасли креативных индустрий, которые традиционно считались наиболее тесно

[1] Surden H. Artificial Intelligence and Law – an Overview of Recent Technological Changes // University of Colorado Law Review. – 2025. – Vol. 96. – P. 375–411.

связанными с человеческим творчеством. С одной стороны, это подрывает позиции профессиональных участников соответствующих рынков – дизайнеров, композиторов, музыкантов, сценаристов и т.д. С другой стороны, предоставляет новые возможности для тех, кто традиционно считался «потребителями» контента – простых пользователей, которые теперь могут воплощать свои творческие идеи в реальные «произведения» и делиться ими при помощи социальных сетей. Сформировался и активно развивается новый тип экономики – «экономика создателей» (creator economy), в которой «цифровые креаторы» и инфлюенсеры зарабатывают на создаваемом ими цифровом контенте.

Однако под влиянием ИИ постепенно трансформируются и более консервативные отрасли – добывающая и перерабатывающая промышленность, строительство, медицина и другие[1]. Автоматизация, основанная на ИИ, революционизирует их, повышая эффективность, снижая затраты и сводя к минимуму человеческие ошибки. Производство, логистика и обслуживание клиентов претерпели значительные изменения благодаря робототехнике, автономным транспортным средствам и чат-ботам на базе ИИ. Такие компании, как Tesla, Amazon и Foxconn, применяют ИИ для управления производственными линиями, складами и для контроля качества, что приводит к более быстрым и точным операциям. Промышленные предприятия, традиционно использующие ручной труд и жесткие технологические процессы, претерпевают глубокие преобразования по мере того, как технологии, основанные на ИИ, меняют производство, цепочки поставок, техническое обслуживание и взаимодействие с клиентами. Предприятия внедряют машинное обучение, компьютерное зрение, обработку естественного языка и робототехнику для повышения эффективности, снижения затрат и повышения конкурентоспособности. Так, «умные фабрики» используют ИИ: для оптимизации производственных линий (ИИ анализирует данные, поступающие от датчиков, в режиме реального времени, чтобы скорректировать настройки оборудования, сокращая время простоя и повышая производительность); технического обслуживания (вместо планового технического обслуживания ИИ прогнозирует отказы оборудования); улучшения контроля качества (системы компьютерного зрения обнаруживают дефекты в продукции с большей точностью, чем люди-контро-

[1] Подробнее см.: Kumar S., Verma A.K., Mirza A. Digital Transformation, Artificial Intelligence and Society. Opportunities and Challenges. – 2024. – 218 p.

леры). Такие компании, как Siemens и General Electric, запускают цифровые двойники, управляемые ИИ, для моделирования и оптимизации производственных процессов перед внедрением. Роботы широко используются на сборочных линиях: манипуляторы, управляемые ИИ, собирают электронику и автомобильные детали с минимальными ошибками, беспилотные транспортные средства перевозят материалы на складах или работают в добывающих карьерах, где людям находиться опасно (например в золотодобывающей компании «Полюс»). ИИ повышает эффективность цепочки поставок за счет прогнозирования спроса и автоматизации управления запасами (например в Walmart и Amazon). Интеллектуальные сети помогают энергетическим компаниям балансировать спрос и предложение, а, следовательно, и нагрузку на сети, сокращать потери энергии (например Россети). Добывающие компании внедряют «цифровые месторождения» для управления добычей в районах крайнего севера и на шельфе (например, Лукойл, Роснефть).

В ряде областей принципиально меняются сами бизнес-модели, когда на смену традиционным трудовым отношениям приходит фриланс (например в работе такси, доставке, программировании, маркетинге, создании дизайна и мультимедиа и т.д.)[1].

В финансовом секторе ИИ анализирует обширные массивы данных, чтобы выявлять тенденции и рекомендовать стратегии, оптимизирует инвестиции, обнаруживает мошенничество и улучшает оценку рисков.

Искусственный интеллект улучшает медицинскую диагностику с помощью таких инструментов, как IBM Watson Health и Google DeepMind, которые анализируют медицинские изображения, прогнозируют прогрессирование заболевания и рекомендуют методы лечения. Носимые устройства на базе искусственного интеллекта (например Apple Watch, Fitbit) отслеживают жизненно важные показатели, позволяя на ранней стадии выявлять такие заболевания, как фибрилляция предсердий или диабет. Помимо этого, ИИ ускоряет разработку лекарств, моделируя молекулярные взаимодействия, сокращая время и затраты на вывод новых лекарств на рынок. Например, Moderna использовала алгоритмы для разработки вакцин против COVID-19. Кроме того, ИИ адаптирует

[1] Подробнее см.: Artificial Intelligence in Application. Legal Aspects, Application Potentials and Use Scenarios / eds. T. Barton, Ch. Müller. – 2024. – 197 p.

методы лечения к индивидуальным генетическим профилям, что способствует развитию точной медицины.

В образовании платформы на базе ИИ, такие как Khan Academy и Duolingo, настраивают уроки в зависимости от успеваемости учащихся, повышая их вовлеченность. Чат-боты используются в репетиторстве, а аналитика, основанная на искусственном интеллекте, помогает преподавателям выявлять учащихся, испытывающих трудности.

Не менее серьезному влиянию подвержена и сфера государственного управления, начиная от внедрения концепции «умного города» и заканчивая такими сферами, как правосудие или принятие административных решений. Так, система компьютерного зрения позволяет быстро обнаруживать и задерживать преступников, управлять «умными перекрестками», уличным освещением, регулировать энергопотребление в режиме реального времени, выявлять чрезвычайные ситуации и оперативно на них реагировать[1]. Японская система раннего предупреждения о землетрясениях, основанная на ИИ, выдает предупреждения за секунды до начала подземных толчков. Во многих регионах РФ реализованы проекты «безопасный город», «экомониторинг», «лесной дозор», которые передают в операционные центры информацию о пожарах, загрязнении воздуха, штормовые предупреждения и т.д.[2]

В данных примерах ИИ осуществляет чисто технические функции управления инфраструктурой, однако существуют примеры, когда алгоритмы используются непосредственно при выполнении государственных функций: для обработки документов (особенно составленных по шаблону), взаимодействия с гражданами и первичной обработки их обращений, оптимизации делопроизводства, перехода на реестровую модель оказания государственных услуг, помощи при составлении бюджета, для моделирования последствий принятия законов (например налоговых реформ, политики в области здравоохранения), выявления мошенничества с налоговыми декларациями или заявлениями на получение государственной поддержки и т.д.

[1] Подробнее см.: Kumar S., Verma A.K., Mirza A. Digital Transformation, Artificial Intelligence and Society: Opportunities and Challenges. – 2024. – 218 p.

[2] Коданева С.И. Потенциал цифровых технологий для смягчения последствий и адаптации к изменению климата // Россия и современный мир. – 2022. – № 1 (114). – С. 63–85.

В Российской Федерации активно внедряется реестровая модель, которая позволит оказывать меры государственной поддержки по факту жизненной ситуации, а не на основании заявления гражданина[1], служба социального обеспечения США использует ИИ для ускорения обработки заявлений о нетрудоспособности за счет анализа медицинских карт и юридических документов, налоговое управление США использует ИИ для выявления случаев уклонения от уплаты налогов, ежегодно возвращая миллиарды долларов в бюджет, система ИИ во Франции выявляет мошеннические заявки на пособие по безработице, Национальная служба здравоохранения Великобритании использует ИИ для прогнозирования поступления пациентов и сокращения времени ожидания, Департамент полиции Лос-Анджелеса использует алгоритмы прогнозирования для снижения уровня преступности, Правительство Южной Кореи создало метавселенную для взаимодействия с гражданами и предоставления им государственных услуг, Европейский союз использует ИИ для оценки экономических последствий климатической политики до ее реализации.

Однако ИИ используется не только как помощник при принятии административных решений или прогнозирования последствий принятия того или иного нормативного правового акта. Его все чаще применяют при принятии судебных решений. Например, в феврале 2023 г. судья Хуан Мануэль Падилья из Картахены (Колумбия) попал в заголовки газет, использовав ChatGPT для вынесения судебного решения[2]. В другом случае федеральный судья Бразилии использовал ту же программу для вынесения решения. Однако оказалось, что ChatGPT в результате так называемой «галлюцинации» выдал несуществующие прецеденты Верховного суда Бразилии. Адвокат проигравшей стороны заметил мошенничество, сообщил об этом, и дело было направлено в Национальный совет правосудия Бразилии[3].

---

[1] Коданева С.И. Цифровое правительство: государство как платформа // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2022. – № 3. – С. 8–20.

[2] Xukang Wang, Ying Cheng Wu. Balancing Innovation and Regulation in the Age of Generative Artificial Intelligence // Journal of Information Policy. – 2024. – Vol. 14. – P. 385–416.

[3] Moretti J.L., Zuffo M.M. Artificial Intelligence in Law: Utilisation by Brazilian Legal Practitioners and Regulatory Challenges // Beijing Law Review. – 2025. – Vol. 16, N 1. – P. 331–352.

Для избежания подобных случаев «галлюцинаций» бесплатной версии ChatGPT судебные органы ряда стран стремятся создавать собственные системы ИИ. Например, система JurisprudênciaGPT, разработанная по заказу Апелляционного суда штата Парана (Бразилия), заняла второе место на конкурсе Gartner Eye on Innovation Awards 2024 для правительств Северной и Южной Америки. Она значительно оптимизирует юридические исследования, позволяя судьям и персоналу суда запрашивать обширную базу данных, содержащую более 4,9 млн судебных постановлений. Инструмент предоставляет точные ответы, подкрепленные ссылками, облегчая принятие решений и повышая эффективность судебной системы. Запущенный в 2018 г. Верховным судом Бразилии и Университетом Бразилиа проект Victor ускоряет обработку документов. Среди ключевых функций системы ИИ – преобразование изображений в текст, классификация и разделение документов, а также выявление повторяющихся юридических тем для более быстрого разрешения. В результате время анализа документов по одному делу сократилось с сорока четырех минут до пяти секунд[1].

В Китае проводится национальная политика, направленная на модернизацию юридического сектора путем внедрения «умных» судов. Цифровизация и использование технологий в судебной системе были включены в Национальную стратегию развития информатизации Китая в 2016 г.[2]

Таким образом, ИИ, несомненно, преобразует общество, коренным образом меняет бизнес-процессы, повышая эффективность, инновации и конкурентоспособность предприятий. Представляется, что компании, использующие ИИ, – от «интеллектуальных» фабрик до автономных цепочек поставок – возглавят следующую волну промышленного развития. Точно так же трансформируется государственное управление. ИИ повышает его эффективность, совершенствуя процессы принятия решений и их реализации. Правительства по всему миру используют ИИ для автоматизации бюрократических процессов, оптимизации распределения ресурсов и улучшения качества государственных услуг. От прогнозирования действий полиции и выявления мошенничества до чат-ботов на базе ИИ для взаимодействия с гражданами ИИ меняет принципы

[1] Moretti J.L., Zuffo M.M. Artificial Intelligence in Law: Utilisation by Brazilian Legal Practitioners and Regulatory Challenges // Beijing Law Review. – 2025. – Vol. 16, N 1. – P. 331–352.

[2] Ibid.

работы государственных органов. Вместе с тем столь стремительное развитие технологий и их массовое внедрение создает новые вызовы и риски, требующие оперативного осмысления и реакции юридического сообщества и законодательных органов.

Риски, связанные с внедрением искусственного интеллекта

Говоря о рисках внедрения ИИ, следует начать с их разграничения на технологические и социальные. Первые обусловлены как недостатками самих алгоритмов, приводящими к «галлюцинациям» и другим сбоям, так и возможностями для их противоправного использования для причинения вреда отдельным лицам. Вторые носят более глобальный и даже системный характер, поскольку сопряжены с потенциальной угрозой для основ государства и права.

Начнем с первых. Традиционно наибольшее внимание в научной литературе обращено проблемам конфиденциальности и безопасности персональных данных. Это связано с тем, что ИИ для полноценной работы необходимо обучаться на больших массивах данных, включая персональные. При этом разработчики ИИ и регулирующие органы сталкиваются с дилеммой: защита данных или качество ИИ и его развитие, поскольку ИИ, обученный на ограниченной выборке, может давать ложные результаты, а слишком жесткое регулирование в данной области затормозит развитие технологии. Существующие нормативные требования обязывают операторов ИИ обезличивать данные, однако на практике иногда происходят сбои, приводящие к нарушению прав человека. Новой тенденцией стало использование изображений и голосов для создания глубоких подделок (Deep Fakes). Количество контрактов на продажу лиц, в рамках которых покупаются, продаются и лицензируются как реальные, так и созданные ИИ данные о лицах, растет, поднимая новые юридические и этические вопросы о том, кому принадлежат права на лица тех, кто представлен в онлайн- и дополненной реальностях. Возникают двоякие риски: потенциальное неправильное использование персональных данных реального лица и введение в заблуждение посредством использования изображения, сгенерированного ИИ[1].

[1] Artificial Intelligence and Cybersecurity in Face Sale Contracts: Legal Issues and Frameworks / Lobna Abdalhusen Easa Al-saeedi, Doaa Fadhil Gatea Albo Mohammed, Firas Jamal Shakir, Faric Kamil Hasan, Ghadeer Ghazi Shayea, Yahya Layth

Следующей проблемой является достоверность результатов работы ИИ. Так, ИИ может вводить в заблуждение посредством алгоритмического обмана (например глубокие подделки, предвзятые выводы, основанные на алгоритме) или некачественных данных, использованных для обучения. Так, ChatGPT упрекают в том, что он выдает результаты на основе непроверенных данных из Интернета. Отсутствие механизма фильтрации на этапе предварительного обучения приводит к генерации ошибочной или ложной информации, что усугубляется сложной природой алгоритмов глубокого обучения[1]. Соответственно, правильность работы ИИ зависит от качества наборов данных, надежной работы алгоритмов в различных сценариях и соответствия полученных результатов реальности. Важно также правильное использование самих алгоритмов, которые различаются по механизмам работы. Соответственно, один и тот же ИИ может правильно предсказывать тенденции развития определенных явлений, но выдать ошибочный результат при решении текущей оперативной задачи, и наоборот. Кроме того, любой ИИ отражает этические и моральные принципы его разработчиков; в результате он может выдавать достоверный результат для одной нации, но ошибочный для другой, придерживающейся других духовных ценностей. Поэтому в научной литературе абсолютное большинство авторов призывают к прозрачности ИИ. Однако следует учитывать, что прозрачность отнюдь не всегда обеспечивает достоверность. Более того, зачастую это два противоречащих друг другу принципа работы ИИ[2]. Прозрачность в ИИ означает ясность и открытость процессов принятия решений: что позволяет пользователям, регулирующим органам и заинтересованным сторонам понимать и тщательно изучать системы ИИ, что, однако, приводит к упрощению алгоритма. Достоверность, с другой стороны, касается точности и надежности результатов ИИ, однако высокоточным моделям ИИ (например, «черным ящикам» глубокого обучения) может не хватать интерпретируемости, что снижает прозрачность.

Khaleel, Mustafa Habeeb // Mesopotamian Journal of Cybersecurity. – 2024. – Vol. 4, N 2. – P. 129–142.

[1] Xukang Wang, Ying Cheng. Wu Balancing Innovation and Regulation in the Age of Generative Artificial Intelligence // Journal of Information Policy. – 2024. – Vol. 14. – P. 385–416.

[2] Подробнее см.: Marwala T. The Balancing Problem in the Governance of Artificial Intelligence. – 2024. – 251 p.

Еще одной широко обсуждаемой проблемой ИИ является алгоритмическая дискриминация. Этот риск повсеместного внедрения ИИ обсуждается наравне с проблемой защиты персональных данных. Здесь следует добавить, что алгоритмическая дискриминация бывает двух типов: корректируемая предвзятость и присущие ИИ ограничения. Первый тип может быть обусловлен нерепрезентативностью данных или ошибкой дизайна алгоритма. Второй – несовершенным уровнем развития технологий, их недостатками (например неспособностью учитывать контекстуальные нюансы), либо нормативными ограничениями (что опять-таки пересекается с проблемой использования персональных данных для обучения алгоритмов). Соответственно, бороться с первым типом алгоритмической дискриминации можно чисто техническими способами. Во втором случае возможно информирование пользователей о заложенных недостатках, а также вовлечение всех заинтересованных сторон в разработку ИИ для поиска путей устранения данного типа алгоритмической дискриминации.

Что касается социальных рисков, то наиболее обсуждаемыми из них являются сокращение рабочих мест за счет автоматизации рутинных рабочих процессов, а также уже упоминавшаяся трансформация ряда отраслей посредством перехода на модель фриланса, когда люди из работников, защищенных трудовым законодательством, переходят в разряд самозанятых, лишенных всех трудовых прав и гарантий.

Еще одним распространенным явлением стала «макдонализация» многих сфер хозяйства, которая означает распространение бизнес-принципов предприятий быстрого питания на рабочие процессы других учреждений. Например, электронные системы медицинского контроля дегуманизируют медицинскую практику, поскольку врачи проводят 40% своего рабочего времени за компьютерами и только 12% – с клиентами. При этом они все в большей мере полагаются на Интернет, переставая запоминать многие важные для клинической практики вещи. Высказываются опасения, что это будет способствовать де-профессионализации врачей и сокращению рабочих мест.

Р. Вон Майдель и К. Мензель обращают внимание на трансформацию антиконкурентных практик, поскольку цифровые монополии получают массу возможностей для злоупотреблений в рамках действующего законодательства. В связи с этим они призывают принимать антимонопольные меры на ранней стадии, а не после осознания того, что фирмы достигли доминирующего поло-

жения на рынке. Это касается таких практик, как алгоритмический сговор, «огороженные сады» (когда платформы навязывают пользователям различные сервисы, вынуждая их оставаться в рамках одной экосистемы), «убийственные приобретения» (покупка стартапов с единственной целью недопущения конкуренции) и т.п.[1]

Широкое распространение глубоких подделок позволяет создавать гиперреалистичные тексты, изображения, аудио и видео. С одной стороны, это может быть полезно в индустрии игр и развлечений. Однако все чаще технология используется в преступных целях – для создания фейковых новостей и ложного контента, как для мошенничества, так и для манипулирования общественным сознанием. Нашумевшим примером первого стал случай, когда банковского менеджера в Гонконге обманом заставили перевести 35 млн долл. после того, как он услышал голос руководителя, созданный с помощью ИИ. Второй вариант неправомерного использования ИИ представляет собой значительный социальный риск. В сочетании с так называемыми «эхо-камерами», системой таргетирования на основе анализа пользовательских запросов с помощью ИИ, происходит фрагментация публичного дискурса, наполнение его ложными нарративами, ограничение доступа людей к полной и достоверной информации. Система фильтров, используемых социальными платформами, также сужает сферу, в которой граждане, делящиеся своим мнением, могут быть услышаны. Как отмечает С.Х. Кан, такое подавление свободы выражения мнений фактически разрушает основу демократии, которая всегда строилась на свободном обмене мнениями и идеями. Он подчеркивает, что деятельность платформ социальных сетей по модерации онлайн-контента представляет угрозу свободе выражения мнений в киберпространстве, особенно учитывая, что модерацию осуществляет ИИ, который не способен распознавать культурные нюансы, например в пародии или сатире. Одновременно инструменты компьютерной пропаганды, включая ботов и троллей, стали новым типом политического ресурса, владея которым, партии получают конкурентное преимущество перед своими оппонентами, что ока-

[1] Maydell R. von, Menzel Ch. The Rise of Artificial Intelligence: Towards a Modernisation of Competition // AI in Business and Economics. – 2024. – P. 3–16. – URL: https://www.researchgate.net/publication/383929954_Chapter_1_The_Rise_of_Artificial_Intelligence_Towards_a_Modernisation_of_Competition_Policy (дата обращения: 12.04.2025).

зывает негативное влияние на выборы как основную форму представительной демократии[1].

Одновременно ИИ предоставляет широкие возможности для массовой слежки и контроля за поведением миллионов людей по всему земному шару. Причем возможностями этими пользуются не только и не столько государства, сколько транснациональные корпорации, получающие неограниченные возможности влияния как на массовое сознание и поведение людей, так и на сферу государственного управления. Это усиливается в случае чрезмерного и неконтролируемого использования алгоритмов в государственной сфере, особенно, когда пользователи – чиновники и государственные служащие – не имеют достаточных компетенций для проверки достоверности полученных с помощью ИИ результатов.

Таким образом, социальные риски использования ИИ таят в себе угрозу не только отдельным людям, страдающим от мошенников или алгоритмической дискриминации. Они способны создавать дисбалансы или даже разрушать целые отрасли экономики, а также подрывать правовые основы демократического государственного управления.

Правовые подходы к преодолению рисков использования искусственного интеллекта

Практически все страны мира озабочены выработкой собственных подходов к правовому регулированию использования ИИ. Основное внимание при этом уделяется защите персональных данных, прозрачности ИИ, особенно используемого в сфере государственного управления, а также защите от подделок. Преимущественно государства придерживаются трех принципиальных подходов: в США правовое регулирование довольно обширно, однако преимущественно направлено на стимулирование развития ИИ. Что касается ограничений, то они устанавливаются отраслевыми ведомствами посредством утверждения технических стандартов. Законодательство Евросоюза, напротив, характеризуется направленностью на защиту от рисков, прежде всего, когда речь идет о

[1] Kan C.H. Artificial Intelligence (AI) in the Age of Democracy and Human Rights: Normative Challenges and Regulatory Perspectives // International Journal of Eurasian Education and Culture. – 2024. – Vol. 9, N 25. – P. 145–166.

правах человека[1]. При этом правоприменительная практика в странах ЕС также отличается жесткостью. Например, в Италии и Польше ChatGPT запретили как нарушающий принципы обработки персональных данных. Ряд стран (например Китай, Южная Корея, ОАЭ) принимают государственные планы, стратегии или политики, направленное на подконтрольное государству развитие технологии. Страны Латинской Америки, в частности Бразилия, при разработке собственного правового регулирования стараются учитывать требования ЕС, балансируя их с собственными национальными особенностями развития[2].

Однако по-прежнему остается ключевым вопрос о поиске наиболее оптимального подхода к правовому регулированию ИИ, учитывая необходимость соблюдения баланса между защитой общественных интересов, развитием этичного ИИ и поощрением инноваций. Двумя принципиально различными подходами являются нормативное регулирование и саморегулирование. Саморегулирование охватывает процесс, посредством которого индустрия искусственного интеллекта устанавливает и внедряет свой собственный набор правил. Этот подход основан на использовании знаний и опыта профессионалов бизнеса, поощряя творческий подход и позволяя быстро адаптироваться к технологическому прогрессу, предлагать индивидуальные решения для уникальных проблем, связанных с развитием ИИ. Очевидным недостатком саморегулирования является то, что бизнес всегда будет думать, прежде всего, о своей прибыли. Поэтому установление представителями отрасли внутренних правил и этических принципов не позволит в полной мере защищать более широкие, общественно значимые ценности, такие как защита персональных данных, единство технических требований и стандартов, обеспечивающих безопасность ИИ, и т.п. Инновации и рыночная конкуренция могут вступать в противоречие с этическими соображениями и важностью предупреждения рисков, что, в итоге, может привести к снижению уровня стандартов безопасности.

[1] Алферова Е.В., Скурко Е.В. Нормативные подходы Европейского союза и Соединенных Штатов Америки к правовому регулированию искусственного интеллекта: сравнительные аспекты // Актуальные проблемы Европы. – 2025. – № 2. – С. 43–57.

[2] Walter Y. Managing the Race to the Moon: Global Policy and Governance in Artificial Intelligence Regulation–A Contemporary Overview and an Analysis of Socio-economic Consequences // Discover Artificial Intelligence. – 2024. – Vol. 4, N 14. – P. 4.

В этом смысле нормативное регулирование является более приоритетным. Однако органам власти трудно оперативно реагировать на стремительное развитие технологий. При этом возможно использование четырех типов государственного регулирования: принятие общих стратегий и политик, законов, регулирование с помощью подзаконных актов (в частности путем установления экспериментальных правовых режимов) и установление технических стандартов, обеспечивающих минимальный уровень безопасности. Как было показано выше, на современном этапе государства, как правило, используют какой-то один из этих правовых подходов либо сочетание двух из них. Например, принятие стратегии и утверждение стандартов (США), принятие политики (принципов разработки ИИ) и реализация экспериментов на уровне провинций, регулируемых местным законодательством (Китай), принятие стратегии и подзаконного регулирования в рамках экспериментальных правовых режимов (Россия), принятие законов (ЕС).

Однако достижение баланса между развитием инноваций и защитой общественных интересов требует комплексного подхода. Во-первых, необходимо законодательно закрепить требование учета этических вопросов при разработке ИИ в форме базовых принципов (объяснимость ИИ в сочетании с достоверностью, отсутствие алгоритмической дискриминации, неприкосновенность частной жизни, обеспечение справедливого доступа к ИИ для всех). Во-вторых, необходим государственный контроль за соблюдением этих руководящих принципов. В-третьих, – расширение использования «цифровых песочниц» для выработки оптимального правового регулирования ИИ в сочетании с постоянным мониторингом и оценкой формирующихся правоотношений с целью оперативной адаптации государственной политики с учетом возникающих проблем и возможностей ИИ. В-четвертых, – тесное взаимодействие между государством, обществом, представителями отрасли ИИ, и использующими алгоритмы представителями других отраслей бизнеса, а также баланс между регулированием и саморегулированием.

Заключение

Как можно видеть, развитие ИИ значительно опережает даже самые смелые прогнозы специалистов в данной области технологий. Не отстает от него и трансформация общественных отношений, формируя принципиально новую социальную реальность.

Это ставит перед лицом юридического сообщества вызов, обусловленный не просто необходимостью поиска инструментальных решений в отдельных отраслях законодательства, но формирования новаторских подходов к осмыслению базовых правовых концепций. В этой связи нельзя не согласиться с П. Бургесом, который в своей монографии анализирует развитие концепции верховенства права под влиянием общественных преобразований, показывая, что эта концепция со временем трансформировалась и расширялась – современное верховенство права означает обязанность государства по недопущению произвола власти, от кого бы он не исходил – государства или частного субъекта. Автор приходит к выводу, что существующие рамки верховенства права, включая его современные концепции, не могут адекватно регулировать использование ИИ. Это означает, что концепция верховенства права должна трансформироваться, чтобы оставаться актуальной в условиях развития ИИ. При этом она не может быть продолжением прошлого – новую концепцию верховенства права необходимо «изобрести заново», чтобы ограничить власть ИИ, сохраняя при этом справедливость, прозрачность и демократическую легитимность, как когда-то заново сформулировал эту концепцию А. Дайси в ответ на проблему, которая возникла в его обществе[1].

Действительно, сегодня общество сталкивается с рисками произвола власти ИИ или тех, кто его разрабатывает / использует. Это означает, что формы правового регулирования отношений могут видоизменяться. Неизменными должны оставаться две вещи. Во-первых, на государстве должна лежать ответственность за недопущение произвола власти и нарушения прав человека любым субъектом регулирования, будь то государственный аппарат или технологические компании. Во-вторых, в какой бы форме не осуществлялось государственное управление и как бы при этом не использовался ИИ, ответственность всегда лежит на конкретном человеке. Должностные лица не должны в обоснование своих решений ссылаться на ИИ, перекладывая ответственность на алгоритмы. Они должны четко осознавать, что алгоритм – это не более чем инструмент, помощник, но любое решение, влекущее правовые последствия – хоть для одного человека, хоть для общества в целом, – принимает конкретный государственный служащий, несущий за это решение полную ответственность.

[1] Burgess P. AI and the Rule of Law. The Necessary Evolution of a Concept. – 2024. – 200 p.

УДК 004.8; 34.096 DOI: 10.31249/iajpravo/2025.03.02

ЯДОВА М.А.[1] СОЦИАЛЬНЫЙ ПОРТРЕТ РОССИЙСКИХ ПОЛЬЗОВАТЕЛЕЙ СЕРВИСАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПОПЫТКА АНАЛИЗА (Статья)

Аннотация. В статье анализируются социально-демографические характеристики пользователей сервисами искусственного интеллекта в России и за рубежом. Отмечается существенный (почти взрывной) рост количества пользователей ИИ-сервисов и объем трафика, потраченного на эти сервисы, в последние годы. Анализируется отечественный рынок запросов к ИИ-сервисам и примеры применения искусственного интеллекта в повседневной жизни, образовательной деятельности, деловой сфере и т.п. Особое внимание уделяется рискам и возможностям использования искусственного интеллекта, в том числе обсуждаются вопросы этико-правового характера.

Ключевые слова: пользователи сервисами искусственного интеллекта; российское общество; риски и возможности использования ИИ; права человека; молодежь.

YADOVA M.A. Social Portrait of Russian Users of Artificial Intelligence Services: An Attempt at Analysis (Article)

Abstract. The article analyzes the socio-demographic characteristics of users of artificial intelligence services in Russia and abroad. It marks a significant (almost explosive) growth in the number of users of AI services and the volume of traffic spent on these services in recent years. It analyzes the domestic market of requests for AI services and examples of AI application in everyday life, in the educational sphere, in the business sphere, etc. The risks and opportunities of using AI are given special attention, including discussion of ethical and legal issues.

[1] *Ядова Майя Андреевна*, заведующая отделом социологии и социальной психологии ИНИОН РАН, кандидат социологических наук.

Keywords: users of artificial intelligence (AI) services; Russian society; risks and opportunities of using AI; human rights; youth.

Для цитирования: Ядова М.А. Социальный портрет российских пользователей сервисами искусственного интеллекта: попытка анализа (Статья) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2025. – № 3. – С. 23–32. – DOI: 10.31249/iajpravo/2025.03.02.

Введение

В 2023 г. авторы известного британского словаря *Collins*, проанализировав огромный массив информации, представленной во всем мире в Интернете, СМИ, книгах и пр., назвали словом года термин «искусственный интеллект» (ИИ). Несмотря на то, что не все это осознают, продукты и сервисы, связанные с ИИ, уже стали частью нашей повседневной жизни: миллионы людей ежедневно с ними взаимодействуют, воспользовавшись персональными рекомендациями в онлайн-магазинах и для проведения досуга, заручившись помощью виртуальных помощников или используя технологии «умного дома». Согласно данным ряда актуальных социальных исследований, уровень осведомленности россиян и жителей зарубежных стран о возможностях технологий ИИ растет с каждым годом. По словам К.О. Вишневского, директора Центра стратегической аналитики и больших данных ИСИЭЗ НИУ ВШЭ, «былые завышенные ожидания от технологий ИИ сегодня сменились более продуманным отношением: решения на их основе постепенно становятся неотъемлемым инструментом бизнеса и применяются практически во всех сферах деятельности – от мониторинга сельхозугодий и управления космическими аппаратами до помощи в написании научных работ и новостей СМИ»[1].

Растущий интерес к этой сфере и расширение соответствующих потребительских запросов населения привели к появлению новых бизнес-возможностей на основе ИИ. Особую популярность приобрели многозадачные и мультимодальные мегамодели, одновременно работающие с разными типами данных (текстом, изображениями, речью). Скорость внедрения технологий ИИ в нашу повседневную жизнь впечатляет: например, она в два раза

[1] Туровец Ю.В., Вишневский К.О. Искусственный интеллект в России: кто, что и как внедряет. – 2023. – 26 сентября. – URL.: https://issek.hse.ru/news/862013645.html (дата обращения: 20.04.2025).

выше, чем была в эпоху появления персональных компьютеров и Интернета. Согласно результатам опроса сотрудников крупнейших компаний из 101 страны мира, проведенного исследователями McKinsey & Company в 2024 г., 72% современных организаций используют в своей деятельности сервисы, связанные с искусственным интеллектом, хотя еще в 2023 г. число таких организаций не превышало 50%[1]. Это позволяет говорить о всплеске интереса к сервисам ИИ на глобальном уровне.

Штрихи к портрету пользователя ИИ-сервисами

Опираясь на данные ряда социологических исследований, попытаемся составить социальный портрет типичного пользователя ИИ-сервисами. Согласно данным американского исследовательского центра Pew (исследование проводилось в 2022 г.), 90% американцев хотя бы немного слышали о возможностях ИИ, тогда как треть осведомлена о них достаточно хорошо. Заметим, что степень осведомленности напрямую связана с уровнем образования опрошенных: чем он выше, тем более открыт человек ИИ-технологиям[2]. Особый интерес пользователей вызывают возможности генеративных программ, способных создавать текст и изображения (типа ChatGPT). В США 58% взрослых и 67% подростков 13–17 лет знакомы с подобными программами, причем среди подростков почти каждый пятый использует чат-боты в учебе[3]. По другим данным, в США почти 40% взрослых американцев в возрасте от 18 до 64 лет в той или иной мере прибегают к помощи генеративного ИИ, около трети респондентов делают это ежедневно или, по крайней мере, несколько раз в неделю[4]. Примечательно, что технологии ИИ чаще используют дома (32,6%), чем на работе (28,1%)[5].

[1] Burmagina K. Artificial Intelligence Usage Statistics and Facts. – URL.: https://elfsight.com/blog/ai-usage-statistics/ (дата обращения: 20.04.2025).

[2] Faverio M., Tyson A. What the Data Says about Americans' Views of Artificial Intelligence. – URL: https://www.pewresearch.org/short-reads/2023/11/21/what-the-data-says-about-americans-views-of-artificial-intelligence/ (дата обращения: 20.04.2025).

[3] Ibid.

[4] Burmagina K. Op. cit.

[5] Ibid.

Очень популярны технологии ИИ в Китае, в стране разработано более 200 крупных ИИ-моделей, а число пользователей сервисов и приложений на основе генеративного искусственного интеллекта составило в 2024 г. 600 млн[1]. Китайские исследователи нередко пытаются совместить возможности чат-ботов с другими высокотехнологичными разработками (человекоподобные роботы, смартфоны, компьютеры, самоуправляемые автомобили и пр.), это способствует прорывам в промышленной, финансовой, медицинской, образовательной и других сферах.

Если говорить об отечественных реалиях, то среди россиян уровень осведомленности об ИИ-технологиях очень высок. Например, согласно совместному проекту «Новое российское общество: граждане и искусственный интеллект» консалтинговой компании «Яков и Партнёры» и исследовательского холдинга РОМИР, 84% россиян знают, что такое искусственный интеллект[2]. По данным исследования ВЦИОМ, в общей сложности 94% россиян в той или иной степени информированы о технологиях ИИ. По сравнению с 2022 г. доля россиян, хорошо разбирающихся в «хитростях» ИИ, выросла с 36% до 50%, в 2024 г. число впервые услышавших об этом явлении ничтожно мало и составляет всего лишь 6%, а в 2021 г. таковых было втрое больше (18%)[3]. Наверное, закономерно, что чем моложе человек, тем лучше он ориентируется в мире высоких технологий. Согласно данным ВЦИОМ, 74% в группе 18–24-летних, 67% среди 25–34-летних, 57% среди 35–44-летних способны примерно объяснить механизмы работы ИИ, и наоборот, россиян старше 45 лет вопросы об ИИ часто ставят в тупик (51–59%)[4].

---

[1] Подробнее см.: Искусственный интеллект (рынок Китая). – 2025. – 17 апреля. – URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D1%81%D0%BA%D1%83%D1%81%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B8%D0%BD%D1%82%D0%B5%D0%BB%D0%BB%D0%B5%D0%BA%D1%82_(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%9A%D0%B8%D1%82%D0%B0%D1%8 F) (дата обращения: 20.04.2025).

[2] Новое российское общество: граждане и искусственный интеллект / Яков и партнеры, РОМИР. – 2024. – URL.: https://yakovpartners.ru/publications/russian-citizens-and-ai/ (дата обращения: 20.04.2025).

[3] Доверие к ИИ / ВЦИОМ. – 2024. – 24 декабря. – URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/doverie-k-ii (дата обращения: 20.04.2025).

[4] Там же.

Такой высокий показатель осведомленности сопоставим с приведенными выше данными о США и значительно выше, чем в Великобритании (64%) и Германии (61%)[1]. Вероятно, это связано с тем, что наша страна имеет собственные крупные разработки в области искусственного интеллекта, наиболее известными из которых являются GigaChat, Kandinsky (Сбербанк), YaLM («Яндекс»).

По данным исследования РОМИР, около четверти россиян (24%) используют генеративный ИИ в личных или рабочих целях, причем почти каждый второй (47%) из их числа отдает предпочтение российским чат-ботам, а 36% пользуются одновременно российскими и зарубежными продуктами[2]. Наиболее активными пользователями ИИ-сервисов в течение последнего года были представители младшей когорты поколения центениалов (зумеров) – юноши и девушки в возрасте 18–19 лет, а также респонденты с высоким уровнем дохода[3]. Так, среди младших зумеров генеративным ИИ пользуются 42%, с возрастом опрошенных снижается частота использования таких сервисов. Например, среди 20–37-летних доля тех, кто пользуется технологиями генеративного ИИ, составляет уже 28%, в возрастной группе от 38 до 58 лет – 22%, а в подвыборке 59–64-летних – лишь 11%. Стоит подчеркнуть, что россияне всех возрастных групп в большей степени пользуются ИИ-сервисами в повседневных личных целях, нежели для работы. Доля тех, кто использует чат-боты в личных целях, варьируется от 46% среди зумеров до 24% в старших возрастных группах; в профессиональных целях применяют ИИ не более 10–12% опрошенных[4].

---

[1] Новое российское общество: граждане и искусственный интеллект / Яков и партнеры, РОМИР. – 2024. – URL.: https://yakovpartners.ru/publications/russian-citizens-and-ai/ (дата обращения: 20.04.2025).

[2] Там же.

[3] В данной работе мы используем устоявшиеся названия первых цифровых поколений в нашей стране и за рубежом – миллениалы и центениалы (зумеры). Кратко поясним их. Термин «миллениалы» (от лат. millennium – тысячелетие) был предложен исследователями в конце прошлого столетия для обозначения детей, которые должны были окончить среднюю школу на рубеже веков. Обычно к этому поколению относят родившихся в середине 1980-х – конце 1990-х годов. Представители следующего за миллениалами поколения центениалов (от англ. centennial – столетний), или Поколения Z (зумеры), родились уже в XXI веке, т.е. старшим из них не более 25 лет.

[4] Там же.

Ключевые сферы взаимодействий россиян с ИИ – это, как правило, социальные сети и Интернет, искусство, развлечения, технологии «умного дома». Интернет и соцсети – самое частое место встречи с возможностями ИИ для представителей всех возрастных групп. Исследователи нередко отмечают специфические поколенческие предпочтения при обращении к ИИ-сервисам. Например, миллениалы, представляющие наравне с зумерами еще одно цифровое поколение россиян, активнее всего используют в повседневной жизни технологии «умного дома» и разработки, касающиеся сферы искусства и развлечений[1].

Вместе с тем популярность сервисов ИИ не снимает чувствительных вопросов, связанных с этичностью применения этих технологий в определенных случаях. Чуть более половины россиян (52%) склонны скорее доверять ИИ-технологиям, а каждый третий (38%) скорее не доверяет; лишь молодежь до 25 лет верна себе: уровень доверия в этой когорте составляет 79%[2]. И если с причинами доверять ИИ все достаточно понятно (они делают нашу жизнь более комфортной, беспристрастность ИИ снижает вероятность ошибок и т.п.), то к причинам недоверия наших соотечественников к ИИ-технологиям стоит присмотреться внимательнее. Прежде всего опасения россиян вызывают вероятные сбои в работе ИИ (28%), выход из-под контроля человека (26%), возможность использования ИИ в корыстных целях (23%), риск утечки данных, собираемых ИИ (21%), возможная личностная деградация, спровоцированная «замещением» человека бездушной машиной (20%)[3].

Искусственный интеллект vs личность: риски и возможности использования ИИ-технологий

Подчеркнем, что тема «очеловечивания» ИИ и возможной «замены» им человека волнует исследователей давно. Предлагаем поразмышлять над тем, насколько эти страхи оправданны. Один из самых известных современных ученых, занимающихся осмыслением феномена ИИ, профессор Гарвардского университета М. Риссе полагает, что нам стоит готовиться к новому миру (по-

[1] Новое российское общество.

[2] Доверие к ИИ / ВЦИОМ. – 2024. – 24 декабря. – URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/doverie-k-ii (дата обращения: 20.04.2025).

[3] Там же.

хожему на те, что показаны в антиутопиях), в котором наравне с человеком будут существовать новые сверхинтеллектуальные «формы жизни»; в связи с этим социальным исследователям необходимо адекватно оценивать новые вызовы и искать пути их преодоления[1]. Риссе убежден, что активное внедрение в нашу жизнь систем ИИ негативно влияет на сферу прав человека. Он считает, что человечеству придется выработать «правила игры» для нового мира, игроками которого будут в числе прочих интеллектуальные машины. Причем, по его мнению, необходимо отрегулировать механизм взаимодействия с ИИ таким образом, чтобы была возможность неукоснительно защищать права человека от «самоуправства» машинного сверхинтеллекта[2]. М. Риссе, безусловно, прав: в цифровую эпоху как никогда должны соблюдаться принципы приватности, свободы слова, справедливости и равенства, а работу алгоритмов ИИ следует подчинить этико-правовым нормам.

В последние годы в нашей стране и за рубежом был разработан ряд этических кодексов относительно деятельности ИИ. Например, в 2021 г. в России был подписан Кодекс этики в сфере ИИ, в котором говорится о человеческой ответственности за моральные риски разработки и внедрения ИИ и фиксируется необходимость учета гуманистической направленности этой работы[3]. Широкую известность получили также рекомендации ЮНЕСКО, которые касаются этичного применения ИИ-технологий и учета возможных последствий разработок в области ИИ «для людей, сообществ, окружающей природной среды и экосистем»[4]. Подобные рекомендации становятся своего рода стандартом для дальнейшей этической и нормативно-правовой оценки аспектов использования технологий ИИ. Кроме того, в разных странах, например, в США, Китае, государствах Евросоюза, в последние годы были приняты

[1] Risse M. Political Theory of the Digital Age: Where Artificial Intelligence Might Take Us. – Cambridge, 2023. – P. XI–XII.

[2] Risse M. Human Rights and Artificial Intelligence: An Urgently Needed Agenda. – 2018. – May 18. – (HKS Working Paper; N RWP18–015. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3180741 (accepted 20.04.2025).

[3] Подробнее см.: Кодекс этики в сфере ИИ. – URL: https://ethics.a-ai.ru/ (дата обращения: 20.04.2025).

[4] Государства-члены ЮНЕСКО принимают первые глобальные соглашения по этическим аспектам искусственного интеллекта. – URL: https://unesdoc.unesco.org/ark:/48223/pf0000380455_rus (дата обращения: 20.04.2025).

законы, призванные защитить права людей от потенциальных негативных последствий применения ИИ.

Также интерес для обществоведов представляет тема уместности использования разработок на основе ИИ в зависимости от социального контекста. Например, исследователи из Австралии и Нидерландов (С. Келли с коллегами)[1], проведя метаанализ результатов 60 проектов о готовности современного человека применять ИИ-технологии в повседневной жизни, обнаружили, что на желание или нежелание взаимодействовать с системами ИИ влияет комплекс факторов, включая социокультурные и социально-демографические особенности. Стоит допустить, что при всей полезности использования ИИ в образовательной деятельности, в некоторых учебных коллективах такая практика вряд ли будет продуктивна. Так, члены христианских общин не считают правильным использовать возможности ИИ в процессе религиозного обучения[2]. Объясняется это тем, что религиозное образование включает в себя передачу духовного опыта и установление эмоционального контакта между учителем и учащимся; ИИ обеспечить такую связь не может. В другом исследовании обнаружилось, что на отношение подростков к практикам использования ИИ непосредственно влияет их ближайшее окружение сверстников; в таком случае интерес к экспериментам с ИИ может быть своеобразной данью моде[3].

Кажущиеся безграничными возможности ИИ «спотыкаются» о неспособность автоматизированных систем к социальности. По мнению британского социолога М. Арчер, ИИ проигрывает личности по нескольким причинам: ИИ-системы не имеют представлений о нормативности, и у них отсутствует эмоциональный и чувственный опыт[4]. С.М. Арчер согласен ее коллега Г. Коллинз,

[1] Kelly S., Kaye Sh.-A., Oviedo-Trespalacios O. What Factors Contribute to the Acceptance of Artificial Intelligence? A systematic review // Telematics and Informatics. – 2023. – Vol. 77. – P. 1–33.

[2] Tran K., Nguyen T., Kimura T. Preliminary Research on the Social Attitudes toward AI's Involvement in Christian Education in Vietnam: Promoting AI Technology for Religious Education // Religions. – 2021. – Vol. 12, N 3. – P. 208.

[3] Social Influence on Risk Perception During Adolescence / Knoll L.J., Magis-Weinberg L., Speekenbrink M., Blakemore S.-J. // Psychological Science. – 2015. – Vol. 26, N 5. – P. 583–592.

[4] Archer M.S., Morgan J. Contributions to Realist Social Theory: an Interview with Margaret S. Archer // Journal of Critical Realism. – 2020. – Vol. 19, N 2. – P. 179–200. – DOI: 10.1080/14767430.2020.1732760

отмечающий в качестве ключевых признаков человеческого мышления социальность и моральность; по его мнению, процесс социализации невозможно заменить лишь колоссальными объемами информации[1]. В данном контексте ущербность систем ИИ очевидна, они – если оперировать терминологией М. Риссе, скорее внесоциальны и внеморальны.

Как показывают вышеприведенные данные, наибольший интерес к ИИ-технологиям, как правило, наблюдается у представителей самого младшей возрастной группы, и наоборот, у старших поколений тема ИИ находится на периферии сознания. Кажется очевидным, что эти реакции зависят от уровня цифровой компетентности опрошенных. Согласно массовым опросам, проведенным специалистами ИСИЭЗ НИУ ВШЭ, лучше всего цифровые навыки развиты у поколения зумеров (15–24 года): 2/3 из них обладают высоким или базовым уровнем цифровой грамотности. Примерно схожие цифры можно наблюдать в группе миллениалов, представителей первого цифрового поколения в мире[2]. В старших возрастных группах, начиная примерно с 45-летнего возраста, уровень цифровой грамотности постепенно снижается, для чуть менее половины россиян старше 65 лет не существует даже Интернета, не говоря уж о других более продвинутых технологиях. Если предположить, что разработки в сфере ИИ будут продолжать внедряться в нашу повседневную жизнь теми же темпами, что сейчас, то можно спрогнозировать постепенное вовлечение в мир высоких технологий и искусственного интеллекта даже представителей самого старшего «мобилизационного» поколения, которое обычно считается потерянным для освоения цифровых навыков. Конечно, такая вовлеченность невозможна без помощи более продвинутых в цифровом плане младших родственников или друзей. Данная гипотеза косвенно подтверждается результатами некоторых социально-психологических исследований. Например, по результатам исследования, проведенного отечественными психологами Г.У. Солдатовой и Е.И. Рассказовой, цифровая компетентность и интернет-активность представителей старших поколений россиян зачастую зависит от интенсивности их контактов с младшими род-

[1] Collins H. Why Artificial Intelligence Needs Sociology of Knowledge: parts 1, 2 // AI & Society. – 2024. – May 18. – URL: https://link.springer.com/article/10.1007/s00146-024-01954-8 (accessed: 20.04.2025).

[2] Петрова В. Интернет по возрасту считают // Коммерсант. – 2022. – 27 июля. – URL: https://www.kommersant.ru/doc/5481130 (дата обращения: 20.04.2025).

ственниками, которые выполняют роль медиаторов в процессе освоения старшими информационных технологий[1].

Заключение

Подводя итоги, отметим, что в последние годы сервисы, связанные с применением ИИ, прочно вошли в нашу повседневную жизнь. Множество людей, даже не осознавая этого, ежедневно прибегают к помощи технологий ИИ, например используя персонализированные подсказки ИИ, отбирая нужную информацию для работы, учебы или продумывая варианты досуга. По уровню осведомленности о деятельности ИИ россияне в целом не уступают жителям зарубежных стран, а в некоторых случаях даже их превосходят. Согласно результатам ряда социологических исследований, молодежь традиционно наиболее продвинута в освоении технологий ИИ, особенно возможностей генеративных чат-ботов. Кроме того, молодые люди отличаются от старших поколений большим технологическим оптимизмом по отношению к ИИ и последствиям его деятельности, гораздо реже видя угрозы со стороны новейших технологий. Вместе с тем внедрение систем ИИ породило немало чувствительных вопросов этико-правового характера, касающихся возможных рисков для человечества. Это требует выработки новых теоретических и практических подходов для осмысления феномена искусственного интеллекта и поиска безопасных и гуманистически ориентированных алгоритмов взаимодействий с ним.

[1] Солдатова Г.У., Рассказова Е.И. «Цифровой разрыв» и межпоколенческие отношения родителей и детей // Психологический журнал. – 2016. – Т. 37, № 5. – С. 44–54.

УДК 34.096 DOI: 10.31249/iajpravo/2025.03.03

КАРЦХИЯ А.А.[1] НОВЫЕ ГРАНИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПРАВОВОЙ АСПЕКТ (Статья)

Аннотация. Современное общество переживает трансформационные изменения, обусловленные достижениями в области искусственного интеллекта и других передовых технологий, которые меняют мировую экономику, повышают производительность и стимулируют инновации во всех отраслях. Быстрое развитие генеративного ИИ произвело революцию в производительности труда и творческих процессах, но породило ряд проблем и рисков, решение которых возможно только совместными усилиями международного сообщества, направленными на то, чтобы сбалансировать инновации в области ИИ с защитой прав человека, национальными ценностями и контролем с учетом рисков.

Ключевые слова: искусственный интеллект; нейронные сети; безопасность искусственного интеллекта; кибербезопасность; технологический суверенитет; угрозы и риски технологии ИИ; устойчивое развитие.

KARTSKHIYA A.A. New Facets of Artificial Intelligence: Legal Aspect (Article)

Abstract. Modern society is undergoing transformational changes driven by advances in artificial intelligence and other advanced technologies that are reshaping the global economy, increasing productivity and stimulating innovation in all industries. The rapid development of generative AI has revolutionized labor productivity and creative processes, but it has created a number of problems and risks that can only be solved through the joint efforts of the international community aimed at

[1] © *Карцхия Александр Амиранович*, профессор РГУ нефти и газа (НИУ) им. И.М. Губкина, доктор юридических наук.

balancing AI innovation with the protection of human rights, national values, and risk-based control.

Keywords: artificial intelligence; neural networks; artificial intelligence security; cybersecurity; technological sovereignty; threats and risks of AI technology; sustainable development.

Для цитирования: Карцхия А.А. Новые грани искусственного интеллекта: правовой аспект (Статья) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2025. – № 3. – С. 33–46. – DOI: 10.31249/iajpravo/2025.03.03

Введение

Искусственный интеллект стал одной из самых преобразующих технологий XXI века, изменяющей экономику, общество и структуры управления по всему миру. Стремительный прогресс в области ИИ, особенно в таких генерирующих моделях, как ChatGPT, Claude и Gemini от Google, ускорил внедрение инноваций в различных отраслях, одновременно подняв важные этические, юридические вопросы и проблемы безопасности. Правительства, корпорации и международные организации в настоящее время сталкиваются с двойной задачей – использовать потенциал искусственного интеллекта и одновременно снижать связанные с ним риски.

Ключевые тенденции развития искусственного интеллекта

Современное общество переживает технологическую революцию, движимую ИИ, большими данными, квантовыми вычислениями и биотехнологиями. Согласно Концепции внешней политики РФ, утвержденной Указом Президента РФ от 31.03.2023 № 229, этот сдвиг приводит к перестройке мировой экономики, при этом ИИ играет центральную роль в инновациях, производительности и национальной безопасности.

В Национальной стратегии развития искусственного интеллекта Российской Федерации на период до 2030 г., утвержденной указом Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024), отмечается, что ИИ является одной из важнейших доступных человечеству технологий, обладающей огромным потенциалом в таких областях, как повышение конкурентоспособности экономики; улучшение здравоохранения, образования и государственных услуг; укрепление национальной безопасности, повышение эффек-

тивности правоохранительных органов. Владение этой технологией позволит России добиться технологического суверенитета и занять на мировой арене лидирующие позиции в области научно-технологического развития.

Аналогичным образом Закон Европейского союза об ИИ и Национальная инициатива США в области ИИ отражают стратегическую важность ИИ для поддержания технологического суверенитета[1].

С момента запуска в 2022 г. ChatGPT, а затем GPT-4 в 2023 г., Claude (Anthropic) и Gemini от Google, сфера ИИ претерпела значительные изменения. Ключевые достижения включают: мультимодальный ИИ (обработка текста, изображений, аудио и видео), автономные агенты ИИ (способные взаимодействовать с системами реального мира), снижение затрат (повышение доступности ИИ для бизнеса). Новые языковые модели ИИ (LLM) позволяют значительно повысить базовую производительность труда человека при существенном повышении качества получаемых результатов. Но этот эффект достигается в значительной мере при тесном взаимодействии человека и технологий ИИ[2].

Новые языковые модели ИИ (LLM) позволяют значительно повысить базовую производительность труда человека при существенном повышении качества получаемых результатов. Но этот эффект достигается в значительной мере при тесном взаимодействии человека и технологий ИИ[3]. По прогнозам компании McKinsey Research, генеративный ИИ может ежегодно приносить мировой экономике от 2,6 до 4,4 трлн долл. за счет автоматизации до 70% повторяющихся задач и повышения производительности в отраслях, основанных на знаниях. Если другие технологии сохраняли осторожный инвестиционный профиль в течение 2024 г., то инвестиции в GAI выросли в 7 раз благодаря существенным достижениям в создании текстов, изображений и видео. Ожидается, что в

[1] Алферова Е.В., Скурко Е.В. Нормативные подходы Европейского союза и Соединенных Штатов Америки к правовому регулированию искусственного интеллекта: сравнительные аспекты // Актуальные проблемы Европы. – 2025. – № 2. – С. 43–57.

[2] Navigating the Jagged Technological Frontier: Field Experimental Evidence of the Effects of AI on Knowledge Worker Productivity and Quality / F. Dell'Acqua, E. McFowland, E. Mollick, [et all]. – 2023. – 58 p. – (Harvard Business School Working Paper). – URL: https://ssrn.com/abstract=4573321 (дата обращения: 12.04.2025).

[3] Ibid.

сфере технологий, медиа и телекоммуникаций (TMT) использование ИИ нового поколения принесет от 380 до 690 млрд долл. прибыли: от 60 до 100 млрд долл. в сфере телекоммуникаций, от 80 до 130 млрд долл. в сфере средств массовой информации и около 240 млрд в сфере инвестиций, 460 млрд долл. – в высокие технологии[1].

Кроме того, разработка программного обеспечения нового поколения включает в себя инструменты и технологии, которые позволяют создавать современные конвейеры развертывания кода и автоматизировать генерацию, тестирование, рефакторинг и перевод кода. Это может повысить качество приложений и процессов разработки. В 2022–2023 гг. наблюдался самый значительный рост инноваций в области прикладного ИИ и машинного обучения, чему способствовал растущий интерес к генеративному ИИ.

Возросшие возможности ИИ, как отмечают современные исследования[2], повысили интерес, инвестиции и инновации в технологиях ИИ, открывают новую эру квантовых технологий, робототехники и автоматизации, расширяют перспективы биоинженерии и космических технологий (включая спутниковые системы, ракеты-носители и технологии жизнеобеспечения, которые позволяют осуществлять инновационные космические операции и предоставлять космические услуги). Более зрелые современные технологии, например, облачные и периферийные вычисления (сервисы), расширенные возможности их подключения, способствуют внедрению других новых технологий. Большие базовые модели, обеспечивающие генеративный ИИ, такие как LLM, интегрируются в различные корпоративные программные инструменты, включая применение ориентированных на клиентов чат-ботов, создание рекламных кампаний, ускорение поиска лекарств и многое другое. Процесс масштабирования внедрения технологий ИИ требует соз-

[1] Beyond the hype: Capturing the Potential of AI and Gen AI in Tech, Media, and Telecom. – URL: https://www.mckinsey.com/industries/technology-media-and-telecommuni-cations/our-insights/beyond-the-hype-capturing-the-potential-of-ai-and-gen-ai-in-tmt (дата обращения: 12.04.2025).

[2] McKinsey Technology Trends Outlook 2024. – URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech (дата обращения: 20.03.2025); Глобальный индекс внедрения искусственного интеллекта / IBM Global AI Adoption Index // Enterprise Report. – URL: https://ai.gov.ru/knowledgebase/vnedrenie-ii/2024_globalynyy_indeks_vnedreniya_iskusstvennogo_intellekta_ibm_korporativnyy_otchet_ibm_global_ai_adoption_index_enterprise_report_ibm/?ysclid=maie5nshri406586085 (дата обращения: 12.04.2025).

дания благоприятной экосистемы, в которой решающее значение играют доверие и подготовленность пользователей, экономическая модель бизнеса, нормативно-правовая база и наличие подготовленных кадров. Эти экосистемные факторы варьируются в зависимости от географии (европейские страны, латиноамериканский регион, США, КНР, Индия и др.) и отрасли (банковско-финансовая деятельность, производственные сектора экономики, госуслуги и образование и др.). Технологии ИИ играют значительную роль в развитии использования возобновляемых источников энергии с охватом всей цепочки производства, хранения и распределения энергии. Эти технологии включают в себя возобновляемые источники энергии, такие как солнечная и ветровая энергия; экологически чистые источники энергии, ядерная энергия и водород, экологичные виды топлива и биоэнергия, а также решения для хранения и распределения энергии, такие как аккумуляторные системы длительного хранения и интеллектуальные сети.

США и Китай доминируют в разработке ИИ. Например, в так называемой «доктрине Шмидта» говорится о том, что укрепление глобального лидерства США в области технологий является императивом, как экономики, так и национальной безопасности государства. США находятся в долгосрочном стратегическом соревновании с Китаем, который, по оценкам Шмидта, стремится к технологическому лидерству за счет стратегических инвестиций в широкий спектр важнейших технологических областей, в том числе в рамках инициативы Made in China 2025[1]. Однако и другие страны, включая Великобританию, Индию, Саудовскую Аравию, Россию и страны – члены ЕС, вкладывают значительные средства, чтобы избежать зависимости. Таким образом, ключевыми тенденциями являются:

– китайский рынок ИИ вырастет с 371,6 млрд юаней (2022) до 1,573 трлн юаней (2027);

– доминирование США в базовых моделях (OpenAI, Anthropic, xAI), подкрепленное инвестициями Кремниевой долины;

– внимание России к суверенному ИИ.

[1] Ларина Е., Овчинский Б. Доктрина Шмидта – новые технологии и будущее национальной безопасности США // Завтра.ру. – 2021. – 26.02 – URL: https://zavtra.ru/blogs/doktrina_shmidta (дата обращения: 12.04. 2025); Киссинджер Г., Шмидт Э., Хаттенлокер Д. Искусственный разум и новая эра человечества. – Москва, 2025. – 200 р.

Вместе с тем внедрение ИИ сопряжено со множеством трудностей и возможностей, связанных с изменением корпоративной культуры, поиском значительного объема набора данных и обеспечением интерпретируемости результатов, предоставляемых моделями, а также нехваткой специалистов и подготовкой руководителей высшего звена. И все это – на фоне меняющегося нормативно-правового и этического ландшафта, который создает дополнительную неопределенность. Но разработка системы протоколов и защитных механизмов (например создание «моделей модерации» для проверки результатов на наличие различных рисков и обеспечения согласованности ответов для пользователей) станет важным шагом на пути к снижению новых рисков, связанных с ИИ. Еще одним ключевым фактором станет управление изменениями – вовлечение конечных пользователей в процесс разработки моделей ИИ. По оценкам McKinsey Research[1], ближайшие перспективы развития ИИ связаны:

– с созданием мультимодальных моделей ИИ, охватывающих текст, код, изображения и аудио, которые открывают новые возможности как для создания контента, так и для его понимания;

– взаимодействием ИИ нового поколения с окружающим миром, а модели ИИ нового поколения способны подключаться к данным и ИТ-системам для чтения и записи данных;

– управлением новым поколением моделей ИИ, которые позволят легче управлять, а конечные пользователи получат более согласованные результаты от вероятностных моделей благодаря новым функциям (например установка начального уровня);

– упрощением разработки генеративного ИИ: практически любому пользователю возможно создать чат-бота на базе gen-AI, используя интерфейсы с низким содержанием кода или без него (пример OpenAI, GPTs);

– созданием платформенных решений генеративного ИИ, т.е. торговых площадок GPT, где пользователи смогут создавать и публиковать свои новые приложения;

– кратным снижением затрат на генеративный ИИ (например GPT-4 API) для корпоративных клиентов.

[1] McKinsey Technology Trends Outlook 2024. – URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech (дата обращения: 10.04.2025).

Современное понимание искусственного интеллекта

Согласно Концепции технологического развития на период до 2030 г., утвержденной распоряжением Правительства РФ от 20.05.2023 № 1315-р, основным приоритетом технологической политики Российской Федерации является достижение технологического суверенитета Российского государства, под которым понимается наличие в стране (под национальным контролем) критических и сквозных технологий собственных линий разработки и условий производства продукции на их основе, обеспечивающих устойчивую возможность государства и общества достигать собственных национальных целей развития и реализовывать национальные интересы. ИИ относится к таким сквозным технологиям, поэтому разработкам в данной области должно уделяться приоритетное значение.

При этом, как это ни покажется странным, единого подхода к определению понятия ИИ в мире до сих пор не существует. Каждая страна или международная организация уделяют внимание отдельным аспектам. Так, Закон Евросоюза 2024 г. об ИИ использует понятие *системы ИИ*, под которой понимается «машинная система, предназначенная для работы с различными уровнями автономии, которая может проявлять адаптивность после развертывания и которая для достижения явных или неявных целей делает выводы на основе получаемых входных данных, как генерировать выходные данные, такие как прогнозы, контент, рекомендации или решения, которые могут повлиять на физическую или виртуальную окружающую среду». При этом особое внимание в нем уделено классификации ИИ по уровню риска (неприемлемый, высокий, ограниченный, минимальный).

Согласно подп. «а» п. 5 Национальной стратегии развития искусственного интеллекта в Российской Федерации, на период до 2030 г. *искусственный интеллект* – это «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе то, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений».

Согласно определению, принятому в Рекомендации ОЭСР по искусственному интеллекту (2019), *система искусственного интеллекта – это система на основе машин*, способная для заданного набора определенных человеком задач формулировать прогнозы, рекомендации или решения, влияющие на реальную или виртуальную среду.

Технологии ИИ, точнее нейросети, все шире используются в маркетинге, новостной журналистике, избирательных кампаниях, предотвращении и расследовании преступлений, в медицинской и судебной практиках, в биржевых операциях с ценными бумагами и т.д. В сфере творческой деятельности часто используют нейросети в написании литературных опусов, в сочинении музыкальных произведений и в подготовке книжных иллюстраций. Но, наверное, самые широкие горизонты открываются в сфере разведки – коммерческой, финансовой, военной, научно-технической, политической и любой другой. ИИ позволяет упростить сбор и обработку разведывательной информации, и то же время «нейросети позволяют вывести производство и распространение дезинформации на качественно новый, более высокий уровень, фактически стирая грань между реальным и воображаемым, между фактами и мнениями, между правдой и ложью» [1].

С другой стороны, злонамеренное использование ИИ, возможностей нейросетей становится исключительно актуальной проблемой – в частности, использование нейросетей в информационно-психологической сфере. Поддержание безопасности в информационно-психологической сфере, а также социально-политической стабильности в обществе формулируется в качестве ключевого компонента национальной безопасности государства. Практика показывает, что противодействие угрозам злонамеренного использования технологий ИИ в самых разнообразных сферах, включая сферу информационно-психологической безопасности (угрозы, связанные с автоматизацией производства, кибербуллинг, использование технологий *deep fake* в политическом противоборстве и т.д.), служит объектом особого внимания в национальной политике многих государств.

[1] Кортунов А. На пути к искусственному интеллекту – пришествие демона Лапласа // Российский совет по международным делам. – 2023. – 31 окт. – URL: https://russiancouncil.ru/analytics-and-comments/analytics/na-puti-k-iskusstvennomu-intellektu-prishestvie-demona-laplasa/ (дата обращения 12.04.2025).

К примеру, политика правительства КНР свидетельствует о необходимости принятия мер по противодействию рискам злонамеренного использования ИИ, включающих разработку национальной и международной нормативно-правовой регуляторной среды для ИИ, создание системы этики информационной грамотности населения, а также осуществление общественного мониторинга путем налаживания системы социального доверия. Расширение практик злонамеренного использования ИИ и когнитивная война в контексте современного геополитического соперничества великих держав создает, по мнению экспертов, опасность поляризации между многосторонними альянсами, такими как БРИКС, ШОС, ЕС, НАТО[1].

В сентябре 2023 г. в г. Хиросима на саммите большой семерки были приняты Руководящие принципы по развитию ИИ (Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI system), которые призваны обеспечить этическую основу для организаций, разрабатывающих передовые системы искусственного интеллекта, уделяя особое внимание безопасности, прозрачности и подотчетности. Они поощряют ответственное развитие искусственного интеллекта путем устранения рисков, обеспечения контроля со стороны персонала и содействия международному сотрудничеству. В Руководящих принципах также подчеркивается важность инклюзивности, справедливости и приведения достижений в области искусственного интеллекта в соответствие с общественными выгодами и этическими стандартами.

В ноябре 2023 г. в Блетчли (Великобритания) 28 стран-участниц (Россия в саммите участие не принимала), а также компании-лидеры IT-отрасли подписали Декларацию по вопросам безопасности ИИ (The Bletchley Declaration on AI safety), в которой признаются преобразующий потенциал ИИ и его огромные возможности для продвижения глобального процветания, инноваций и общественного блага. Вместе с тем подписанты декларации обращают внимание на значительные риски, связанные с ИИ, осо-

[1] Михалевич Е. Проблемы злонамеренного использования ИИ в контексте международной информационно-психологической безопасности БРИКС // Российский совет по международным делам. – 2023. – 31 окт. – URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/problemy-zlonamerennogo-ispolzovaniya-ii-v-kontekste-mezhdunarodnoy-informatsionno-psikhologicheskoy/?sphrase_id=170678531 (дата обращения 12.04. 2025).

бенно с его передовыми системами («Frontier AI»), которые могут иметь серьезные последствия, если не управлять ими ответственно. Поэтому подчеркивается настоятельная необходимость международного сотрудничества для обеспечения безопасности ИИ с участием правительств, представителей промышленности, научных кругов и гражданского общества. Документ призывает к разработке единых подходов к определению рисков, связанных с ИИ, включая потенциальное неправильное его использование, потерю контроля и непреднамеренные вредные последствия. Участники обязуются способствовать прозрачности, подотчетности и созданию надежных систем управления для смягчения угроз, связанных с ИИ, и развитию ИИ таким образом, чтобы оно соответствовало правам человека и этическим принципам. В Декларации также подчеркивается важность научных исследований, а кроме того государственно-частного партнерства для обеспечения широкого распространения преимуществ ИИ при минимизации вреда.

Таким образом, участники саммита полагают, что Блетчлийская декларация закладывает основу постоянного глобального сотрудничества для продвижения единых политики и стандартов безопасности ИИ.

17 мая 2024 г. Комитетом министров Совета Европы принята Рамочная конвенция Совета Европы об искусственном интеллекте и правах человека, демократии и верховенстве закона (СДСЕ № 225) (далее – Рамочная конвенция), в разработке которой участвовали также страны, не входящие в Совет Европы. Рамочная конвенция открыта для присоединения не только государств – членов Совета Европы, но и других стран. На данный момент ее подписали Андорра, Грузия, Исландия, Норвегия, Молдова, Сан-Марино, Великобритания, Израиль, США и ЕС[1]. Цель Рамочной конвенции – обеспечение деятельности в рамках жизненного цикла систем ИИ в полном соответствии правам человека, демократии и верховенства закона и направлена на содействие эффективному осуществлению установленных национальным законодательством и международными договорами прав человека. Данная Конвенция не охватывает все аспекты деятельности систем ИИ или технологий

[1] Карцхия А.А. Правовые аспекты публичного и частноправового регулирования в сфере обеспечения информационной безопасности // Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности: сб. докл. участников XVIII Международного форума. – Москва, 2024. – С. 88–92.

ИИ как таковых, а определяет меры регулирования систем ИИ, которые потенциально могут нарушать права человека, демократию и верховенство закона, включая все этапы деятельности систем ИИ для противодействия рискам его применения (как настоящим, так и будущим) с учетом быстрого и зачастую непредсказуемого развития технологий. Страны – участники Рамочной конвенции вправе продолжать использовать существующее правовое регулирование ИИ, упростить, уточнить или усовершенствовать его, способствовать улучшению его правоприменения и повышению доступности существующих средств правовой защиты и мер регулирования. Такого рода меры могут включать: новое законодательство, политику регулирования, основанную на правилах, принципах или целях, механизмы и стандарты их соблюдения, а также административные и иные юридические меры, рекомендации, толкования, циркуляры, внутренние механизмы и процессы или судебную практику. Рамочная конвенция требует от ее участников принятия законодательных, административных или иных мер для предотвращения нарушения прав человека, стабильности и целостности демократических процессов, обеспечения верховенства закона со стороны систем искусственного интеллекта и предусматривает поэтапный и дифференцированный подход, т.е. – принимаемые меры должны соответствовать серьезности и вероятности негативных последствий, связанных с искусственным интеллектом.

Важную роль в регулировании ИИ имеют документы ООН. Так, Глобальный цифровой договор, как отмечают эксперты[1], продолжает практику глобальных договоров ООН и представляет собой набор общих принципов, призванных регулировать деятельность различных акторов мировой политики. Глобальный цифровой договор ООН – международная инициатива, направленная на содействие инклюзивному и устойчивому цифровому сотрудничеству для решения глобальных проблем, таких как подключение к Интернету, управление данными и соблюдение прав

[1] Кортунов А. Саммит будущего ООН: от наброска к картинке / Российский совет по международным делам. – 2024. – 26 сент. – URL: https://russiancouncil.ru/en/analytics-and-comments/analytics/un-summit-of-the-future-from-a-sketch-to-a-picture (дата обращения: 12.04. 2025); Зиновьева Е. Что не так с Глобальным цифровым договором? / Российский совет по международным делам. – 2024. – 12 нояб. – URL: https://russiancouncil.ru/en/ analytics-and-comments/analytics/what-s-wrong-with-the-global-digital-compact/ (дата обращения: 12.04.2025).

человека в Интернете. Его целью является установление общих принципов для открытого, свободного и безопасного цифрового будущего, а также сокращения цифрового разрыва и обеспечения равного доступа к технологиям. Однако этот документ имеет существенные недостатки. Основное внимание в нем уделено саморегулированию частных компаний и продвижению западных либеральных ценностей, что размывает принципы национального суверенитета.

Феномен киберпреступности в условиях применения искусственного интеллекта

Расширение внедрения ИИ и других цифровых технологий породило новый социальный феномен – *киберпреступность*. Действуя анонимно через цифровые сети, преступники могут удаленно повреждать электронные данные или системы ИКТ, красть данные и финансовые активы или заниматься сексуальной эксплуатацией детей, нанося огромный финансовый ущерб и причиняя серьезный личный вред отдельным лицам, предприятиям и правительствам по всему миру. В то время как преступники действуют без юридических или географических ограничений, правоохранительные органы должны уважать границы юрисдикции. Это создает значительные препятствия: электронные доказательства часто разбросаны по нескольким странам и могут исчезнуть до завершения процесса оказания правовой помощи, а различия в национальных законах еще больше усложняют расследование и судебное преследование. Таким образом, киберпреступность рассматривается как одна из наиболее серьезных глобальных проблем нашего времени. Первым глобальным договором, который установил стандарты криминализации правонарушений, методы расследования и трансграничное сотрудничество, стала Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.). Однако развитие, как технологий, так и форм преступности в Сети требует разработки новой всеобъемлющей конвенции, чтобы устранить существующие пробелы и охватить большее число стран, особенно тех, которые не подпадают под действие Будапештской конвенции. С такой инициативой выступила Россия. Одобренная Генеральной Ассамблеей ООН 24 декабря 2024 г. Конвенция ООН против киберпреступности призвана стать основой для налаживания сотрудничества правоохранительных органов разных стран в противодействии использо-

ванию ИКТ в преступных целях. ИКТ-технологии произвели революцию в нашем мире, предоставив людям беспрецедентные возможности для общения, инноваций и коммерции. Однако повсеместное распространение систем ИКТ, таких как компьютеры и смартфоны, в равной степени открывает перед преступниками новые возможности для использования технологий в преступных целях. Конвенция ООН состоит из Преамбулы и девяти глав. Сферой ее применения является предупреждение киберпреступлений, возвращение доходов от них и укрепление международного сотрудничества, особенно в трансграничном обмене электронными доказательствами – как преступлений, связанных с Конвенцией, так и других серьезных преступлений. Особое внимание уделено необходимости уважения прав человека и основных свобод, таких как свобода выражения мнений, совести, убеждений, религии или вероисповедания, мирных собраний и ассоциаций, а также уважения суверенного равенства и территориальной целостности всех государств.

Криминализация наиболее распространенных форм киберпреступности имеет важное значение для усилий по предотвращению этой растущей угрозы и борьбе с ней, а также для устранения ее повсеместного воздействия на общество, поэтому Конвенция закрепляет обязанность государств-участников создавать всеобъемлющую систему борьбы с такими преступлениями, в том числе посредством их криминализации. Дается примерный перечень киберпреступлений. Установлены четкие и гибкие правила, препятствующие преступникам использовать пробелы в юрисдикции, чтобы избежать наказания. При этом Конвенция разграничивает правовые сферы, которые могут регулироваться государствами-участниками. Кроме того, устанавливаются глобальные рамки, которые позволяют сторонам Конвенции оказывать друг другу помощь в расследованиях, судебных преследованиях, возвращении активов и судебных разбирательствах через границы.

Заключение

Таким образом, распространение генеративного ИИ увеличивает риск нарушения прав человека, что обусловлено способностью цифровых технологий влиять на глобальную политику и экономику. Появление генеративного ИИ представляет собой «парадокс прогресса»: с одной стороны, это изобретение может решить сложные проблемы и вызвать революцию в образе жизни

людей, а с другой – усиливает серьезные риски, которые могут ущемлять достоинство и права человека. Необходимо, чтобы права человека были основой развития всего жизненного цикла технологий искусственного интеллекта[1]. Мировое сообщество должно сотрудничать в разработке международных стандартов применения ИИ, в том числе этических основ его функционирования и предотвращения злоупотреблений. Поскольку ИИ продолжает развиваться, выбор, сделанный сегодня, определит, станет ли он движущей силой национального и международного процветания или источником нестабильности.

[1] Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General. – URL: https://documents.un.org/doc/undoc/gen/g21/249/21/pdf/g2124921.pdf (дата обращения: 12.04.2025).

УДК 34.096 DOI: 10.31249/iajpravo/2025.03.04

ИСАКОВ В.Б.[1] **ПЕРСПЕКТИВЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВЕ (Обзор)**

Аннотация. В обзоре раскрываются понятие, отличительные признаки и виды искусственного интеллекта. Показаны возможные сферы применения искусственного интеллекта в социальном управлении, в законотворчестве и правоприменении. Обсуждаются опасности и риски, связанные с его внедрением. Высказано мнение о правовом статусе искусственного интеллекта с точки зрения действующего российского законодательства и методологической несостоятельности попыток «очеловечить» робота, применить к нему юридические категории и подходы, выработанные в отношении человека.

Ключевые слова: искусственный интеллект; сильный искусственный интеллект; слабый искусственный интеллект; сферы применения искусственного интеллекта; опасности и риски искусственного интеллекта; правовой статус искусственного интеллекта.

ISAKOV V.B. Prospects of Artificial Intelligence in Law (Review)

Abstract. The review reveals the concept, distinctive features and types of artificial intelligence. The possible fields of application of artificial intelligence in social management, lawmaking and law enforcement are shown. The dangers and risks associated with its implementation are discussed. An opinion is expressed on the legal status of artificial intelligence from the point of view of current Russian legislation and the methodological failure of attempts to “humanize” a robot, apply to it legal categories and approaches developed in relation to humans.

[1] © *Исаков Владимир Борисович*, доктор юридических наук, профессор, Национальный исследовательский университет «Высшая школа экономики».

Keywords: artificial intelligence; strong AI; weak AI; areas of application of AI; dangers and risks of AI; legal status of AI.

Для цитирования: Исаков В.Б. Перспективы искусственного интеллекта в праве (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2025. – № 3. – С. 47–62. – DOI: 10.31249/iajpravo/2025.03.04

Введение

В научной литературе искусственному интеллекту дается множество разных определений. Под *искусственным интеллектом* понимают:

1) качество (свойство) технических устройств, которое может быть реализовано на различной элементной базе;

2) класс машин, способных осуществлять функции, которые ранее были доступны исключительно человеку (компьютеры, нейросети, роботы и др.);

3) информационные процессы, комплексы информационных технологий, моделирующих интеллектуальную деятельность человека;

4) междисциплинарное направление науки, изучающее системы представления знаний машиной, и др. [7; 10].

Базовое определение ИИ дано в подп. «а» п. 5 Национальной стратегии развития искусственного интеллекта до 2030 г., утвержденной Указом Президента РФ от 10.10.2019 (ред. от 15.02.2024). Оно принято нами за основу. В зависимости от контекста обсуждаемой проблемы в статье могут быть использованы и иные подходы.

Системы, наделенные ИИ, обладают рядом признаков, отличающих его от других устройств, созданных человеком:

– способность к решению задач высокой сложности, которые раньше считались исключительной прерогативой человека;

– относительная автономность;

– нелинейность поведения;

– потенциал к творчеству, эвристике;

– восприимчивость к самообучению;

– адаптивность;

– интерактивность (способность к коммуникации с человеком) [8, с. 91–109].

Классификация систем искусственного интеллекта

Классификации систем ИИ чрезвычайно разнообразны, и по причине стремительного развития предмета они окончательно не устоялись. Рассмотрим некоторые из них, представляющие наибольший интерес в рамках обсуждаемой темы (см. рис. *1*).

Рисунок 1. Некоторые классификации систем искусственного интеллекта

Исходя из уровня развитости, ИИ принято разграничивать на слабый и сильный [13].

Слабый ИИ (ANI), называемый иногда «узким» или «прикладным», – нацелен на осуществление отдельных человеческих функций и, соответственно, способен решать ограниченный круг задач. К системам этого типа относят: поисковики и редакторы документов; переводчики с иностранных языков; игровые компьютеры; распознаватели образов, текста, речи. К этой же категории причисляют также: чат-боты; компьютеры, пишущие картины, музыку, сочиняющие стихи, научные и художественные тексты; голосовые помощники; автопилоты и аналогичные системы управления транспортом; системы управленческого консультирования; системы медицинской диагностики и др.

Слово «слабый» применительно к ИИ не должно дезориентировать и восприниматься в уничижительном смысле. Большинство из названных систем вполне современны, успешно развиваются, активно внедряются в практику, наращивают свой позитивный функционал.

Сильный ИИ (AGI) – создается для решения широкого спектра задач, сопоставим по своим функциям с человеческим интеллектом и в перспективе может его превзойти. Сферами применения сильного ИИ являются разработка и принятие стратегических управленческих решений; выравнивание баланса искусственного и естественного в среде обитания человека; расшифровка генома человека, выявление и устранение причин неизлечимых болезней; изучение высших проявлений сознания и самосознания; научное и художественное творчество; создание новых поколений интеллектуальных машин. Совершенствование сильного ИИ связано не только с громадными материальными и финансовыми затратами, но и разнообразными морально-этическими и правовыми ограничениями [там же].

Основные направления развития искусственного интеллекта

Коротко охарактеризуем ключевые направления развития ИИ. Заметим, что в их описании отсутствует единство наименования и понимания. И тем не менее, к их числу исследователи относят [5, с. 40–103; 15, с. 64–186]:

1) *извлечение, представление и использование знаний*. В том числе – обработка огромных массивов накопленной информации, машинное обучение, компьютерное зрение, создание экспертных систем различного назначения, в том числе в области юриспруденции;

2) *игры и творчество.* В этой сфере ИИ проявил себя наиболее ярко и убедительно. Это шахматные компьютеры, устройства для игры в го и в покер и др. Искусственный интеллект постепенно осваивает сферу художественного творчества – пишет стихи, художественную прозу, рисует картины, сочиняет музыку;

3) *анализ и обработка языка.* Все человеческие знания зашифрованы в знаках языка. Поэтому ИИ привлекается для создания пользовательских компьютерных интерфейсов, энциклопедий и справочников, машинных переводов, реферирования и аннотирования источников, извлечения фактов из массивов больших данных;

4) *обучение и самообразование.* Это одна из приоритетных и быстро растущих сфер применения. Искусственный интеллект используется для оптимизации образовательных систем и учебных программ, формирования сплоченных творческих команд, диагностики и формирования коммуникативных навыков, разработки учебных заданий и оценки полученных знаний;

5) *разработку систем ИИ нового поколения.* Разработчики уже подошли к рубежу, когда не всегда и не полностью понимают логику действий ИИ. Естественно, что с этим багажом трудно двигаться дальше, к созданию систем ИИ новых поколений. Поэтому источником новых идей и разработок все чаще становится сам искусственный интеллект.

На рис. 1 (в третьей колонке схемы) перечислены отдельные виды ИИ, привлекающие наибольший интерес исследователей и практических потребителей: это большие языковые модели; генеративный ИИ; экспертные системы; интеллектуальные роботы различного назначения. По каждому из этих направлений можно найти множество комментариев в приведенных выше источниках.

Сферы применения искусственного интеллекта

Очевидно, что ИИ даже в нынешних, пока не самых совершенных формах, может иметь множество сфер практического применения.

Во-первых, ИИ представляет собой эффективный инструмент поиска информации. Сегодня человечеству доступны гигантские, просто невообразимые объемы информации. Но в ней трудно найти именно то, что требуется здесь и сейчас, что необходимо для решения вашей проблемы. Похоже, что ИИ способен справиться с этой задачей. Он опирается на базы данных, содержащие миллионы единиц информации, и использует оптимальные на текущий момент алгоритмы поиска.

Правда, как показывает практика, ИИ не всегда удовлетворительно справляется с поставленной задачей: отвечает на запросы неточно и даже «придумывает» целые списки несуществующих авторов и источников. Оправдывается, извиняется, но затем продолжает в том же духе. Проблема, по-видимому, в изначальных формулировках запросов на естественном языке, который конфликтует с алгоритмами информационных технологий. Тем не менее можно предположить, что уже в ближайшем будущем станет

невозможным написать научную статью или опубликовать монографию, не проверив и не уточнив их содержания с помощью ИИ.

Во-вторых, ИИ способен не только искать информацию, но и создавать новое знание, т.е. выявлять новые связи и отношения, находить закономерности, делать открытия и не только использовать, но и развивать существующее знание. Творческие возможности ИИ пока недостаточно изучены. Но очевидно, что он способен выявлять новые артефакты, которые оказались вне внимания человека, а стало быть, и вне его практической деятельности. Исследователи отмечают, что, например, на основе статистики и биографических данных человека нейросеть научилась рассчитывать примерную продолжительность его жизни [2]. Достоинством ИИ можно считать то, что он не просто сообщает о своих научных открытиях, но и немедленно включает выявленные связи и закономерности в оборот, начинает учитывать их в построении моделей и проведении расчетов.

В-третьих, ИИ может стать для человека отличным помощником-ассистентом. В принципе, он уже умеет это делать. Но есть существенные ограничения. В случае принятия решений, воздействующих непосредственно на личность, предполагающих оценку фактов биографии, целей, мотивов, эмоционального состояния человека, – в медицине, педагогике, юриспруденции – искусственный интеллект обязательно должен находиться под контролем человека. Окончательное решение в этих сферах должен принимать человек и нести за него всю полноту ответственности.

В-четвертых, ИИ может освободить человека от трудоемких и непродуктивных видов интеллектуальной деятельности, таких как составление оглавлений, указателей, индексов, а также резюме, аннотаций, отчетов и справок.

На наш взгляд, внедрение ИИ предполагает полный пересмотр всех звеньев профессионально-предметной деятельности, начиная с постановки целей и задач, организации работы, применяемых технологий и, конечно, процессов управления. При этом нередко выясняется, что одна часть трудового коллектива приветствует изменения и инновации, другая – настроена на сохранение существующего порядка. Разумеется, задачи подобного масштаба и сложности не решаются одномоментно, в один присест. Они требуют продуманной стратегии, затрат времени, сил и средств. Но другого пути, видимо, нет. Практика показала, что трансляция в сферу ИИ существующих форм бюрократической отчетности не

только не влечет повышения эффективности управления, но и может выступить причиной ее снижения.

В-пятых, на основе ИИ могут создаваться системы управления с высокой степенью автономности, действующие без прямого участия человека. В некоторых видах производства, в сфере банковских расчетов такие системы уже работают. Обнадеживающая информация приходит из сферы транспорта, где успешно эксплуатируются беспилотные транспортные средства: поезда метро в некоторых странах уже ходят без машиниста. Правда, пределы автономии таких систем не безграничны. Обязательно предусматривается уровень управления, на котором в случае сбоя или отказа автоматики происходит подключение человека.

В сфере государственного управления системы с искусственным интеллектом могут взять на себя не только относительно простые учетно-регистрационные функции, но и более сложные задачи – начисление налогов, пенсий, платежей, штрафов, контроль за их своевременной уплатой и т.д. Они могут полностью освободить граждан от утомительного ожидания в приемных и хождения по кабинетам. Подобные системы могут быть созданы также в сфере контроля за состоянием окружающей среды, мониторинга погоды, здоровья человека. При этом они могут не только наблюдать и регистрировать, но и активно реагировать доступными средствами на опасные отклонения.

На наш взгляд, использование ИИ в сфере государственного управления допускает и даже предполагает различные эксперименты. Однако в любом случае такие эксперименты должны проходить строгую и беспристрастную научную и общественную экспертизу, официально законодательно оформляться, находиться в зоне общественного контроля и прокурорского надзора. По итогам проведенного эксперимента должен представляться и утверждаться отчет, на основе которого – приниматься окончательное решение о прекращении эксперимента либо о дальнейшем развитии и масштабировании положительно зарекомендовавших себя инновационных управленческих решений. В противном случае может оказаться реальной угроза формирования в стране тесно перевязанного компьютерными технологиями, предельно заформализованного и забюрократизированного «технотронного общества», о котором с тревогой предупреждают ученые и фантасты.

Опасности и риски искусственного интеллекта

Как это нередко случалось в прошлом, каждый очередной этап научно-технической революции влечет за собой не только достижения и преимущества, но и новые угрозы и риски. Современный этап научно-технического прогресса не является исключением. Какие угрозы и риски несет широкое распространение устройств, наделенных искусственным интеллектом, отличительной особенностью которых является способность в определенных рамках принимать решения и действовать автономно, независимо от человека? Рассмотрим их «в обратном порядке», от относительно легких – к более сложным и фундаментальным.

1. *Вытеснение человека из социально значимых сфер деятельности, перехват рабочих мест.* Совершенно очевидно, что наделенные элементами интеллекта роботы – прямые конкуренты человека в сфере трудовой деятельности. Они неприхотливы к условиям труда, не требуют повышения заработной платы и перерывов на обед, не объединяются в профсоюзы, не устраивают забастовок. Уже сегодня стоимость роботов и их функциональные свойства позволяют предпринимателям заменять ими «живую рабочую силу». С точки зрения совокупных общественных затрат замена живого человеческого труда на машинный должна рассматриваться как благо, однако не все так просто. Проблема заключается в том, что современное государство не планирует и не собирается обеспечивать достойные условия жизни тем, кто в результате подобной замены вытесняется из сферы производства.

2. *Снижение уровня образования и квалификации работников, влекущее деградацию человеческого интеллекта.* Замена роботами человека в интеллектуально насыщенных сферах деятельности влечет за собой двоякий эффект. С одной стороны, формируется узкая группа ученых, аналитиков, разработчиков, инженеров, создающих новые и новые, все более совершенные средства автоматизации производства и управления. От внедрения роботов в материальном и интеллектуальном плане они только выигрывают. Однако параллельно растет слой проигравших, на долю которых остаются простейшие виды работ, замещение которых роботами себя экономически не оправдывает – подноска, обслуживание, профилактика, уборка помещений и т.д. Эти виды работ не требуют высокой квалификации, что приводит к деградации образования, интеллекта, человеческой личности в целом.

3. *Развращение человечества праздным и бессмысленным существованием, ведущим к его физической и культурной деградации.* Успехи компьютеризации и роботизации постепенно превращают человека в «технологического рантье», ведущего праздный образ жизни, озабоченного тем, куда деть свободное время. Именно на их, потребителей материальных и духовных благ, скучающих бездельников, начинает ориентироваться и так называемая «массовая культура».

4. *Принятие роботами ошибочных решений – технических, экономических, финансовых, экологических, медицинских и т.д.* Никто не гарантирован от ошибок, в том числе и роботы. Несмотря на прогнозируемое упрощение социальных отношений, экономическая и политическая жизнь общества останется достаточно сложной, сохранятся экономическая и финансовая нестабильность. Обострятся экологические проблемы. Не исчезнут эпидемии и иные виды заболеваний. Останутся сложные научно-технические проблемы. Во всех этих сферах возможны не только правильные решения, но тяжелые по своим последствиям ошибки. Интеллектуальный робот, как и человек, может инициировать ошибочное решение, вызываемое сложностью решаемой проблемы.

5. *Опасные сбои промышленных роботов и компьютеризированных управляющих систем (автопилоты, управляющие системы сетей, предприятий, электростанций и т.д.).* Как и любая техническая система, роботы подвержены случайным сбоям. Чем более сложны системы производства и управления, чем больше в них автоматических, программируемых, действующих без вмешательства человека элементов, тем больший урон может быть нанесен случайным сбоем. Это видно хотя бы по той болезненной реакции, которую вызывает даже кратковременные сбои в банковском обслуживании населения: жизнь замирает, рушатся сделки, люди опаздывают на поезда и самолеты и т.д. Зависимость человека от все более усложняющихся компьютеризированных систем в перспективе будет только расти.

6. *Умышленное использование роботов с целью причинения вреда.* В российской и зарубежной практике появились примеры, когда компьютеризированные системы использовались как орудие для умышленного причинения вреда. Например, система мониторинга за состоянием человека, находящегося в реанимации, была использована для замедления ритма сердечной деятельности, фактически – для дистанционного технологического убийства человека. Дистанционное изменение программы работы высокоскорост-

ных центрифуг в Иране привело к их взрыву и т.д. Использование ИИ как орудия преступлений – новый элемент в правоохранительной деятельности, который еще предстоит изучить, осмыслить и адекватно отразить в законодательстве и правоприменительной практике [3, с. 24–28; 4, с. 96–105; 6, с. 104–112; 9, с. 10–53].

Правовой статус искусственного интеллекта

В силу названных выше причин отнюдь не случайно, что в научных публикациях все чаще возникает вопрос о правовом статусе систем, наделенных искусственным интеллектом. Что они собой представляют: предметы и объекты материального мира, функционирующие в системе общественных отношений, или, может быть, находящуюся в процессе становления новую категорию субъектов права?

В научной литературе обсуждается возможность признания за роботами определенной правосубъектности, предоставлении им гражданства [14]. Сообщалось, в частности, о предоставлении гражданства Саудовской Аравии роботу «София» [16]. Однако изучение процедуры предоставления гражданства Саудовской Аравии, предусмотренной Законом о гражданстве Саудовской Аравии[1], заставляет в этом усомниться. Решение о предоставлении гражданства в этой стране принимает министр юстиции при соблюдении целого ряда условий и ограничений, и вся процедура носит достаточно длительный характер. Из публикаций не видно, что все юридические условия предоставления гражданства были выполнены. Также нельзя не обратить внимания, что публичные сообщения о предоставлении гражданства роботу делались на конгрессно-выставочных мероприятиях и носили характер сенсации. Сказанное позволяет предположить, что речь идет, скорее всего, об информационном фейке, преднамеренно запущенном в рекламных целях.

Дело не только в том, что правовые условия предоставления гражданства роботу не были выполнены до конца и не могли быть выполнены. С точки зрения действующего сегодня законодательства это действие представляется лишенным какого-либо смысла. Предоставление статуса гражданина предполагает приобретение

[1] См.: Закон о гражданстве Саудовской Аравии. – URL: https://translated.turbopages.org/proxy_u/en-ru.ru.f419e744-680a2ed2-2c1b86f8-74722d776562/https/en.wikipedia.org/wiki/Saudi_Arabian_nationality_law (дата обращения: 24.04.2025).

субъектом комплекса прав и обязанностей, которые данный субъект должен исполнять. Может ли робот, даже наделенный искусственным интеллектом, пользоваться политическими правами, служить в армии, платить налоги, заключать сделки и отвечать по ним? Ответ очевиден.

Конечно, для рекламного пиар-эффекта можно допустить робота к избирательной урне, показать под блицы фотокамер, как он опускает туда бюллетень, но задумаемся о смысле этого действа. Голосуя за или против кандидата, мы тем самым поддерживаем или отвергаем программу его политической деятельности. Другими словами, вместе с голосованием за или против кандидата мы голосуем за тот или иной вариант своего будущего. При чем тут робот? Какое отношение он имеет к выбору моего будущего?

С точки зрения действующего права три элемента правового статуса – права, обязанности, ответственность – находятся в единстве и неразрывной взаимосвязи. Права – это потенциальная социальная возможность, «частичка свободы», которую государство гарантирует субъекту для достижения его интересов и целей. Какие собственные цели и интересы могут быть у робота?

Обязанности – мера должного поведения субъекта по отношению к другому субъекту, государству, обществу. Способен ли робот сознавать меру должного поведения и руководствоваться ею? И вообще, что такое «мера должного поведения» для робота? Кому и что он «должен»?

Наконец, злоупотребление субъекта своими правами и неисполнение обязанностей влечет применение к нему ответственности – мер лишения личного, имущественного или организационного порядка. Какие меры ответственности могут быть применены к роботу, нарушившему свои обязанности? Имущества и денег у него нет, понизить в должности его невозможно. Вопрос об утрате доверия, чести и достоинства, по-видимому, тоже не стоит. Отключение у робота отдельных функций, ограничение круга его деятельности в качестве меры наказания – явная нелепость. Остается только «высшая мера наказания» – отключение робота от электрического питания и разбор его на составные части. Получается, что робот неуязвим перед возможными правовыми мерами ответственности за нарушение обязанностей и в целом за свое «ненадлежащее поведение».

Очевидно, что попытки «очеловечить» робота, применить к нему юридические категории и подходы, выработанные в отношении человека, методологически несостоятельны и заводят пробле-

му в тупик. Человеческая позиция в системе социальных и правовых отношений уникальна и может быть занята только человеком – существом, наделенным сознанием, волей, автономными интересами и целями, социальными возможностями, позволяющими отвечать за свои действия. Другое дело, что люди, вполне юридически вменяемые, наделенные здоровым человеческим интеллектом, используют свои способности по-разному – и в каких-то случаях значительно хуже роботов.

На ситуацию можно взглянуть с исторической точки зрения. Генетически роботы выросли из системы машин – от палки-копалки до современного суперкомпьютера, – помогающих человеку, облегчающих, ускоряющих, делающих более эффективной его физическую и умственную деятельность. Можно сказать, что они представляют собой качественно новую ступень эволюции инструментов человеческой деятельности: машины, получившие определенную степень автономии, независимости от человека. Но генетически, по своему происхождению, они остаются *инструментами*, т.е. объектами, а не субъектами правовых отношений. Любой робот имеет производителя, т.е. субъекта, который его изготовил и наделил определенными инструментальными функциями, и владельца – субъекта, который использует робот для достижения своих целей и интересов. От человека робота отличает отсутствие сознания, свободы воли, автономных целей и интересов, т.е. отсутствие необходимых основ «социальной субъектности».

Свободу воли при этом не следует смешивать со свободой выбора. Свобода выбора, точнее, элемент выбора, есть у любого программируемого автоматического устройства, включая автоматы для продажи газированной воды. Этот автомат может отказать вам в обслуживании, если ваша монета покажется ему дефектной. Тем более свобода выбора есть у автоматов, играющих на бирже, покупающих и продающих ценные бумаги, проектирующих изделия, заключающих сделки и т.д. Но вот свободы воли у них нет. Подобные устройства представляют собой сверхсложные автоматические устройства, преследующие интересы и цели своего владельца, и выполняющие, в конечном счете, *его волю*. Этот же владелец будет отвечать, если в результате ошибки или сбоя искусственный интеллект причинит кому-то вред.

Можно ли создать интеллектуального робота, который будет обладать самосознанием, волей, автономными интересами и целями? Ответ на этот вопрос зависит от того, что мы понимаем под *сознанием* [12]. Не уходя вглубь этого крайне сложного вопроса,

полагаем, что возможно создание устройств, которые будут обладать техническими аналогами высших человеческих функций – рефлексии, критики и самокритики, креатива, юмора, творческими способностями и т.д. Машины догоняют и обгоняют человека практически во всех сферах; очевидно, что догонят и обойдут и в этих.

В настоящее время в общественных отношениях интеллектуальные роботы выступают исключительно как объекты и предметы – инструменты человеческой деятельности, предметы сделок, объекты научных исследований и экспериментов и т.д. Это предопределяет их место в системе правоотношений в качестве объектов. Можно ли в принципе создать интеллектуального робота, который будет способен претендовать на роль субъекта права? Полагаю, что для этого нет непреодолимых технических препятствий. Другой вопрос, для чего это нужно, кроме как для целей научного, «пробирочного» эксперимента?

Интеллектуальные роботы могут стать автономными и саморазвивающимися субъектами только в том случае, если человек по каким-то неведомым причинам посчитает нужным «отпустить их на волю», освободить от своего контроля, или это произойдет по недосмотру, случайно. Реальные последствия такого события могут выразиться не только в изменении социального и правового статуса интеллектуальных машин, но и повлечь за собой резкое усиление тех глобальных угроз и рисков, которые рассматривались нами выше.

Использование искусственного интеллекта в законотворчестве и правоприменении

В сфере права ИИ может осуществлять широкий спектр услуг, рассмотренных в предыдущих пунктах, а также участвовать в законотворчестве, правоприменении, правовом консультировании, контроле за состоянием законности, уровня правовой культуры, предупреждать о появлении или нарастании в обществе или в регионе негативных социальных тенденций и т.д. [1; 17].

Уже сегодня ИИ способен разрабатывать проекты правовых документов и следить за их движением. В перспективе это приведет к тому, что огромная армия чиновников-делопроизводителей среднего уровня квалификации окажется невостребованной и может потерять работу. Очевидная тенденция заключается в том, что бумага и бумажный документооборот будут постепенно уходить

из сферы управления, замещаясь безлюдными технологиями, автоматическим обменом информацией и автоматизированным принятием решений.

Некоторые виды правовых отношений, на наш взгляд, не могут быть компьютеризированы и должны оставаться в компетенции человека, принимающего окончательное решение. Трудно себе представить, например, что решения о разводе, оставлении детей у родителя, разделе наследства между родственниками, мерах воспитания и предупреждения, размере и видах уголовного наказания за преступления и т.п. – будут приниматься не человеком, а машиной с ИИ.

Исходя из анализируемой юридической литературы и результатов личной коммуникации с ИИ, видятся следующие наиболее очевидные направления его использования в законотворческой и правоприменительной практике:

1) замещение нормативно-правового регулирования отдельных видов общественных отношений их автоматическим или полуавтоматическим регулированием на основе ИИ;

2) анализ существующей системы законодательства в целях ее оптимизации, устранения дублирования и противоречий юридических норм. Создание предпосылок для отраслевой и межотраслевой систематизации и кодификации законодательства;

3) анализ и оптимизация структуры нормативных правовых актов. Создание предпосылок для формирования крупных кодифицированных правовых актов – электронных кодексов;

4) анализ проблем, составляющих предмет правового регулирования, для выявления всего набора возможных социально-правовых решений и выбора среди них оптимального варианта;

5) мониторинг и прогнозирование действия законодательства. Оценка эффективности действующих нормативных правовых актов на основе системы взаимосвязанных критериев;

6) выделение юридических фактов и доказательств из совокупности больших данных;

7) разработка полных и завершенных проектов законодательных и правоприменительных правовых актов;

8) подбор аргументации для формирования правовых позиций участников правоприменительного процесса. Анализ сильных и слабых сторон их правовых позиций:

9) прогнозирование вероятных правовых действий участников правоприменительного процесса, выработка оптимальной правовой стратегии и тактики;

10) правовая экспертиза и правовой консалтинг. Использование ИИ для расчета и обоснования цены, прибыли, вреда, стоимости имущественных комплексов, наследственных долей и т.п.;

11) замена, где это возможно, бумажных контрактов на электронные «умные контракты», использующие возможности искусственного интеллекта;

12) использование ИИ для подготовки и обоснования управленческих и кадровых решений;

13) создание архивов и баз данных законотворческой и правоприменительной информации, оснащенных эффективными поисковыми системами;

14) анализ юридического языка. Создание правовых энциклопедий, справочников, словарей, тезаурусов.

Быстро развивающаяся практика, без сомнения, найдет множество иных сфер применения искусственного интеллекта в законотворческой и правоприменительной деятельности, юридической науке и образовании.

Заключение

Сказанное позволяет сделать вывод, что искусственный интеллект имеет множество сфер, способов и методов применения, как в области законотворчества, так и в правоприменительной деятельности. В качестве современного мощного инструмента научного поиска он способен существенно продвинуть правовую науку и юридическую аналитику.

Список литературы

1. Березина Е.А. Использование искусственного интеллекта в юридической деятельности // Актуальные проблемы российского права. – 2022. – № 12 (145). – С. 25–38.
2. Воронин Н. Нейросеть-нейросеть, сколько мне жить осталось? – URL: https://storage.googleapis.com/gsc-link/www.bbc.com/f78d83b5.html (дата обращения: 04.03.2025).
3. Володенков С.В., Федорченко С.Н. Риски применения алгоритмов искусственного интеллекта в социально-политической сфере: обзор современных научных работ // Дискурс-Пи. – 2024. – № 2. – С. 24–48.
4. Горбачева Т.А. Искусственный интеллект: риски и проблемы внедрения в Российской Федерации // Инновационная экономика: информация, аналитика, прогнозы. – 2025. – № 1. – С. 96–105.
5. Залоило М.В. Искусственный интеллект в праве: науч.-практ. пособие. – Москва: Инфотропик, 2021. – 132 с.

6. Исаков В.Б. Правовой статус робота, наделенного искусственным интеллектом: объект или субъект? // Субъект права: стабильность и динамика правового статуса в условиях цифровизации: сб. науч. тр. / под общ. ред. Д.А. Пашенцева, М.В. Залоило. – Москва: Инфотропик, 2022. – С. 104–112.
7. Наумов В.Б., Камалова Г.Г. Вопросы построения юридических дефиниций в сфере искусственного интеллекта // Труды Института государства и права РАН. – 2020. – № 1. – С. 81–93.
8. Понкин И.В., Редькина А.И. Искусственный интеллект с точки зрения права // Вестник РУДН. Сер. Юридические науки. – 2018. – № 1. – С. 91–109.
9. Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования: монография / [А.Ф. Абдулвалиев и др.; под науч. ред. проф. Е.В. Смахтина, проф. Р.Д. Шарапова, доц. В.И. Морозова]; Министерство науки и высшего образования Российской Федерации, Тюменский государственный университет, Институт государства и права. – Тюмень: Изд-во Тюменского гос. ун-та, 2021. – 376 с.
10. Пшинник К. Искусственный интеллект. Путь к новому миру. – Москва: АСТ, 2025. – 246 с.
11. Риски искусственного интеллекта: учебный портал geeksforgeeks. – URL: https://translated.turbopages.org/proxy_u/en-ru.ru.9900257f-680a2801-d26eae5d-74722d776562/https/www.geeksforgeeks.org/risk-of-ai/ (дата доступа 24. 04.2025).
12. Сознание // Новая философская энциклопедия. – URL: https://iphlib.ru/library/collection/newphilenc/document/HASH01089449209fc347f3553108 (дата обращения: 24.04.2025).
13. Сильный ИИ против слабого ИИ: в чем разница? – URL: https://new-science.ru/silnyj-ii-protiv-slabogo-ii-v-chem-raznica/ (дата обращения: 01.04.2025).
14. Субъект права: стабильность и динамика правового статуса в условиях цифровизации: сб. науч. тр. / под общ. ред. Д.А. Пашенцева, М.В. Залоило. – Москва: Инфотропик Медиа, 2022. – 480 с.
15. Сурова Н.Ю., Косов М.Е. Искусственный интеллект: монография. – Москва: ЮНИТИ - ДАНА, 2021. – 407 с.
16. Человекоподобный робот София получила гражданство Саудовской Аравии. – URL: https://www.ntv.ru/novosti/1945500/ (дата обращения: 24.04.2025).
17. Янковский Р.М. Использование искусственного интеллекта в работе юриста: практ. руководство. – Москва: НОУРУТС, 2025. – 53 с.

УДК 34.096; 341 DOI: 10.31249/iajpravo/2025.03.05

УМНОВА-КОНЮХОВА И.А.[1] **ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МЕЖДУНАРОДНОЕ ПРАВО: НАСТОЯЩЕЕ И БУДУЩЕЕ (Статья)**

Аннотация. Исследуются актуальные аспекты международно-правового регулирования использования искусственного интеллекта в условиях технологических вызовов, которые создает искусственный интеллект международным стандартам прав человека и верховенству права. Рассматриваются правозащитные подходы в совершенствовании международного права в будущем в связи с использованием искусственного интеллекта, и в этих целях систематизируются пути адаптации международного права к вызовам правам человека со стороны искусственного интеллекта. Другой затрагиваемый в статье актуальный аспект касается международно-правового регулирования ценностей и принципов этики искусственного интеллекта, реализация которых также основывается на правозащитном подходе к этике искусственного интеллекта и осуществляется с помощью универсального «мягкого» права, права международных неправительственных организаций и региональных международно-правовых стандартов (на примере Евросоюза).

[1] *Умнова-Конюхова Ирина Анатольевна*, главный научный сотрудник отдела правоведения ИНИОН РАН, доктор юридических наук, профессор.

Ключевые слова: искусственный интеллект; международное право; права человека; принципы; международные организации; этика искусственного интеллекта.

UMNOVA-KONIUKHOVA I.A. Artificial Intelligence and International Law: Present and Future (Article)

Abstract. The article examines current aspects of international legal regulation of the use of artificial intelligence in the context of technological challenges posed by artificial intelligence to international human rights standards and the rule of law. The article considers human rights approaches to improving international law in the future in connection with the use of artificial intelligence and, for this purpose, systematizes ways to adapt international law to the challenges of human rights from artificial intelligence. Another relevant aspect raised in the article concerns the international legal regulation of the values and principles of ethics of artificial intelligence, the implementation of which is also based on a human rights-based approach to the ethics of artificial intelligence and is carried out using universal "soft" law, the law of international non-governmental organizations and regional international legal standards (using the example of the European Union).

Keywords: artificial intelligence; international law; human rights; principles; international organizations; ethics of artificial intelligence.

Для цитирования: Умнова-Конюхова И.А. Искусственный интеллект и международное право: настоящее и будущее (Статья) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2025. – № 3. – С. 63–75. – DOI: 10.31249/iajpravo/2025.03.05

Введение

Вторжение искусственного интеллекта (ИИ) во все сферы развития человеческой цивилизации и в повседневную жизнь каждого человека, его использование во многих профессиях, услугах и отраслях – все это порождает новые запросы на модернизацию права. Передовые технологии имеют большой потенциал в том, чтобы помочь человечеству преодолеть серьезные проблемы, такие как, например, регулирование и оптимизация экономических и социальных систем, движение финансовых потоков и денежных средств, диагностика и лечение заболеваний, управление экологическими ресурсами, борьба с бедностью и достижение других це-

лей устойчивого развития. ИИ все чаще используется органами публичной власти и государственными служащими для оценки деятельности, распределения ресурсов, осуществления правосудия и принятия других решений, которые могут иметь ощутимые последствия для прав человека и верховенства права. Российская Федерация, страны Евросоюза, США, Китай, Япония и многие другие государства уже внедрили новые технологии для выполнения государственных задач и улучшения государственных функций и предпринимают определенные действия для интернационализации и унификации правил использования ИИ.

Несмотря на то что ИИ выполняет множество задач и способен облегчать и упрощать определенные операции и действия, исследователями обоснованно оценивается и прогнозируется потенциал его разрушительного воздействия, что свидетельствует о необходимости формирования комплекса правил и стандартов для использования этой технологии на национальном и международном уровнях. Например, ИИ неизбежно может заменить многие рабочие места и виды деятельности человека и в перспективе без ограничений его использования способен лишить человечество значимого и эффективного участия в его жизни, т.е. повлияет на судьбу настоящих и будущих поколений.

Названные и другие риски обусловливают необходимость правового регулирования процессов использования ИИ и формирования международно-правовых стандартов в этой сфере, позволяющих найти правильный баланс между технологическим прогрессом, защитой прав человека и верховенством права на национальном и международном уровнях.

Предпринимая попытку анализа этих правовых проблем, первый вопрос, который задают исследователи ИИ, – как его определить и добиться унифицированного понимания в международном и национальном праве. Джемин Ли, профессор права Школы права Сеульского национального университета (Южная Корея), отмечает, что этот термин используется в различных контекстах[1]. В самом общем понимании Оксфордский словарь определяет ИИ как «теорию и разработку компьютерных систем, способных выполнять задачи, обычно требующие человеческого

[1] См.: Jaemin Lee. Artificial Intelligence and International Law. – 2022. – P. 1.

интеллекта»[1]. Дж. Ли, анализируя разные определения, считает, что они совпадают в следующих основных признаках: 1) системы; 2) данные и 3) выбор действий, которые необходимо предпринять. Второй элемент (данные) и третий элемент (выбор действия) вместе означают человеческий интеллект[2].

Существует подробное определение ИИ, подготовленное Экспертной группой высокого уровня по ИИ Европейского союза: «Системы [ИИ] – это программные (и, возможно, также аппаратные) системы, разработанные людьми, которые при наличии сложной цели действуют в физическом или цифровом измерении, воспринимают окружающую среду посредством сбора данных, а также интерпретация собранных структурированных или неструктурированных данных, рассуждения на основе полученных знаний или обработки информации, полученной из этих данных, и принятие решения о наилучших действиях для достижения поставленной цели. Системы ИИ могут либо использовать символические правила, либо обучаться численной модели, а также адаптировать свое поведение, анализируя, как их предыдущие действия влияют на окружающую среду»[3]. Таким образом, ИИ «анализирует окружающую среду, собирает данные, делает выводы на основе имеющейся информации или обрабатывает информацию на основе этих данных и принимает решения о том, какие шаги лучше предпринять для достижения определенных целей»[4].

В настоящее время сложилась определенность в том, что существует ИИ с узкими и широкими функциями. К «узким» ИИ относятся переводческие сервисы, чат-боты и автономные транспортные средства, к «общим» («широким») ИИ – самообучающиеся системы, которые могут осваивать человеческие функции и даже превосходить человеческую производительность во всех задачах. Как отмечает Джош Мельцер (старший научный сотруд-

[1] См.: Oxford Dictionary of English. – 2016; Beard J.M., Autonomous Weapons and Human Responsibilities // Georgetown Journal of International Law. – 2014. – Vol. 45. – P. 624.

[2] Ibid.

[3] См.: EU High-Level Expert Group on AI. A definition of AI, main capabilities and scientific disciplines. EU Commission. – 2019. – P. 6. – URL: file:///C:/Users/Администратор/Downloads/ai_hleg_ai_definition_final_DF06F793-EA01-3573-16D2ACD625E2BDB0_56341.pdf (дата обращения: 02.04.2025).

[4] Correia A., Reyes I. AI research and innovation: Europe paving its own way. Working Paper, European Commission. – 2020. – URL: https://doi.org/10.2777/264689 (дата обращения: 05.04.2025).

ник программы глобальной экономики и развития Института Брукингса в Вашингтоне, США), «общий ИИ поднимает более широкие экзистенциальные проблемы, такие как согласование целей такой системы с нашими собственными, чтобы предотвратить катастрофические результаты, но общий ИИ по-прежнему остается технологией, которую еще предстоит развивать в отдаленном будущем»[1].

Правовое регулирование ИИ на международном уровне развивается преимущественно с помощью мягкого права. Другая особенность заключается в многоотраслевом охвате сфер правового регулирования. С точки зрения Аббаса Пурхашеми (Канадский институт международно-правовой экспертизы, Торонто), сложный ландшафт международного права предопределяет необходимость определения взаимодействия между искусственным интеллектом и такими важнейшими областями, как права человека, уголовное право, торговое право, арбитраж и другие сферы применения ИИ[2].

Правозащитные подходы в совершенствовании международного права в связи с использованием искусственного интеллекта

Искусственный интеллект упрощает вмешательство и мониторинг деятельности людей, который получил название в правовой литературе «алгоритмическая слежка». Как отмечает Саназ Шабани Колахи (магистр права в области интернет-технологий в Университете Боккони, Милан, Италия), алгоритмическая слежка затрагивает различные виды прав человека, включая право на недискриминацию, равенство перед законом, справедливое обращение со стороны суда, неприкосновенность частной жизни, свободу передвижения и проживания, свободу мысли и религии, свободу мнений и их выражения, право на собрания, право на демократию, право на социальное обеспечение, право на труд и право на образование. Некоторые из них еще более хрупки в противостоянии с технологиями и искусственным интеллектом, что представляет

[1] Meltzer J.P. The Impact of Artificial Intelligence on International Trade. Brookings. – 2018. – 13 Dec. – URL: https://www.brookings.edu/articles/the-impact-of-artificial-intelligence-on-international-trade/#footnote-1 (дата обращения: 07.04.2025).

[2] См.: Artificial Intelligence and the Future of International Law Bridging Rights, Trade, and Arbitration / ed. Abbas Poorhashemi. – 2024. – P. VII.

собой значительный риск для равноправного и надлежащего внедрения. В связи с этим крайне важно, по мнению С.Ш. Колахи, иметь строгие границы для контроля технологий слежки[1].

Особое внимание эксперты и правозащитники обращают на юридические гарантии права на неприкосновенность.

Дж. Ли, высказывая озабоченность о сложности реализации данного права в условиях новых технологий, пишет о том, что ИИ позволяет собирать данные о передвижениях, речах, поведении и различных действиях людей в режиме реального времени. Собранные таким образом данные могут быть оперативно обработаны для многих целей. Как следствие, правительства (или любые другие органы, владеющие данными) могут отслеживать людей, что продемонстрировали технологии контроля во время COVID-19. Системы искусственного интеллекта, такие как дроны, автономные объекты и роботы-убийцы в настоящее время создают множество юридических сложностей в отсутствие элементарного нормирования и регулирования, как во внутренних, так и в международных правовых системах[2].

В Докладе Верховного комиссара ООН по правам человека от 3 августа 2018 г. «Право на неприкосновенность частной жизни в цифровую эпоху» подчеркивается важность обязательств государств и корпораций в области неприкосновенности частной жизни. Они заключаются в обязанности защищать право на неприкосновенность частной жизни в цифровую эпоху, а также в обеспечении надлежащих мер безопасности и эффективного надзора[3].

Адаптация международного права к вызовам правам человека со стороны ИИ происходит разными путями. Один из них – наиболее распространенный – совершенствование действующего международного права. Речь идет, в частности, о поправках в Женевскую декларацию в сфере медицины (принята Генеральной ассамблеей Всемирной медицинской ассоциации (BMA) в Женеве в

[1] См.: Kolahi S.Sh. Artificial Intelligence and Human Rights // Artificial Intelligence and the Future of International Law Bridging Rights, Trade, and Arbitration / ed. Abbas Poorhashemi. – 2024. – P. 1–2.

[2] См.: Jaemin Lee Artificial Intelligence and International Law. – 2022. – P. 2.

[3] См.: A/HRC/39/29. United Nations High Commissioner for Human Rights. The Right to Privacy in the Digital Age. – 2017. – URL: https://www.ohchr.org/ru/documents/right-privacy-digital-age-report-united-nations-high-commissioner-human-rights (дата обращения: 17.03.2025).

1948 г. и дополнена и изменена в 1968, 1983, 1994, 2005, 2006, 2017 гг.)[1]. Так, 68-я Генеральная ассамблея ВМА в октябре 2017 г. с учетом внедрения ИИ в медицину дополнила Декларацию такими принципами, как уважение к самостоятельности пациента; взаимное уважение к учителям, коллегам и студентам-медикам, которые делятся медицинскими знаниями на благо своих пациентов и для развития здравоохранения; требование к врачам заботиться о собственном здоровье так же, как и о здоровье своих пациентов. Кроме того, пересмотренный текст предназначен для использования всеми практикующими врачами.

Другой путь адаптации международного права к вызовам правам человека – принятие целевых международно-правовых актов, направленных на комплексное регулирование вопросов использования ИИ в контексте требований защиты прав человека.

Примером такого комплексного подхода является принятие Европейским парламентом и одобрение Советом ЕС 13.03.2024 г. *Регламента (Закона) об искусственном интеллекте*, предусматривающего некоторые ограничения, которые до сих пор не имели четкой правовой основы или были отраслевыми. В ст. 5 Закона ЕС об искусственном интеллекте признаются некоторые ситуации, в которых использование искусственного интеллекта запрещено. Некоторые из них связаны с обстоятельствами слежки. Например, согласно пп. 1b, 1c и 1g, дискриминационная слежка запрещена. Кроме того, п. 1d запрещает профилирование с помощью ИИ в преступных целях. Распознавание лиц, являющееся эффективным инструментом для целей наблюдения, в соответствии с п. 1 e ограничено «созданием или расширением баз данных распознавания лиц путем нецелевого извлечения изображений лиц из Интернета или записей с камер видеонаблюдения».

В некоторых случаях устанавливаются исключения для использования конкретной технологии ИИ, но с особой осторожностью. Один из случаев – использование дистанционной биометрической идентификации только полицией в условиях использования ИИ с высоким риском и выполнения соответствующих правил. Кроме того, в Акте дается разрешение полиции на системы ИИ,

[1] См.: Женевская декларация Всемирной медицинской ассоциации. – URL: https://medpravo.com.ru/?page_id=328&ysclid=m9a7spahbc634554608 (дата обращения: 22.03.2025).

которые обрабатывают данные о чувствительных / защищенных характеристиках для маркировки или фильтрации[1].

Вопросы защиты частной жизни в странах – членах ЕС регулируются также *Общим регламентом о защите персональных данных* (*General Data Protection Regulation* (далее – GDPR), утвержденным постановлением 2016/679 Европейского парламента и Совета ЕС (вступил в силу в 2018 г.)[2]. На основе этого акта ЕС усиливает и унифицирует защиту персональных данных всех лиц в Союзе. GDPR обеспечивает гражданам возможность контроля над собственными персональными данными и унифицирует нормативную базу для международных экономических отношений в рамках ЕС.

Общий регламент по защите данных требует, чтобы каждый, кто собирает данные, информировал владельца и получал согласие. Однако неправомерное использование данных часто не оспаривается теми, чьи персональные данные собираются, потому что они либо не могут этого сделать, либо беспомощны в решении проблемы.

Статья 22 GDPR запрещает несанкционированную обработку и профилирование. GDPR устанавливает строгие штрафы для предприятий, разрабатывающих ИИ, за несоблюдение правил Регламента. Автоматизированное принятие решений имеет два условия, при которых корпорация несет ответственность за создание юридических или аналогичных значимых последствий. Корпорации несут ответственность за свои решения со стороны ИИ в области прав человека, и они обязаны учитывать GDPR в этих вопросах.

Еще один заметный документ в международном праве – *Руководящие принципы по искусственному интеллекту* ОЭСР от 22.05.2019 г. (ред. 2024 г.)[3] (насчитывается 47 стран – участников

[1] См.: Регламент (Закон) Европейского союза об искусственном интеллекте. – 2024. – 13.03. – URL: https://ai.gov.ru/knowledgebase/dokumenty-po-razvitiyu-ii-v-drugikh-stranakh/2024_reglament_evropeyskogo_soyuza_ob_iskusstvennom_intellekte_ano_cifrovaya_ekonomika_/?ysclid=m9a67ht9wr302890215 (дата обращения: 03.04.2025).

[2] The General Data Protection Regulation. The EU General Data Protection Regulation (GDPR) Governs how the Personal Data of Individuals in the EU may be Processed and Transferred. – URL: https://www.consilium.europa.eu/en/policies/data-protection-regulation/ (дата обращения: 27.03.2025).

[3] См.: Principles for Trustworthy AI. – URL: https://oecd.ai/en/ai-principles (дата обращения: 07.04.2025).

этой организации по состоянию на февраль 2023 г., Россия участником не является ОЭСР). Принципы формируют правовые основы применения ИИ в экономике, государственном управлении и других сферах жизнедеятельности. Согласно Руководящим принципам, системы ИИ должны разрабатываться в соответствии с уважением верховенства права, права человека, демократических ценностей и обеспечивать справедливое общество.

Таким образом, принципы ИИ ОЭСР направляют участников деятельности в области ИИ в их усилиях по созданию надежного ИИ и предоставляют директивным органам рекомендации по эффективной политике в области ИИ. Страны используют Принципы ИИ ОЭСР и связанные с ними инструменты управления рисками ИИ, создавая основу для глобальной совместимости между различными юрисдикциями. В настоящее время ООН, ЕС, Совет Европы и другие международные юрисдикции используют приведенное в Руководящих принципах определение системы ИИ и его жизненного цикла в своих актах. Кроме того, многие страны также руководствуются данными Принципами.

Среди актов неправительственных международных организаций заслуживает внимания *Торонтская декларация*: защита прав на равенство и недискриминацию в системах машинного обучения от 16.05.2018 г.[1] – совместное заявление, опубликованное рядом международных неправительственных организаций (e.g. Amnesty International, Access Now), призывающая к ответственной практике в сфере IT-технологий. Цель Декларации – определить «осязаемые и применимые на практике стандарты для государств и частного сектора». Документ призывает к реальным решениям, таким как возмещение ущерба жертвам алгоритмической дискриминации. В Декларации провозглашается равенство и недискриминация в правах человека в связи с использованием IT-технологий. В этом контексте Декларация посвящена проблемам алгоритмической предвзятости и потенциальной дискриминации, которые возникают в результате использования машинного обучения и искусственного интеллекта в приложениях, способных влиять на жизнь людей, «от полиции до систем социального обеспечения, здравоохранения и платформ для онлайн-дискуссий». Важной пробле-

[1] См.: The Toronto Declaration “Protecting the Right to Equality and Non-Discrimination in Machine Learning Systems”. – URL: https://www.torontodeclaration.org/declaration-text/english/(дата обращения: 28.03.2025).

мой, затронутой в документе, является потенциальное нарушение конфиденциальности информации

Третий путь адаптации международного права к вызовам правам человека – защита органами международного правосудия и квазисудебными органами прав человека в связи с использованием ИИ.

Так, рост международного терроризма в начале нынешнего столетия обусловил развитие антитеррористического законодательства государств, в котором были расширены правовые границы и каналы слежки. Возникла научная дискуссия о поиске баланса между правом на частную жизнь и правом на безопасность. Для обеспечения безопасности слежка помогает предотвратить террористические атаки или другие серьезные преступления. Однако без правовых границ вероятен риск массовой и / или дискриминационной слежки. Такой вопрос возник в деле *La Quadrature du Net v. Франция*. Суть требования истца состояла в отмене некоторых постановлений французского правительства, обязывающего провайдеров электронных коммуникаций хранить и обрабатывать огромные объемы пользовательских данных для борьбы с терроризмом. Общее и дискриминационное удержание данных без согласия их владельцев было одним из основных аргументов истца, и это привело к решению Суда ЕС, исключающему национальные законодательные меры, требующие неизбирательного хранения данных о трафике и местоположении[1].

В другом деле – *Google против Испании* (Case C-131/12) – Суд ЕС обратил внимание на важность сохранения конфиденциальности с помощью алгоритмов искусственного интеллекта. Суд ЕС основывал свое решение на Директиве о защите данных[2]. Суд заявил, что согласно ст. 12 названной Директивы субъекту данных предоставляется право на исправление, удаление или блокировку данных, если обработка не соответствует Директиве. Кроме того, на основании ст. 14 Директивы субъект данных может в любое время на веских законных основаниях, связанных с его конкретной ситуацией, возразить против обработки относящихся к нему данных. Это решение было одним из первых, которым была защищена

[1] См.: Kolahi S.Sh. Artificial Intelligence and Human Rights // Artificial Intelligence and the Future of International Law Bridging Rights, Trade, and Arbitration. – 2024. – P. 2.

[2] См.: Directive 95/46/EC. – URL: https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng (дата обращения: 25.03.2025).

конфиденциальность от неограниченного использования ИИ крупными технологическими корпорациями[1].

Международно-правовое регулирование ценностей и принципов этики искусственного интеллекта

Первый международно-правовой стандарт по этике ИИ – Рекомендации об этике искусственного интеллекта – были представлены в рамках ЮНЕСКО (ноябрь 2021 г.)[2]. Этот стандарт международного мягкого права применим ко всем 194 государствам – членам ЮНЕСКО.

Четыре основные ценности в Рекомендациях создают основу для ИИ-систем, работающих на благо человечества, отдельных людей, общества и окружающей среды: 1) права человека и человеческое достоинство (уважение, защита и поощрение прав человека, основных свобод и человеческого достоинства); 2) жизнь в тишине (справедливые и взаимосвязанные общества); 3) обеспечение разнообразия и инклюзивности; 4) процветание окружающей среды и экосистемы.

Реализация данных ценностей основывается на принципах правозащитного подхода к этике ИИ: 1) пропорциональность и ненанесение вреда; 2) охрана и безопасность; 3) обеспечение права на неприкосновенность частной жизни и защиту данных; 4) многостороннее и адаптивное управление и сотрудничество; 5) ответственность и подотчетность; 6) прозрачность; 7) человеческий контроль и решимость; 8) экологичность; 9) осведомленность и грамотность; 10) справедливость и недопущение дискриминации.

Таким образом, Рекомендации направлены на претворение в жизнь основных ценностей и принципов в целях защиты прав человека, обеспечения равноправия и справедливости, охраны окружающей среды и экосистем, содействия образованию и научным исследованиям, развития здравоохранения, социального благополучия, а также многих других сфер.

---

[1] См.: Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. – URL: https:// eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri=CELEX:62012 CJ0131_SUM (дата обращения: 30.03.2025).

[2] См.: Recommendation on the Ethics of Artificial Intelligence – URL: https:// unesdoc.unesco.org/ark:/48223/pf0000381137 (дата обращения: 19.03.2025).

Универсальное международное право по использованию ИИ формируется с учетом регионального опыта. В этом отношении интерес представляет право ЕС.

Так, 8 апреля 2019 г. Экспертная группа высокого уровня по искусственному интеллекту Европейской комиссии представила Этические рекомендации по использованию надежного и безопасного искусственного интеллекта. Им предшествовал проект руководящих принципов (декабрь 2018 г.), к которым после открытых консультаций поступило более 500 комментариев. Согласно Руководству, заслуживающий доверия ИИ должен быть законным, этичным и надежным (как технически, так и с учетом социальной среды)[1].

В 2020 г. данная Экспертная группа высокого уровня по ИИ представила Список оценок надежного искусственного интеллекта (Assessment List for Trustworthy AI) (ALTAI). ALTAI – документ, «предназначенный для целей самооценки» для людей, участвующих в развитии технологии искусственного интеллекта, включая разработчиков, специалистов по обработке данных, сотрудников фронтенда, юристов, управленческий персонал, специалистов по закупкам и т.д. В документе затронут комплекс вопросов, направленных на оценку надежности технологии искусственного интеллекта с учетом этических требований: 1) человеческая деятельность и надзор; 2) техническая надежность и безопасность; 3) конфиденциальность и управление данными; 4) прозрачность; 5) многообразие, недискриминация и справедливость; 6) социальное и экологическое благополучие; 7) подотчетность. В документе также представлен новый глоссарий, который включает в себя важные юридические термины, такие как подотчетность, предвзятость и т.д.[2]

[1] См.: Ethics Guidelines for Trustworthy AI. – URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (дата обращения: 07.04.2025).

[2] См.: Экспертная группа высокого уровня Европейской комиссии по искусственному интеллекту опубликовала окончательный список оценки надежного искусственного интеллекта (ALTAI). – URL: https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment/ (дата обращения: 17.03.2025).

Заключение

В современную эпоху ИИ-технологии все больше интегрируются в жизнь людей и становятся необходимостью для нынешнего и будущих поколений. Между тем международное право сталкивается с множеством новых вызовов в решении актуальных проблем, связанных с использованием технологических разработок, которые включают в себя новые программы, алгоритмы и машины ИИ в глобальных и национальных целях развития. В связи с этим особую озабоченность вызывают правовые последствия, вытекающие из стремительного развития и применения ИИ, что обусловливает необходимость анализа существующих принципов и норм международного права и их совершенствования в условиях новой реальности. Будущее международного права в условиях широкого использования ИИ видится в формировании международно-правовых стандартов, позволяющих найти правильный баланс между технологическим прогрессом, оптимизирующим и улучшающим жизнь людей, с одной стороны, и защитой прав человека, верховенством права – с другой.

УДК 342; 34.096 DOI: 10.31249/iajpravo/2025.03.06

АЛЕШКОВА И.А.[1] ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И РАЗВИТИЕ ЦИФРОВОГО МЕЖДУНАРОДНОГО ПРАВА (Обзорная статья)

Аннотация. Основываясь на анализе научных публикаций, рассматривается влияние международного права на регулирование отношений, возникающих в связи с применением искусственного интеллекта. Обобщаются позиции ученых, исследующих новые принципы внедрения искусственного интеллекта, в том числе принципы этического и социально полезного искусственного интеллекта для решения таких ключевых задач международного права, как поддержание мира, защита прав человека, международное сотрудничество, использование форм экономического, социального и политического взаимодействия и др. Раскрываются точки зрения ученых-правоведов на развитие цифровизации в международных отношениях, на проблемы и пути дальнейшего развития искусственного интеллекта и будущее международного права.

Ключевые слова: искусственный интеллект; международное право, права человека; руководящие принципы; цифровизация.

ALESHKOVA I.A. Artificial Intelligence and the Future of International Law (Review article)

Abstract. Based on the analysis of scientific publications, the influence of international law on the regulation of relations arising in connection with the use of artificial intelligence is considered. The positions of scientists investigating new principles of AI implementation are summarized, including the principles of ethical and socially useful artificial intelligence for the solution of such key tasks of international law as maintaining peace, protecting human rights, international cooperation, the use of forms of economic, social and political interaction,

[1] *Алешкова Ирина Александровна*, ведущий научный сотрудник отдела правоведения ИНИОН РАН, кандидат юридических наук, доцент.

etc. The points of view of legal scholars on the development of digitalization in international relations, on the problems and ways of further development of artificial intelligence and the future of international law are revealed.

Keywords: artificial intelligence; international law, human rights; guiding principles; digitalization.

Для цитирования: Алешкова И.А. Искусственный интеллект и развитие цифрового международного права (Обзорная статья) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2025. – № 3. – С. 76–89. – DOI: 10.31249/iajpravo/2025.03.06

Введение

Появление искусственного интеллекта (ИИ) как технологии, имеющей высокий потенциал для новых возможностей, стало предпосылкой к изменению многих устоявшихся подходов в международных отношениях. Использование ИИ в качестве нового инструмента международного взаимодействия позволяет, в частности, создавать трансграничные цифровые платформы[1] и цифровые экосистемы[2]. В то же время надежность функционирования ИИ связана с совершенствованием законодательства, решения новых правовых вопросов, проблем и минимизации рисков. Ученые и практики активно изучают практику внедрения ИИ, которая, очевидно, будет только развиваться и влиять на глобальные проекты, задающие архитектуру международных отношений цифрового будущего[3]. В связи с вышеизложенным исследование научных позиций в области создания и применения технологий ИИ в международном праве представляется не только интересным, но и важным. Особенно заслуживающим внимания является то, что данная

[1] Терещенко Л.К. Цифровые платформы: подходы к регулированию // Журнал российского права. – 2024. – № 9. – С. 163.

[2] Бурова А.Ю. Цифровые экосистемы: необходимость и содержание законодательного регулирования // Журнал российского права. – 2024. – № 1. – С. 143.

[3] Алферова Е.В., Скурко Е.В. Рецензия на книгу: Искусственный интеллект и нормативные вызовы: международная и сравнительно-правовая перспективы / под ред. А. Корнилакис, Г. Ноускалис, В. Пергантис, Ф. Цимас // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. Государство и право. – 2024. – № 4. – 128–137.

тема отличается высокой динамичностью, и в ней происходят непрерывные изменения.

Новый подход к принципам международного права: конструктивная модель

Стремительное проникновение ИИ в повседневную жизнь и обеспокоенность по поводу рисков, которые они представляют для отдельных лиц и общества, побудили профессиональные ассоциации выпустить руководящие принципы, направленные на установление этических принципов ответственного ИИ.

Сакико Фукуда-Парр, профессор международных отношений в Новой школе в Нью-Йорке, и Элизабет Гиббонс, старший научный сотрудник Центра здоровья и прав человека имени Франсуа-Ксавье Банью (FXB), рассматривая формирующиеся принципы в области применения ИИ, обращают внимание на то, что они направлены на создание этического ИИ. По мнению ученых, несмотря на то что этические принципы не имеют юридической легитимности и формируются профессиональными сообществами, они создают нарративы и выстраивают то, что фактически является консенсусными нормами практики в области цифровизации[1].

Этические принципы ИИ рассматриваются специалистами как руководящие принципы в области управления ИИ. Они закреплены в Рекомендациях по этике искусственного интеллекта (Recommendation on the Ethics of Artificial Intelligence, UNESCO), принятых 193 государствами – членами ЮНЕСКО, на конференции, проходившей в Париже с 9 по 24 ноября 2021 г. Этот документ признается первым в истории глобальным соглашением об этике ИИ[2]. Руководящие принципы «этической практики» стали ответом заинтересованных сторон на растущую обеспокоенность по поводу пагубных социальных последствий ИИ и цифровых технологий. Одна из главных целей Рекомендации – предоставить универсальную базу принципов, которыми государства могли бы руководствоваться при формировании своего законодательства (например принципы общей пользы и непричинения вреда; безо-

[1] Fukuda-Parr S., Gibbons E. Emerging Consensus on “Ethical AI”: Human Rights Critique of Stakeholder Guidelines // Glob Policy. – 2021. – Vol. 12. – P. 32.

[2] Recommendation on the Ethics of Artificial Intelligence – UNESCO. – URL: https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence (дата обращения: 21.04.2025).

пасности и надежности; справедливости и недискриминации и др.)[1].

С. Фукуда-Парр и Э. Гиббонс, проведя на основе библиометрического анализа изучение практики формирования этических принципов ИИ, выявили, что всего за несколько лет эти руководящие принципы для заинтересованных сторон разрослись и уже к дате принятия вышеуказанного документа этот «глобальный реестр», как его назвали авторы, включал более 160 ключевых принципов. По мнению авторов, эти этические принципы, несмотря на их несколько расплывчатые формулировки, следует признать «нормативным ядром подхода к этике и управлению ИИ, основанного на принципах»[2].

На наш взгляд, этические принципы – долженствования, которые оказывают сильное влияние на разработку и реализацию мер политики и правовых норм. Наряду с устоявшимися принципами международного права эти принципы действуют в случаях, когда имеются пробелы или коллизии в праве.

Таким образом, именно эта конструктивная тактика, сочетающая синтезирование правового и этического, формирует новый подход к принципам как регуляторам отношений в области цифровизации, и тем самым закладывается основа будущего цифрового международного права.

Особенности развития цифровых международных отношений

В современный период, характеризующийся интенсивным развитием трансграничных цифровых платформ и цифровых экосистем, которые за сравнительно короткое время существенно изменили образ жизни человека и общества, возникает потребность в регулировании цифровых международных отношений.

В 2018 г. в рамках ООН была создана Группа высокого уровня по цифровому сотрудничеству для выработки предложений об укреплении сотрудничества в цифровой сфере между прави-

[1] Этика ИИ в авангарде мировой повестки. – URL: https://vk.com/wall-46560358_6074?ysclid=maf1716i9a437289103 (дата обращения: 21.04.2025).

[2] Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. / J. Fjeld, N. Achten, H. Hilligoss, A. Nagy. – 2020. – P. 5. – URL:-https://www.researchgate.net/publication/339138141_Principled_Artificial_Intelligence_Mapping_Consensus_in_Ethical_and_Rights-Based_Approaches_to_Principles_for_AI (дата обращения: 05.05.2025).

тельствами, частным сектором, гражданским обществом, международными организациями, научными учреждениями, техническим сообществом. В 2019 г. Группа представила доклад под названием «Эпоха цифровой взаимозависимости» и предложила пять рекомендаций относительно того, каким образом международное сообщество могло бы принять совместные меры в целях оптимизации цифровых технологий и снижения рисков:

1) построение инклюзивной цифровой экономики и общества;

2) укрепление человеческого и институционального потенциала;

3) защита прав человека и его способности активно воздействовать на мир;

4) содействие укреплению доверия, безопасности и стабильности в цифровом пространстве;

5) содействие глобальному цифровому сотрудничеству[1].

А.Х. Абашидзе, доктор юридических наук, профессор, директор Юридического института РУДН им. Патриса Лумумбы, заведующий кафедрой международного права этого университета, обращает внимание на то, что все эти рекомендации взаимосвязаны и их надо рассматривать комплексно, с учетом друг друга[2].

11 июня 2020 г. Генеральный секретарь ООН А. Гутерриш представил Дорожную карту по цифровому сотрудничеству для международного сообщества, которая направлена на поддержку глобального сотрудничества в области ИИ, обеспечение доступного и безопасного Интернета, продвижение цифровых общественных благ и цифровой интеграции, защиту прав человека, а также содействие цифровому доверию[3]. Эта Дорожная карта основана на рекомендациях Группы высокого уровня по цифровому сотрудничеству, а также на мнениях государств – членов ООН, частного

[1] Группа высокого уровня Генерального секретаря ООН по цифровому сотрудничеству [Электронный ресурс] // Официальный сайт ООН. – URL: https://www.un.org/ru/sg-digital-cooperation-panel (дата обращения: 05.05.2025).

[2] Цит. по: Абашидзе А.Х. Влияние цифровизации жизни общества на соблюдение прав человека: международные правовые аспекты // Евразия – 2024: правовая и социально-экономическая интеграция в эпоху цифровизации и искусственного интеллекта: материалы Междунар. науч.-практ. конф. 13–14 сентября 2024 г. / Институт права Уфимского ун-та науки и технологии. – 2024. – С. 15–16.

[3] Дорожная карта Генерального секретаря ООН по цифровому сотрудничеству [Электронный ресурс] // Официальный сайт ООН. – URL: https://www.un.org/en/content/digital-cooperation-roadmap/ (дата обращения: 05.05.2025).

сектора, гражданского общества, технического сообщества и других заинтересованных групп.

Внедрение ИИ повлияло на развитие взаимоотношений государств в различных секторах международного права. По мере расширения использования ИИ в международной практике государств, в том числе в цифровой торговле, сделало, как отмечает Джемин Ли, профессор права на юридическом факультете Сеульского национального университета, экстерриториальную юрисдикцию по ряду вопросов дискуссионной[1]. Обусловлено это тем, что влияние цифровой экономики на международное право особенно велико. Бинарное различение товаров и услуг становится затруднительным в условиях цифровой экономики. Цифровой продукт является не только материальным продуктом, но и поставщиком услуг. Меняющийся характер существующих предметов и целей действующих договоров, т.е. объектов международного права, в результате быстрого появления и интеграции технологий и машин ИИ изменяет конструкции устоявшихся правоотношений. Следовательно, по мнению Джемин Ли, потребуется вносить изменения в действующее законодательство о международной торговле[2].

Цифровая экономика не только создает новые возможности[3], она создает опасности для оборота данных и информации[4], которые собираются, обрабатываются и используются без привязки к национальным границам при осуществлении трансграничных транзакций. В связи с этим потребность в новых правовых принципах защиты персональных данных становится растущей реальностью.

Существующий бинарный подход к рассмотрению товаров и услуг как разных целей или предметов, подлежащих торговле, больше не соответствует реальности в контексте зарождающейся цифровой торговли и электронной коммерции, не говоря уже о новых предметах и системах с поддержкой ИИ. Во всяком случае, товары и услуги продаются и потребляются интегрированным об-

[1] См.: Jaemin Lee. Artificial Intelligence and International Law. – 2022. – P. 237.

[2] Ibid. – P. 242.

[3] Xia Lei, Baghaie S., Mohammad Sajadi S. The Digital Economy: Challenges and Opportunities in the New Era of Technology and Electronic Communications // Ain Shams Engineering Journal. – 2024. – Vol. 15, N 2. – P. 8.

[4] Шахназаров Б.А. Право и информационные технологии в условиях современных трансграничных вызовов. – Москва, 2022. – 200 с.

разом как единый предмет торговли. В центре этой новой транзакции лежат данные и информация, коммерческая ценность которых материализуется с помощью ИИ. В новых обстоятельствах рамки существующего дихотомического подхода больше не действуют. Существует своего рода разрыв между нормами и реальностью. Разрыв увеличивается с каждым днем технологических инноваций[1].

Для адаптации к сложившейся ситуации в 2021 г. Генеральный секретарь ООН представил доклад под названием «Наша общая повестка дня», в котором он предложил провести саммит будущего с технологическим направлением, ведущим к Глобальному цифровому договору[2].

22 сентября 2024 г. Генеральная Ассамблея ООН приняла Пакт во имя будущего и приложения к нему, содержащие Глобальный цифровой договор и Декларацию о будущих поколениях (A/RES/79/L.2). Пакт охватывает широкий спектр тем, включая мир и безопасность, устойчивое развитие, изменение климата, цифровое сотрудничество, права человека, интересы молодежи и будущих поколений, а также трансформацию глобального управления[3].

Как отмечает И.А.Умнова-Конюхова, доктор юридических наук, профессор, главный научный сотрудник отдела правоведения ИНИОН РАН, вопросы реализации принципов международного права в Пакте во имя будущего глубоко привязаны к задачам цифровизации и использования ИИ. «Осознавая позитивный вклад цифровых технологий в обеспечение устойчивого развития, мира и безопасности, – пишет автор, – необходимо в то же время учитывать, что внедрение ИИ в разработку и использование вооружений в периоды конфликтов и войн способно усиливать разрушающую составляющую столкновений, затягивать войны и трансформировать их в гибридные войны технологий[4].

---

[1] Jaemin Lee. Artificial Intelligence and International Law. – 2022. – P. 220.

[2] Наша общая повестка дня // Официальный сайт Организации Объединенных Наций. – URL: https://www.un.org/en/common-agenda (дата обращения: 05.05.2025).

[3] Pact for the Future, Global Digital Compact and Declaration on Future Generations. – URL:https://documents.un.org/doc/undoc/gen/n24/272/24/pdf/n2427224.pdf (дата обращения: 12.05.2025).

[4] Умнова-Конюхова И.А. Пакт ООН во имя будущего и взгляд России на новый международный правопорядок // Baikal Research Journal. – 2024. – Т. 15, № 4. – С. 1385.

Аббас Пурхашеми, доктор права, президент Канадского института экспертизы международного права, подчеркивает, что взаимосвязь между ИИ и международным правом начинается с прав человека и уголовного права и заканчивается перспективами торговли и арбитража. Развитие ИИ во многих различных профессиях, услугах и отраслях показывает, что он необходим для нашего нынешнего и будущих поколений. Однако, считает автор, текущая международная правовая база для ИИ недостаточна. Трудность заключается в том, что регулирование ИИ требует обращения к нескольким отраслям права и видам норм, которые подпадают под национальное и международное право[1].

Право прав человека – одна из областей международного права, непосредственно сталкивающаяся со многими новыми вызовами в эпоху ИИ. Появление ИИ не только возбудило дискуссию о субъектах и объектах права, но и актуализировало проблематику «достойной и качественной жизни». Вместе с тем некоторые права стали особо уязвимыми и требуют разработки новых механизмов защиты, дополнительных гарантий – например, права на неприкосновенность частной жизни и защиту данных[2].

Цифровая трансформация нарушает устоявшиеся модели мировой политико-правовой практики, все больше приближая международные отношения к цифровым международным отношениям. Об этом пишут как российские, так и зарубежные исследователи. Так, в монографии «Цифровые международные отношения», подготовленной коллективом российских ученых под редакцией А.А. Байкова и Е.С. Зиновьевой, исследуются влияние цифровизации на экономику, право и международные отношения, а также широкий круг проблем и новых возможностей, возникающих в связи с цифровой трансформацией международных отношений. Авторы отмечают, что цифровые международные отношения формируют новый режим взаимодействия государств. Ученые обращают внимание на деятельность российского промышленного бизнеса в новой международной повестке кибербезопасности; цифровую трансформацию бизнес-моделей и российской национальной платежной системы; санкции. Существенный интерес исследователи проявляют к государственному суверенитету в циф-

[1] Poorhashemi A. Artificial Intelligence and the Future of International Law Bridging Rights, Trade, and Arbitration. – 2024. – 72 p.

[2] Талапина Э.В. Концепция достоинства в цифровую эпоху // Законы России: опыт, анализ, практика. – 2024. – № 8. – С. 83–87.

ровом пространстве и траекториям изменения принципа суверенного равенства государств в цифровой сфере. Отправной точкой изучения принципа суверенного равенства государств в цифровой сфере, по мнению авторов, является то, что два основных подхода к нормативности принципа уважения суверенитета (отрицание или признание его) сходятся на необходимости международного правотворчества, тогда как соответствующей нормы, применимой к информационно-коммуникационным технологиям, не существует[1].

Так, в частности, Е. Зиновьева и С. Шитков, рассмотрев основные проблемы, возникающие на пути обеспечения суверенитета в цифровую эпоху, предлагают развивать функциональную теорию суверенитета. Согласно этой теории, государство наделено множественными полномочиями и компетенциями, защищаемыми международным правом. Соответственно, государственные компетенции не основываются на международном праве, а являются субъективным правом государств осуществлять свою власть в пределах, признанных международным правом. Данная теория помогает сместить акцент с определения «кибергранниц» на реализацию конкретных функций. Более того, с этой точки зрения, по мнению авторов, суверенитет над ИКТ не подразумевает исключительного осуществления суверенитета, позволяя защищаемым этим принципом областям пересекаться и сосуществовать по отношению к разным государствам. Этот подход, подчеркивают они, фокусируется на правах государств на их собственной территории и за рубежом, но не обязывает их воздерживаться от действий, которые могут нарушить суверенитет других государств[2]. В. Русинова при этом отмечает важность принципа суверенного равенства государств[3].

В монографии «Цифровые международные отношения: технологии, агентство и порядок», подготовленной коллективом авторов под редакцией Корнелиу Бьола и Маркуса Корнпробста, ученые прослеживают то, как цифровое развитие меняет международный мир, безопасность и экономику, защиту прав человека и дипломатию и в целом международное право.

[1] Digital International Relations / eds. Andrey Baykov, Elena Zinovieva. – 2023. – P. 73–90. – URL: https://doi.org/10.1007/978-981-99-3467-6 (дата обращения: 12.05.2025).

[2] Ibid. – P. 89–90.

[3] Ibid. – P. 91–105.

В книге раскрывается три аспекта: 1) влияние цифровой революции на международную политику и право; 2) взаимодействие технологий и правопорядка, вопрос о доверии в цифровых пространствах и влияние транснациональных сетей на общество; 3) алгоритмическая безопасность, международная конкуренция и лидерство в цифровой среде, потенциал социальных сетей, цифровая дипломатия, международное право[1].

Представляется, что отдельное внимание в контексте развития правового регулирования цифровых международных отношений следует уделять не только отношениям государств, но и правам человека, особенно в процессе предоставления трансграничных услуг.

Так, Э.В. Талапина обращает внимание на то, что, несмотря на известные преимущества алгоритмов перед человеком, они способны наносить управленческий вред. В отличие от детерминированных систем, основанных на правилах, системы машинного обучения, управляемые данными, являются вероятностными и основываются на статистике. Это значит, что управленческое решение в отношении гражданина становится вероятностным, что увеличивает в том числе дискриминационные риски. В качестве ключевой категории, как замечает Э.В. Талапина, для понимания дискриминационного потенциала алгоритмов в литературе используется косвенная дискриминация, фокусирующаяся на последствиях норм, критериев и практик, которые могут не быть непосредственно дискриминационными (они применяются ко всем без исключения), но оказывают дифференцированное воздействие на лиц из «защищенных» групп. При этом привлечение к ответственности за косвенную дискриминацию, замечает автор, – довольно сложный процесс, требующий соблюдения многих условий[2].

В научной литературе подчеркивается, что ключевым в контексте оценки негативного воздействия ИИ на общественные отношения является признание все более усиливающегося тренда делегирования частным компаниям (разработчикам) решения все более сложных задач и вопросов, касающихся цензуры и контроля ИИ. При этом ООН предостерегает государства от перекладывания столь чувствительных вопросов на плечи частных корпораций

[1] Digital International Relations: Technology, Agency and Order / ed. by Corneliu Bjola, Markus Kornprobst. – 2024. – 312 p.

[2] Талапина Э.В. Дискриминационный потенциал алгоритмов // Административное право и процесс. – 2025. – № 2. – С. 55–58.

и ссылается на рекомендацию Совета Европы о том, что «решение вопросов, касающихся управления с помощью алгоритмов, и/или разработка нормативных положений являются прерогативой государственной политики и не должны отдаваться в распоряжение только частных субъектов»[1].

Технологический прогресс всегда влиял на поведение государств в соответствии с международным правом. Государства, как и любые другие субъекты права, стремятся использовать новые технологии, когда это необходимо. Использование государствами и их правительствами новых технологий само по себе не является чем-то примечательным. Это происходит постоянно и будет продолжаться в будущем.

Соответственно, государство как заинтересованная сторона в области разработки и применения ИИ должно обеспечить безопасность и суверенитет в области экономических отношений, но при этом и создать защищенность трудовых, семейных, миграционных и иных правоотношений отношений, в том числе и путем международного сотрудничества.

Перспективы развития искусственного интеллекта в международных отношениях

Существенные изменения, происходящие в международном сообществе, обусловливают потребность исследовать то, как интерпретируется и применяется действующее международное право и как формулируются и вводятся нормы права в эру ИИ.

Американский футуролог, профессор теоретической физики Митио Каку (Michio Kaku) предсказывает оптимистическое развитие событий. Для повышения достоверности прогнозов он опирается на фундаментальные законы природы (четыре основные силы взаимодействия, управляющие Вселенной) и приходит к выводу, что «правильное» развитие нанотехнологий и инновационных компьютерных коммуникаций должно привести к «формированию планетарной цивилизации» – цивилизации I типа: «Если общество не падет жертвой сил хаоса и глупости, то переход к планетарной цивилизации неизбежен; это конечный продукт действия неумо-

[1] Цит. по: Бегишев И.Р. Международно-правовые основы регулирования искусственного интеллекта и робототехники // Международное публичное и частное право. – 2021. – № 1. – С. 38.

лимых глобальных сил истории и технического развития, не подвластных никому»[1].

По мнению А.Х. Абашидзе, прогнозы по развитию будущего международного права неутешительные. Объясняется это ученым тем, что, несмотря на принятие на уровне интеграционных и иных объединений специальных директив по цифровизации, как это например, имеет место в рамках ЕС (в 2024 г. вступил в силу Регламент (Закон) ЕС об искусственном интеллекте, направленный на улучшение функционирования внутреннего рынка и содействие внедрению ориентированного на человека и надежного ИИ, обеспечивающего при этом высокий уровень защиты здоровья, безопасности, основных прав, а также поддержку инноваций[2]), или же включение в повестку дня вопроса об обмене информации путем цифровых технологий, как, например, в рамках БРИКС, на заключение международных договоров по данной проблематике имеет определенные сложности. В качестве примера автор приводит подписанный в 2024 г. Договор между США, Евросоюзом и Великобританией об использовании ИИ[3]. Договор фокусируется на защите прав человека, которые затрагиваются системами ИИ. В частности, Договор предполагает, что разработчики ИИ обязаны будут внедрять в свой инструмент механизмы оценки, контроля и смягчения рисков, а пользователям дадут возможность подавать жалобы на нарушение технологиями их прав. Договор устанавливает базовые требования для ратифицировавших его государств по принятию или поддержанию соответствующих внутренних законодательных, административных или иных мер для обеспечения того чтобы деятельность в рамках жизненного цикла систем ИИ не только полностью соответствовала правам человека, демократии и верховенству закона, но и уважала семь общих принципов: (1) человеческое достоинство и индивидуальная автономия; (2) прозрачность и надзор; (3) подотчетность и ответственность; (4) равенство и недискриминация; (5) конфиденциальность и защита персональных данных; (6) надежность и (7) безопасные иннова-

[1] Каку М. Физика будущего. – Москва, 2012. – С. 9–10.

[2] Закон ЕС об искусственном интеллекте. – URL: https://oeil.secure.europarl.europa.eu/oeil/en/document-summary?id=1780523 (дата обращения 12.05.2025).

[3] Рамочная конвенция Совета Европы об искусственном интеллекте и правах человека, демократии и верховенстве закона. – URL: https://rm.coe.int/1680afae3c (дата обращения: 12.05.2025).

ции[1]. С точки зрения А.Х. Абашидзе, «если учесть тот факт, что ведущими разработчиками цифровых технологий и продуктов ИИ являются американские, японские и европейские компании, нетрудно догадаться о причине заключения этого Договора, а именно – иметь рычаг конкурентной борьбы в своих странах». Таким образом, замечает ученый, на универсальном уровне отсутствуют предпосылки для принятия какого-либо глобального договора по цифровизации, и международному сообществу еще предстоит договориться о конкретном наборе норм или регламентов по вопросам, связанным с ИИ[2]. На данный момент каждое государство предоставлено самому себе, и сектор ИИ часто сталкивается с коллизиями в праве.

Признавая высокий потенциал новейших технологий, во многих государствах разработаны национальные стратегии развития ИИ, а также его применения. Их основное предназначение – защита национальных интересов, в числе которых защита прав граждан и государственного суверенитета.

Заключение

Обзор научной литературы позволяет сделать вывод о том, что решением различных проблем в области ИИ озадачены все участники международного сообщества. Наиболее часто обсуждаемыми в исследованиях вопросами являются: принципы реализации ИИ и их влияние на отношения между государствами, правовой статус ИИ, его разработчиков – крупных корпораций, которые рассматриваются как «квазисубъекты» международного права, и персонала, связанного с ИИ. Кроме того, ученые отмечают, что не сформировался однозначный ответ на вопросы о том, как регулировать сам ИИ, он является субъектом или объектом права. Ответы на них должно дать законодательство, дополнения и

[1] Евросоюз, Великобритания и США подписывают международный договор, направленный на устранение рисков ИИ. – URL: https://www.clearyiptechinsights.com/2024/09/the-eu-uk-and-us-sign-international-treaty-addressing-risks-of-ai/#_ftn1 (дата обращения: 12.05.2025).

[2] Абашидзе А.Х. Влияние цифровизации жизни общества на соблюдение прав человека: международные правовые аспекты // Евразия – 2024: правовая и социально-экономическая интеграция в эпоху цифровизации и искусственного интеллекта: материалы Междунар. науч.-практ. конф., Ин-т права Уфимского ун-та науки и технологии, 13–14 сентября 2024 г. – 2024. – С. 17–18.

поправки в двусторонние и многосторонние договоры, чтобы учесть новые вызовы, возникающие в связи с ИИ.

ИИ поднимает также множество вопросов в самых разных областях, таких как международное право по правам человека, международное гуманитарное право, международное экологическое право, международное экономическое право и т.д.

Многие государства мира и международные организации признают:

– важность обеспечения условий применения разработки этических норм и принципов в цифровом международном праве;

– необходимость развития сотрудничества в целях формирования универсальных регуляторов в области внедрения, действия и использования технологий ИИ;

– потребность согласованного действия правовых норм, этических долженствований и технических стандартов в области организации и управления ИИ, которые обеспечивают надежное, безопасное и ответственное его использование.

Таким образом, ИИ стал новым объектом права, регулирование которого осуществляется нормами международного и национального права, а его позитивное развитие зависит от слаженного, конструктивного и доверительного международного сотрудничества государств.

УДК 34.096; 341 DOI: 10.31249/iajpravo/2025.03.07

СКУРКО Е.В.[1] МЕЖДУНАРОДНОЕ ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПЕРВЫЕ ШАГИ МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ (Обзорная статья)

Аннотация. Искусственный интеллект повсеместно в мире приобретает все более важную роль в общественной жизни. В статье анализируется международно-правовое развитие регулирования ИИ, принципы и подходы к формированию международного права искусственного интеллекта, основные направления международного сотрудничества в сфере искусственного интеллекта. Рассматриваются первые акты в области ИИ, принятые Организацией Объединенных Наций, ЮНЕСКО, ОЭСР и др.

Ключевые слова: международное право; искусственный интеллект; международно-правовое регулирование; Организация Объединенных Наций; ЮНЕСКО; ОЭСР; будущее международного права.

SKURKO E.V. International Legal Regulation of Artificial Intelligence: the First Steps of International Organizations (Review article)

Abstract. Artificial intelligence is becoming increasingly important in public life throughout the world. The article analyzes the international legal development of regulation and principles and approaches to the formation of the international law of artificial intelligence, the main directions of international cooperation in the field of artificial intelligence. The first acts in the field of AI adopted by the United Nations, UNESCO, OECD, etc. are being considered.

[1] *Скурко Елена Вячеславовна*, старший научный сотрудник отдела правоведения ИНИОН РАН, кандидат юридических наук.

Keywords: international law; artificial intelligence; international legal regulation; United Nations; UNESCO; OECD; the future of international law.

Для цитирования: Скурко Е.В. Международное правовое регулирование искусственного интеллекта: первые шаги международных организаций (Обзорная статья) // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. Государство и право. – 2025. – № 3. – С. 90–104. – DOI: 10.31249/iajpravo/2025.03.07

Введение

Технологический прогресс и появление ИИ в значительной степени изменяют нашу жизнь и обусловливают особое внимание международных и национальных правотворческих органов к вопросам регулирования внедрения ИИ в различные области человеческой деятельности. Важную роль в развитии правового регулирования в области ИИ призваны играть международные организации – прежде всего ООН и ее специализированные учреждения. Определенные результаты в этом направлении достигнуты ГА ООН, ЮНЕСКО, ИКАО, МОТ, ВОЗ и др. Ежегодно ООН публикует доклады о деятельности органов и учреждений ООН по вопросам ИИ, тенденциях и стандартизации инструментов ИИ – «Отчеты ООН о деятельности в области искусственного интеллекта» (the UN Activities Report on Artificial Intelligence)[1]; 20 сентября 2024 г. был выпущен очередной «Отчет об оперативном использовании искусственного интеллекта в системе ООН»[2].

В декабре 2023 г. Генеральный секретарь ООН созвал Консультативный совет высокого уровня по ИИ с участием заинтересованных сторон, который к концу года представил промежуточный отчет «Управление искусственным интеллектом в интересах человечества», содержащий аргументы в пользу создания наднациональной структуры для системного контроля ООН за внедре-

[1] Ежегодные Отчеты ООН о деятельности в области искусственного интеллекта – United Nations Activities on Artificial Intelligence (AI) (2018–2023). – URL: https://www.itu.int/pub/S-GEN-UNACT (дата обращения: 20.04.2025).

[2] Report on the Operational Use of AI in the UN System / United Nations System HLCM Task Force on the Use of Artificial Intelligence in the UN System 20/09/2024. – URL: https://unsceb.org/sites/default/files/2024-11/Report%20on%20the%20Operational%20Use%20of%20AI%20in%20the%20UN%20System_1.pdf (дата обращения: 20.04.2025).

нием ИИ и заключения специального международного соглашения[1].

Первые исторические документы Генеральной Ассамблеи ООН и ЮНЕСКО в области искусственного интеллекта

В 2024 г. на площадке ООН было принято два документа, посвященных вопросам ИИ. В марте 2024 г. ГА ООН была принята Резолюция «Использование возможностей безопасных, защищенных и надежных систем искусственного интеллекта для устойчивого развития»[2], разработанная при участии 120 государств, которые «решили управлять искусственным интеллектом и не допустить, чтобы он управлял людьми»; преодолеть разрыв между странами и внутри стран в области ИИ и других цифровых технологий»; «содействовать развитию безопасных, защищенных и надежных систем искусственного интеллекта для ускорения прогресса в деле полной реализации Повестки дня в области устойчивого развития на период до 2030 года»[3]. Резолюция призывает к наращиванию международного сотрудничества в области ИИ (обмен знаниями, равный доступ к новейшим технологиям, увеличение финансирования исследований в сфере ИИ), в том числе для обеспечения равного доступа к инновациям. Документ содержит перечень мер, направленных на разработку и внедрение надежных и заслуживающих доверия систем ИИ, в том числе: повышение осведомленности граждан о возможностях систем ИИ; создание механизмов оценки воздействия и мониторинга рисков ИИ, маркировки цифрового контента, возмещения ущерба и привлечения к ответственности, обмена информацией между заинте-

[1] В ООН представили план по управлению искусственным интеллектом. – URL: https://news.un.org/ru/story/2024/09/1456466 (дата обращения: 20.04.2025).

[2] 2024 Резолюция ГА ООН «Использование возможностей безопасных, защищенных и надежных систем ИИ для устойчивого развития» / Seizing the opportunities of safe, secure and trustworthy AI Systems for Sustainable Development. – URL: https://ai.gov.ru/knowledgebase/mezhdunarodnye-dokumenty-po-razvitiyu-ii/2024_rezolyuciya_ispolyzovanie_vozmoghnostey_bezopasnyh_zaschischennyh_i_nadeghnyh_sistem_ii_dlya_ustoychivogo_razvitiya_seizing_the_opportunities_of_safe_secure_and_trustworthy_ai_systems_for_sustainable_development_generalynaya_assambleya_oon/ (дата обращения: 20.04.2025).

[3] Там же.

ресованными сторонами; обеспечение прозрачности систем ИИ; сохранение культурного и языкового многообразия и др.[1]

1 июля 2024 г. ГА ООН единогласно приняла инициированную Китаем Резолюцию «Об укреплении международного сотрудничества в области наращивания потенциала искусственного интеллекта»[2]. В Резолюции подчеркивается, что ИИ должен развиваться на «человеко-ориентированных принципах», приносить пользу человечеству; призывает к международному сотрудничеству и практическим действиям, чтобы помочь всем, особенно развивающимся странам, укрепить свой потенциал в области ИИ. Резолюция выступает за «открытую, справедливую и недискриминационную деловую среду» и поддержку ООН в сфере наращивания потенциала ИИ, направлена на достижение инклюзивного, полезного и устойчивого развития ИИ, способствуя реализации Повестки ООН в области устойчивого развития на период до 2030 г.[3]

В ноябре 2021 г. ЮНЕСКО утвердила первый в истории глобальный стандарт по этике ИИ – «Рекомендацию об этических аспектах искусственного интеллекта», которую приняли все 193 государства – члена ООН[4]. Цели Рекомендации – заложить основу, которая позволит использовать ИИ на благо всего человечества, отдельного человека, сообществ, окружающей среды и экосистем и не допустить причинения им вреда, стимулировать использование систем на основе ИИ в мирных целях, помочь заинтересованным сторонам реализовать принцип совместной ответственности на основе глобального межкультурного диалога. Рекомендация предлагает разработать согласованный на глобальном уровне нормативный инструмент, содержащий ценностные этические установки и принципы деятельности в сфере ИИ[5].

---

[1] Там же.

[2] Генеральная Ассамблея ООН приняла предложенную Китаем резолюцию об укреплении международного сотрудничества в области наращивания потенциала ИИ // Российская газета. – 2024. – 2 июля. – URL: https://rg.ru/2024/07/02/generalnaia-assambleia-oon-priniala-predlozhennuiu-kitaem-rezoliuciiu-ob-ukrepleniimezhdunarodnogo-sotrudnichestva-v-oblasti-narashchivaniia-potenciala-ii.html (дата обращения: 20.04.25).

[3] Там же.

[4] Рекомендация об этических аспектах искусственного интеллекта / ЮНЕСКО SHS/BIO/REC-AIETHICS/2021. – 2021. – URL: https://unesdoc.unesco.org/ark:/48223/pf0000380455_rus (дата обращения: 20.04.2025).

[5] Там же.

Так, в мировом и научно-практическом сообществе все прочнее утверждается позиция, что в настоящее время зарождается международное «право искусственного интеллекта», которое представляет собой комбинацию «жесткого» и «мягкого» права, возникающего в результате комплексного развития и внедрения ИИ в социальной практике.

Направления международно-правового сотрудничества в сфере применения искусственного интеллекта

Международные требования и стандарты, предъявляемые к ИИ, лучше понятны, если рассматривать ИИ в рамках международной деятельности и отношений, охватывающих различные международно-правовые сферы сотрудничества и правовые режимы.

Международная торговля товарами и услугами

Всемирная торговая организация (ВТО) прогнозирует, что цифровые технологии, одним из компонентов которых является ИИ, повлияют на торговлю товарами и услугами несколькими способами[1]. Это – снижение издержек в международной торговле; изменение структуры торговли, сопровождающееся увеличением объема торговли цифровыми услугами; изменения в структуре торговли товарами. Так, снижение торговых издержек частично происходит за счет снижения транспортных расходов. В этой сфере ИИ внедряется во всех видах транспорта, таких как автомобили, грузовики, поезда и суда, для управления эксплуатацией и маршрутами этих транспортных средств, а также в их вспомогательной инфраструктуре. Особый интерес представляет разработка автономных судов и грузовых самолетов. Такие приложения ИИ требуют внимания в международном праве и международных отношениях, поскольку суда, беспилотные летательные аппараты и, в меньшей степени, иные транспортные средства будут пересекать международные границы или, в случае судов, действовать в открытом море и пересекать границы внутренних вод.

Что касается структуры международной торговли, то ВТО ожидает, что торговля товарами в области информационных тех-

[1] Trading with Intelligence: How AI Shapes and is Shaped by International Trade / WTO. – Geneva, 2024. – 118 p. – URL: https://www.wto.org/english/res_e/booksp_e/trading_with_intelligence_e.pdf (дата обращения: 20.04.2025).

нологий, таких как компьютеры и полупроводники, будет расширяться. Другие технологии, такие как блокчейн, облегчат торговлю товарами, к которым предъявляются требования по срокам годности; товарами, к которым предъявляются требования по сертификации и маркировке; товарами, продажа которых регулируется группами контрактов, например коносаментами, договорами перевозки и т.п., используемыми при международной продаже товаров; товарами, подлежащими таможенному оформлению. Развитие 3D-печати может привести к сокращению торговли некоторыми товарами, поскольку их можно будет производить в большем количестве внутри стран, а развитие бизнес-моделей, таких как совместное использование транспортных средств, может снизить спрос на товары длительного пользования вроде как автомобилей. ВТО прогнозирует, что цифровые технологии повысят важность прав интеллектуальной собственности по мере того, как все больше цифровых продуктов будут передаваться по лицензии, а не продаваться[1].

ВТО предполагает, что с развитим цифровой экономики у менее развитых стран появится конкурентное преимущество в сфере труда. Но, с другой стороны, цифровые технологии и ИИ требуют более высококвалифицированной рабочей силы, и в той мере, в какой они заменяют рабочую силу, в некоторых отраслях и на производствах, где применяется ИИ, те становятся более капиталоемкими. Наконец, поскольку ИИ в значительной степени опирается на данные, фирмы в странах с большим населением и рынками, которые служат источниками данных, будут иметь конкурентное преимущество перед фирмами с небольших рынков[2].

Международные финансовые операции

Приложения ИИ в сфере финансов в основном внедряются на национальном уровне. Однако некоторые приложения затрагивают системные аспекты финансов, которые могут иметь международное значение. Например, это использование ИИ для оценки соответствия банков стандартам достаточности капитала. В разработке находятся вопросы, каким образом ИИ может использоваться в различных аспектах платежных систем. При соответствующем

[1] Ibid. См. также: Chinen M. The International Governance of Artificial Intelligence. – 2023. – P. 14.

[2] Ibid.

обучении ИИ может найти применение для прогнозирования международных потоков капитала. В настоящее время на стадии разработки находится 38 моделей ИИ, которые помогут принимать торговые и инвестиционные решения, оценивать риски и управлять ими[1].

Международные потоки рабочей силы

У международного сообщества существует некоторая обеспокоенность по поводу вытеснения рабочей силы искусственным интеллектом; опасения, что автоматизация лишит людей работы. Контраргументом, по мнению исследователей, является то, что новые технологии улучшают условия человеческого труда либо позволяют осваивать новые отрасли, которые благодаря технологиям стали более производительными и эффективными, а это приводит к росту спроса на рабочую силу. Таким образом, хотя некоторые профессии, особенно требующие низкой квалификации, подвержены риску сокращения, это не относится к большинству профессий. Отличительная проблема, связанная с ИИ, заключается в том, что приложения ИИ обладают возможностями, которые, как ранее считалось, присущи исключительно людям, поэтому даже профессии, требующие больших навыков и специальных знаний, могут оказаться в сфере конкуренции с ИИ[2].

Международный мир и кибербезопасность

Сегодня в мире идут исследования и разработки в области ИИ и автономных систем для ведения боевых действий. Цель состоит в том, чтобы ИИ поддерживал и оценивал военную оперативную обстановку, планирование и проведение военных операций. Предполагается использование автономных и полуавтономных систем с возможностью обучения, а также приложений ИИ для киберзащиты и др. Это направление включает в себя использование систем компьютерного зрения (computer vision systems), помогающих аналитикам распознавать потенциальные цели, прогнозировать потребности в техническом обслуживании оборудования и глубоком обучении для обнаружения ранее неизвестных угроз.

[1] Ibid. – P. 16.

[2] Ibid. – P. 17–18.

Использование ИИ в военных целях вызывает, по крайней мере, две проблемы для международного мира и безопасности. Во-первых, ИИ улучшает все аспекты военной стратегии и операций, но при этом наибольшее внимание уделяется смертоносным автономным системам вооружения (LAWS). Хотя принято считать, что «роботы-убийцы» – пока перспектива отдаленного будущего, тем не менее есть опасения, что автономное оружие произведет революцию в военном деле, позволит вести войну быстрее и в большем масштабе. Кроме того, автономное оружие может быть использовано в качестве средства устрашения и, значит, сделает «асимметричную войну» более смертоносной и доступной для субгосударственных и негосударственных субъектов.

Во-вторых, большую обеспокоенность вызывают кибератаки на правительственные учреждения, предприятия, поскольку они наносят ущерб интересам национальной безопасности. Поскольку ИИ способен повысить эффективность всех видов военной деятельности, правительства вынуждены разрабатывать и внедрять приложения ИИ в оборонной сфере, по крайней мере для сохранения своих относительных стратегических позиций. То есть, ИИ может оказывать в целом дестабилизирующее воздействие и приводить к необходимости пересматривать прежние стратегии (государственной) безопасности. Даже если применение ИИ не станет дестабилизирующим, оно станет фактором гонки инноваций по другим военным технологиям – таким как «роевые» технологии, гиперзвуковые ракеты и т.п., что отразится на международной стабильности[1].

По мнению ряда авторов, внедрение ИИ станет фактором, увеличивающим риск дестабилизации ядерного сдерживания. Другие исследователи, напротив, утверждают, что ИИ будет служить фактором повышения ядерной стабильности, например за счет улучшения качества систем раннего предупреждения и предотвращения ложных срабатываний систем обнаружения ядерных атак[2].

[1] Chinen M. Op. cit. – P. 19–20.

[2] Johnson J.S. Artificial Intelligence: A Threat to Strategic Stability // Strategic Studies Quarterly. – 2020. – Vol. 14. – URL: https://abdn.elsevierpure.com/en/publications/artificial-intelligence-a-threat-to-strategic-stability (дата обращения: 20.04.2025); Cox J., Williams H. The Unavoidable Technology: How Artificial Intelligence // The Washington Quarterly. – 2020. – 16 Jun. – URL: https://www.tandfonline.com/doi/full/10.1080/0163660X.2021.1893019 (дата обращения: 20.04.2025).

На практике системы ИИ часто имеют двойное назначение и могут использоваться как во вред, так и во благо; они эффективны и масштабируемы, могут превосходить возможности человека; системы ИИ могут повысить анонимность и психологическую дистанцию между преступниками и их жертвами; приложения ИИ сравнительно легко распространять и т.п. Поэтому небезосновательны опасения, что ИИ позволит большему числу акторов осуществлять разного рода вредоносные атаки, увеличит их частоту и расширит число потенциальных целей. Более того, ИИ будет создавать угрозы, которые не могут быть созданы человеком, такие как вредоносное программное обеспечение и «рои»; характер атак при применении ИИ изменит их качественно и количественно, они могут стать более регулярными, более целенаправленными, их будет труднее отслеживать. Кроме того, системы ИИ имеют свои уникальные уязвимости – из-за их зависимости от данных и способа обучения моделей, особенностей функционирования, что может создавать новые виды угроз и причинять новые виды ущерба[1].

Окружающая среда и изменение климата

Искусственный интеллект используется для решения проблем, связанных с охраной окружающей среды. ИИ позволяет осуществлять мониторинг изменений климата и его моделирование; прогнозирование климатических сценариев; контроль и сокращение выбросов парниковых газов, переход на более устойчивые источники энергии; смягчение и адаптацию к последствиям климатических изменений. Вместе с тем инфраструктура, поддерживающая ИИ, может оказывать негативное воздействие на окружающую среду. Так, для обучения ИИ требуется большое количество энергии; устройства и оборудование, управляемые ИИ, создают проблемы с потреблением энергии и электронными отходами; крупные центры, где физически хранятся данные для облачных вычислений и других приложений ИИ, предъявляют высокие требования к энергии, а также к воде для охлаждения. В одном из исследований было подсчитано, что в 2018 г. на серверы обработки данных приходилось около 1% мирового потребления энергии.

[1] Chinen M. Op.cit. – P. 21.

Ожидается, что доля потребления энергии в связи с ИИ будет нарастать[1].

Международное общественное здравоохранение

В области глобального здравоохранения есть надежда, что ИИ может быть использован для удовлетворения потребностей в здравоохранении в странах с низким и средним уровнем дохода. Приложения ИИ потенциально могут быть использованы для улучшения здоровья населения, отдельных людей, качества систем здравоохранения, фармацевтики и медицинских технологий. Однако для обеспечения того, чтобы технологии ИИ разрабатывались и внедрялись справедливо и надлежащим образом, необходимо развитие государственного управления и правового регулирования в данном вопросе[2].

Субъекты и ландшафт международного регулирования искусственного интеллекта

Различные субъекты вносят свой вклад в разработку нормативного регулирования ИИ на международном уровне. Во-первых, это – государства и группы международных (межгосударственных) организаций; во-вторых – частные фирмы; в-третьих – неправительственные организации (НПО). Каждый из этих трех типов субъектов обладает различной компетенцией, необходимой для введения нормативного регулирования: независимостью, репрезентативностью, опытом и оперативным потенциалом – и никто из них не обладает всеми компетенциями в необходимом объеме для полноценного регулирования ИИ[3].

Специалистами было выявлено 634 программы мягкого права (soft law ‘programs’), которые применяются в сфере регулирова-

[1] Recalibrating Global Data Center Energy-Use Estimates / E. Masanet, A. Shehabi, N. Lei, S. Smith, J. Koomey // Science. – 2020. – Vol. 367, N 6481. – P. 984–986. – URL: https://www.science.org/doi/10.1126/science.aba3758#BIBL (Дата обращения: 20.04.2025).

[2] Chinen M. Op. cit. – P. 23; Коданева С.И. Правовые аспекты использования метавселенной в медицине и здравоохранении (Статья) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2025. – № 2. – С. 51–65.

[3] Ibid. – P. 39–40.

ния ИИ[1]. «Мягкое право ИИ» принимает формы рекомендаций и стратегий, принципов, стандартов, профессиональных руководств и кодексов поведения, партнерств, сертификационных или добровольных программ, добровольных мораториев и, наконец, запретов (ban)[2].

Большинство из программ мягкого права в сфере ИИ – это рекомендации и стратегии (54,26%), а также принципы (25%); около 9,5% программ составляют стандарты; остальные формы – это профессиональные руководства или кодексы поведения, партнерства, сертификационные или добровольные программы, добровольные моратории или запреты (3,6%, 3,3%, 2,5% и 1,9% соответственно). Содержательно международное регулирование ИИ затрагивает: этические принципы; моратории и запреты; данные и обучение алгоритмов; контроль со стороны человека; критерии объяснимости и прозрачности работы ИИ; тестирование[3].

Принципы и стратегии государств в области искусственного интеллекта, разработанные Организацией экономического сотрудничества и развития и национальная практика их реализации

В 2019 г. ОЭСР разработала, а в 2024 г. внесла дополнения в Рекомендации Совета по искусственному интеллекту (Recommendation of the Council on Artificial Intelligence), определяющие «Принципы искусственного интеллекта ОЭСР» (OECD AI Principles)[4], основу которых составляет принцип поощрения заслуживающего доверия ИИ, уважающего права человека и демократические ценности.

В рамках своей деятельности Обсерватория ОЭСР по разработке политики в области ИИ подразделяет национальную политику и стратегии государств в области ИИ на четыре типа: 1) «управление в целом» (governance in general) (национальные

[1] Gutierrez C.I., Marchant G. A Global Perspective of Soft Law Programs for the Governance of Artificial Intelligence. – 2021. – 64 p.

[2] Ibid.

[3] Chinen M. Op. cit. – P. 58–67.

[4] OECD/LEGAL/0449 Recommendation of the Council on Artificial Intelligence. – URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (дата обращения: 20.04.2025); OECD AI Principles. – URL: https://oecd.ai/en/ai-principles (дата обращения: 20.04.2025).

стратегии, органы координации или мониторинга, общественные консультации с заинтересованными сторонами, использование ИИ в государственном секторе); 2) «финансовая поддержка» (институциональное финансирование государственных исследований, различного рода гранты, закупки, долевое финансирование и образовательные кредиты, стипендии); 3) «стимулирование ИИ» (AI enablers and other incentives) (научные и инновационные задачи, награды и гранты, программы создания сетей и сотрудничества, платформы и инфраструктура ИИ, доступ к данным, кампании по информированию общественности, навыки и образование в области ИИ); 4) «руководство и регулирование» (формирование нормативного регулирования и регулирующих органов, а также органов по надзору за соблюдением этических норм). В 2022 г. веб-сайт ОЭСР содержал данные по более чем 700 принятым различными государствами политическим инициативам в области ИИ – из 60 стран и Евросоюза. Обсерватория ОЭСР предоставляет доступ к 171 национальной стратегии, повесткам дня и планам, разработанным национальными правительствами[1].

Государственные стратегии в сфере ИИ развиваются под влиянием культуры и традиционных ценностей на управление новыми технологиями. В разработке ряда национальных стратегий можно отметить значительный уровень участия частного предпринимательского сектора и коммерческих компаний, что обусловлено высокой ролью частного сектора в разработке и коммерциализации продуктов с ИИ[2].

Показателен опыт Китая в области стратегий ИИ. За последние пять лет Китай занял одно из ведущих мест в области международного управления ИИ и внедряет ИИ для продвижения национальной политики в трех областях: международная конкуренция, экономическое развитие и социальное управление (international competition, economic development, and social governance). Китай считает, что развитие ИИ будет способствовать росту его ВВП на 26% и занятости на 12% в течение 20 лет. Национальная стратегия ИИ Китая заложена в Национальный план ИИ нового (или следующего) поколения 2017 г. (the 2017 National New (or next)

[1] OECD.AI Policy Observatory, National AI policies & strategies. – 2021. – URL: https://oecd.ai/en/dashboards (дата обращения: 20.04.2025).

[2] Также см.: Chinen M. Op. cit. – P. 141.

Generation AI Plan)[1]. В этом Плане Китай ставит перед собой цель стать мировым лидером в области теории, технологий и приложений ИИ к 2030 г.

Хотя план разработан центральным правительством, ожидается, что реальные инновации и преобразования будут осуществляться частным сектором и местными органами власти. В частном секторе Планом определены национальные лидеры в области ИИ, которые согласились на дальнейшее развитие в русле стратегических целей правительства. Взамен такие ИИ-компании получат льготные условия для заключения контрактов, более легкий доступ к финансированию, а иногда и защиту доли рынка. План предусматривает стимулы для местных органов власти оказывать содействие в развитии ИИ. С этой целью Китай, согласно прогнозам, инвестирует 1,6 трлн долл. США в разработку ИИ. Это уже позволило создать пилотные зоны для тестирования разработок ИИ и т.п.[2]

Искусственный интеллект и будущее международного права

Расширяющееся применение ИИ порождает многочисленные глобальные возможности и вызовы, с которыми сталкивается международное право. От нарушений прав человека до облегчения диагностики состояния здоровья, от угроз трудоустройству до обеспечения взаимодействия людей через социальные сети – лишь малые примеры применения этой новой технологии в современном обществе, и в любом случае следует признать, что проблемы, связанные с ИИ, требуют ответа со стороны международного права.

Международное право предусматривает разнообразные стандарты в области ИИ, множество способов его использования, но вместе с тем до сих пор отсутствует универсальное определение ИИ и его регулирование. Существующая международно-правовая база, по оценке экспертов, для ИИ недостаточна. Сложность заключается в том, что регулирование ИИ требует обращения к нескольким отраслям права и типам норм, которые подпадают под действие национального и международного права.

[1] Full Translation: China's 'New Generation Artificial Intelligence Development Plan'. – 2017. – URL: https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/ (дата обращения: 20.04.2025).

[2] Chinen M. Op.cit. – P. 143.

Разработка и внедрение международных нормативных актов, регулирующих использование технологий ИИ, имеет решающее значение для будущего развития международного права. В ответ на проблемы, с которыми сталкивается ИИ, некоторые государства и международные организации самостоятельно ищут правовую базу для минимизации рисков, связанных с ИИ.

По мнению специалистов, сегодня назрела необходимость, чтобы международное сообщество создало универсальный механизм, занимающийся искусственным интеллектом. Глобальный институт может консультировать и помогать государствам и международным организациям в разработке и внедрении международных норм и правил[1].

Большинство инициатив в области ИИ, разработанных во всем мире за последние годы, в основном осуществлялись без надзора регулирующих органов, не обладали достаточной юридической силой. За исключением этических норм, законодателям во всем мире еще предстоит разработать комплексные подходы в правовом регулировании ИИ.

Для будущих исследований, касающихся ИИ и международного права, важно учитывать, что государства и международные организации в настоящее время берут на себя добровольные обязательства, основанные на этических принципах и технических стандартах, по защите прав человека, эволюции мягкого права и, поощрению развития национального законодательства и, наконец, нормативного развития путем принятия и осуществления международных договоров и конвенций, регулирующих использование ИИ[2].

Регулирование ИИ в международном праве, как сходятся во мнении специалисты, следует развивать в отраслевом ключе: ИИ и права человека; ИИ и международное уголовное право; ИИ и международное торговое право; ИИ и международный арбитраж – и другим отраслям[3].

Заключение

Развитие международно-правового регулирования ИИ – одна из актуальных задач, решение которой пока не найдено. Вместе

[1] Artifcial Intelligence and the Future of International Law: Bridging Rights, Trade, and Arbitration / ed. A. Poorhashemi. – 2024. – P. 61.

[2] Ibid. – P. 62–63.

[3] Ibid. – P. IX.

с тем практика показывает эффективность подхода, сочетающего «жесткое» и «мягкое» право в сфере ИИ, в том числе, поскольку развитие технологий ИИ происходит в трансграничном пространстве, с высокой долей участия «частной сферы» и предпринимательства. Роль публично-правового регулирования, как в международном праве, так и в национальных правовых системах в большей части обусловлена требованием защиты прав человека, его персональных данных, конфиденциальности и недискриминации в цифровой среде.

УДК 342, 343; 34.096 DOI: 10.31249/iajpravo/2025.03.08

ЗАХАРОВ Т.В.[1] ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА СИСТЕМУ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ВООРУЖЕННЫЕ КОНФЛИКТЫ (Обзор)

Аннотация. В обзоре представлены позиции российских и зарубежных ученых по отдельным вопросам международной информационной безопасности, в том числе различия в стратегиях США и России в этой области международного права. Рассматриваются вопросы применения технологий искусственного интеллекта в сфере национальной безопасности и в случае вооруженных конфликтов, проблемы злонамеренного использования искусственного интеллекта в целях изменения баланса сил в международной системе безопасности и юридической ответственности в области использования искусственного интеллекта в военных целях.

Ключевые слова: международное право; международная информационная безопасность; национальная безопасность; искусственный интеллект; автономные системы вооружения.

ZAKHAROV T.V. The Impact of the Artificial Intelligence on International Information Security System and Armed Conflicts (Review)

Abstract. The review presents the positions of Russian and foreign scientists on certain issues of international information security, including differences in the strategies of the United States and Russia in this area of international law. The issues of the use of artificial intelligence technologies in the field of national security and in the event of military conflicts, the problems of the malicious use of artificial intelligence in order to change the balance of power in the international secu-

[1] *Захаров Тимофей Владимирович* – научный сотрудник отдела правоведения ИНИОН РАН.

rity system and legal responsibility in the field of the use of artificial intelligence for military purposes are considered.

Keywords: international law; international information security; national security; artificial intelligence; autonomous weapons systems.

Для цитирования: Захаров Т.В. Влияние искусственного интеллекта на систему международной информационной безопасности и вооруженные конфликты (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2025. – № 3. – С. 105–117. – DOI:10.31249/iajpravo/2025.03.08

Введение

На фоне стремительного развития информационно-коммуникационных технологий (ИКТ) и процессов глобализации актуальность вопросов информационной безопасности стала особенно очевидной, как и то, что практически каждая страна использует ИКТ в военно-политических и экономических целях. На наших глазах проходят противоборства стран в киберпространстве и информационные войны государств, которые включают проведение компьютерных атак на государственные ресурсы других стран, проведение в глобальном информационном пространстве действий, которые мешают стабильности, безопасности и поддержанию международного мира [1, с. 116].

Сегодня системы международной информационной безопасности подвергаются сложной проверке широким внедрением ИИ в экономическую и военную сферы. Использование ИИ, в частности, в военных целях зачастую опережает не только правовое регулирование, но и прогнозирование возможных последствий. В связи с этим внимание ученых сосредоточено на сложных вопросах юридической, международно-правовой ответственности.

В обзоре рассматриваются стратегии России и США в сфере международной информационной безопасности, влияние внедрения технологий ИИ на системы международной безопасности и их нормативные основы, предпосылки юридической ответственности за применение ИИ в военных целях.

Сходства и различия в стратегиях США и России в сфере международной информационной безопасности

Как показали результаты исследования, проведенные М.Р. Загайновым, доцентом кафедры правового регулирования экономи-

ческой деятельности юридического факультета Финансового университета при Правительстве РФ, США стремятся стать единственным лидером в глобальном информационном пространстве и подчинить себе другие страны, в то время как Россия организует международный диалог по информационной безопасности и сотрудничеству с другими странами, вовлекая их в качестве партнеров [1, с. 117].

После создания сети Интернет США локализовали управление этой Сетью преимущественно на своей территории. Придание ей глобального характера позволяет США использовать свое доминирование для решения собственных, в том числе силовых задач, как то: организация масштабных разведывательных операций и проведение компьютерных атак на критическую информационную инфраструктуру суверенных государств. Как отмечает М.Р. Загайнов, для сохранения своей лидирующей позиции США пытается принять всевозможные меры для изоляции информационного пространства от неугодных стран, меняя ранее установленные подходы. Чтобы противостоять этому, Россия неоднократно выступала за введение регулирования для обеспечения международной информационной безопасности [там же, с. 117].

Россия, констатирует М.Р. Загайнов, последовательно реализует свой подход к ответственному поведению государств в цифровой среде, как на своей территории, так и во внешней политике. В частности, 26 мая 2021 г. на заседании ООН была принята предложенная Россией резолюция 75/282 «Противодействие использованию информационно-коммуникационных технологий в преступных целях». В это же время была завершена деятельность рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ, созданной по российской инициативе еще в 2018 г. Ее итоговый доклад включает рекомендации о необходимости продолжить переговорный процесс по международной информационной безопасности под эгидой ООН в ближайшие пять лет.

Развивая идею объединения стран в сфере обеспечения международный информационной безопасности, Россия предложила создать реестр контактных пунктов, чтобы наладить прямую связь между компетентными органами стран. Это могло бы не только помочь своевременному реагированию на компьютерные атаки, но и значительно снизить напряженность в случае неправильного понимания киберинцидентов [там же, с. 119].

Американский подход к информационной безопасности в киберпространстве

Подход США к безопасности в киберпространстве, по мнению М.Р. Загайнова, кратко можно назвать: «лучшая форма защиты – нападение». Основная идея нормативно-правового регулирования в США вопросов кибербезопасности сводится к информационному господству [там же, с. 119–120].

В это же время Соединенные Штаты совместно с более чем 55 странами подписали в 2022 г. Декларацию о будущем Интернета, разработанную в США. Эти государства, согласно Декларации, выступают против подавления свободы выражения мнений, цензуры независимых новостных источников, продвижения дезинформации, вмешательства в выборы других стран. Как отмечает заместитель секретаря Совета безопасности РФ О.В. Храмов, «подписанты Декларации фактически делегировали Вашингтону свое суверенное право на обладание национальной информационной инфраструктурой, поскольку корпорация по управлению доменными именами и IP-адресами (ICANN), на которую возложены контрольные функции над глобальной сетью, на практике полностью подчинена американскому правительству» [цит. по: 1, с. 120]. По сути, считает Загайнов, данный документ наделяет США монополией в области регулирования и позволяет Вашингтону подмять под себя информационные инфраструктуры суверенных государств [там же, с. 120].

Одной из наиболее актуальных проблем в сфере международной информационной безопасности можно назвать односторонние киберсанкции США. Так, США ограничили импорт высокотехнологичной продукции в Россию и запретили участие России во Всемирном мобильном конгрессе. В июне 2022 г. Белый дом заявил, что сведет на нет сотрудничество в области технологий и науки с государственными российскими исследовательскими учреждениями и лицами, связанными с ними [там же, с. 122].

Искусственный интеллект как фактор изменения баланса сил в международной системе информационной безопасности

Одной из проблем в области мировой информационной безопасности нового поколения можно назвать злонамеренное использование искусственного интеллекта, например, для упрощения практик дезинформации с помощью создания фейковых

аудиоклипов и видеороликов. Также отмечается использование технологий ИИ для осуществления пропагандистской деятельности террористическими организациями [1, с. 122].

В связи с этим, именно ИИ рассматривается в качестве фактора изменения баланса сил в системе международной информационной безопасности. При этом решения алгоритма ИИ заранее предугадать невозможно [там же, с. 122].

При этом Госдеп США с 2022 г. уже использует ИИ и другие передовые ИТ-технологии для пропаганды против России и Китая. По заявлению Госсекретаря США Э. Блинкина, Соединенные Штаты используют ИИ для сбора доказанных фактов российской дезинформации, чтобы сообщить о ней партнерам по всему миру. В 2024 г. администрация президента Д. Байдена заявила о том, что рассматривается возможность по ограничению доступа к развитым моделям ИИ России, Китая и некоторых других стран. По сути, США открывает новый фронт с целью оградить ряд стран от американских технологий ИИ [там же, с. 122].

Способность разрабатывать и внедрять новейшие технологии, в том числе ИИ, рассматриваются М. Горовицем, профессором Пенсильванского университета (США), Ш. Пиндайк, исследователем в области технологий и международной безопасности Института глобальных конфликтов и сотрудничества Калифорнийского университета (США), Ливерморской и Лос-Аламосской национальных лабораторий (США) и К. Махони, докторантом факультета политических наук Пенсильванского университета, исследователем Вашингтонского центра новой американской безопасности (Center for a New American Security (CNAS)). Государства, стремящиеся быть на шаг впереди других, часто ищут стратегии, использующие новые технологии для усиления своей способности оказывать влияние на международной арене, подчеркивают они [2, p. 914].

В зависимости от того, как используются достижения ИИ в военной сфере, здравоохранении, образовании, производстве, финансах, социальных службах и других видах деятельности, зависит национальное могущество государства. Однако быстрые темпы внедрения ИИ во многих сферах затрудняют прогнозирование его влияния на глобальный баланс сил. Различия – в том, как национальные экономики и вооруженные силы используют ИИ сегодня. По мнению авторов, применение ИИ усугубляет неопределенность в отношении как возможностей, так и уязвимостей, которые ИИ создает для государств, стремящихся к власти [Ibid, p. 914].

Факторы, такие как внешняя и организационная среда, отношения между государством и обществом и идеологический дух, предопределяют то, насколько широко государства способны разрабатывать и применять системы ИИ. Риски и уязвимость, характерные для любой технологии, также влияют на то, как их внедрение меняет возможности государств по реализации своих интересов. Повсеместное использование алгоритмов для дополнения или замены ролей, ранее выполнявшихся людьми, может изменить ключевые особенности принятия решений в гражданской и военной сферах. Учитывая эти факторы, аналитики и практики могут наилучшим образом понять влияние ИИ на распределение международной власти, чтобы разработать оптимальные стратегии национальной безопасности [Ibid, p. 915].

В самом широком смысле международные нормы часто, как замечают авторы, разрабатываются и принимаются в результате процесса, в ходе которого ведутся активные дискуссии вокруг проектов «инициаторов-нормотворцев». Широкий круг участников, вовлеченных в дебаты о правильном использовании ИИ, в целом говорит о том, что в инициаторах создания нормы нет недостатка. Так, помимо промышленно развитых стран, которые лидируют в разработке ИИ, государства Глобального Юга взяли на себя ведущую роль в некоторых областях, особенно в дискуссиях об ограничениях на автономные системы вооружения [Ibid, p. 927]. Появление регулирующих норм, ограничивающих то, какие виды систем ИИ государства должны или не должны использовать в каких-либо (или в определенных) контекстах, обязательно будет зависеть от аргументированности позиции «инициаторов-норматворцев». До сих пор, как в демократических, так и в автократических государствах те, кто обладает наибольшими возможностями для применения ИИ в военных целях, не решались присоединиться к рядам призывающих к запрету автономных систем вооружения. Изменится ли это в будущем – вероятно, будет зависеть от изменений в контексте дискуссий, полагают авторы. Например, нормы, запрещающие автономное или другие классы оружия с поддержкой искусственного интеллекта, могут следовать по стопам табу ядерного оружия, возникшего в результате его катастрофического применения. Альтернативой могут быть аргументы в пользу более строгого регулирования военного ИИ, потенциально способного нарушать международное гуманитарное право. В то время как аргументы, основанные на международном гуманитарном праве, помогли разработать негативные нормы, запрещающие ослепляющие

лазеры и другое оружие неизбирательного действия, уникальные характеристики оружия, основанного на ИИ, позволяют вести дискуссии о возможности применения позитивных норм, предписывающих контроль со стороны человека [Ibid, p. 927].

Особое значение имеет вопрос о том, будут ли государства, внедряющие технологии ИИ в смертоносных целях, использовать такие технологии надлежащим образом. С точки зрения М. Горовица, Ш. Писайк и К. Махони, первые попытки Евросоюза ввести нормативные стандарты этичного ИИ в своем Общем регламенте по защите данных (General Data Protection Regulation (GDPR)) показывают, что государства склонны игнорировать значимость международных норм, когда речь заходит о защите основных интересов национальной безопасности. Права на поддающийся объяснению искусственный интеллект и защиту данных ограничены положениями ст. 23 Общего регламента о национальной безопасности, в соответствии с которыми государства – члены ЕС могут ограничивать права отдельных субъектов данных в целях национальной и общественной безопасности, обороны и связанных с ними целях [Ibid, p. 927].

С другой стороны, некоторые государства – лидеры в области ИИ предприняли шаги, которые являются реакцией на общественное давление по соблюдению норм применения ИИ в военных целях. В сентябре 2020 г. США учредили Партнерство по искусственному интеллекту в интересах обороны (AI Partnership for Defense (PfD) между государствами-единомышленниками (like-minded states), внедряющими ИИ в военных целях, для укрепления практического сотрудничества по обмену данными, взаимодействия в других областях. По мнению авторов, политические рамки, разработанные государствами с наиболее мощными вооруженными силами, включая США и Китай, в соответствии с международными стандартами и этическими соображениями дают основания полагать, что международные нормы и практика государств будут продолжать развиваться параллельно, в диалоге друг с другом [Ibid, p. 928].

Возможные пути создания системы международной безопасности с помощью искусственного интеллекта

Один из вопросов, рассматриваемых М. Горовицом, Ш. Писайк и К. Махони, – направления наибольшего сосредоточения усилий государств на создании системы международной безопасности, все более насыщаемой средствами ИИ. Здесь авторы отмечают следующие проблемы:

1) большинство государств по-прежнему находятся на ранних стадиях обдумывания того, как ИИ будет интегрирован в гражданскую и военную сферы, и как можно использовать такие изменения, особенно в долгосрочной перспективе, для повышения своей способности достигать национальных целей. Целый ряд новых организаций и многосторонних форумов обсуждают риски, связанные с «милитаризацией» ИИ, и тем самым помогают формировать у государств представление не только о затратах и выгодах, связанных с обеспечением безопасности, но и о том, как это может повлиять на восприятие законности и целесообразности использования таких технологий;

2) помимо усилий государств, сосредоточенных на прогнозировании и разработке стратегии на десятилетия вперед, государства также осуществляют краткосрочные инвестиции в целях застраховаться от возможных преимуществ «первопроходцев», которые такие государства, как Соединенные Штаты и Китай, могли бы получить от ИИ;

3) стремление государств прогнозировать развитие ИИ и управлять ИИ влияет на их интересы в области безопасности и, по мнению авторов, будет по-прежнему осложняться скоростью, с которой новаторы в частном секторе опережают возможности регулирующих органов [2, p. 928–929].

Гиперглобализация продолжает способствовать быстрому распространению технологий и разработке новых инструментов, выходящих за рамки государственных исследований и разработок. То, как государства решат организовать свою внутреннюю политическую экономику в сфере применения ИИ, также будет иметь последствия для их успеха или неспособности сохранить возможность влиять на условия, в которых они конкурируют с другими в вопросах безопасности. Таким образом, заключают М. Горовиц, Ш. Писайк и К. Махони, во многих отношениях реакция государств на внутриполитические вызовы, связанные с инновациями в области ИИ, сыграет решающую роль в их позиционировании на международной арене [Ibid, p. 929].

К вопросу юридической ответственности в случае применения искусственного интеллекта в военных операциях и системах вооружений

На этой теме сосредоточен И. Нвагбара, исследователь из Канадского института международно-правовой экспертизы. В цен-

тре его внимания следующие вопросы: в какой степени системы ИИ надлежит использовать в конфликтных ситуациях; должны ли они использоваться для ведения боевых действий или должны ограничиваться разведкой, наблюдением и рекогносцировкой? Главный юридический вопрос в связи с применением ИИ в военных целях, волнующий автора и других ученых: кто несет ответственность за ущерб и жертвы, возникшие в результате автономных решений систем ИИ [3, p. 18–19].

Если системы оружия с искусственным интеллектом, такие как робототехника или смертоносные автономные системы вооружения (lethal autonomous weapons systems (LAWS)), используются для ведения физического боя, возникает вопрос, могут ли системы ИИ адекватно различать комбатантов и гражданских лиц? Ожидается, что в эти системы могут быть введены опознавательные знаки различных национальных вооруженных сил. Таким образом, у систем ИИ не могло бы возникнуть проблем с идентификацией и различением комбатантов в международных вооруженных конфликтах. Однако в категории немеждународных вооруженных конфликтов, которые составляют в современных конфликтах основную часть, возникает затруднение, когда для существующих и потенциальных негосударственных вооруженных группировок не существует установленных знаков отличия. В соответствии с международным гуманитарным правом, негосударственные вооруженные группы в немеждународных вооруженных конфликтах не имеют статуса комбатантов, как и члены организованных вооруженных групп, принимающие активные отличия [Ibid, p. 19].

Возникают следующие вопросы: как системы вооружения с ИИ, развернутые для ведения боевых действий в немеждународных вооруженных конфликтах, могут отграничивать тех, кто активно участвует в боевых действиях, от тех, кто не принимает активного участия в боевых действиях, в отсутствие знаков отличия? Будут ли системы ИИ, такие как роботы, обучены реагировать только в случае первоначального нападения со стороны людей? Если так, то системы ИИ будут лишены возможности самостоятельно наносить упреждающие удары в целях самообороны, что может лишить сторону военного преимущества, которое она стремится получить, применяя ИИ. Что представляет собой «атака» со стороны людей, и какой ответ системы ИИ дадут на такую «атаку» [Ibid, p. 20]?

Вместе с тем усовершенствованные технологии, включая системы ИИ с улучшенными возможностями наведения на цель, мо-

гут способствовать дальнейшему проведению различий между комбатантами и не комбатантами во время вооруженного конфликта [Ibid, p. 20].

Возникает спор о том, должны ли такие боевые роботы быть способны самостоятельно принимать решение о нанесении удара как система ИИ, или же это должны быть люди-операторы, наблюдающие за ситуацией с помощью монитора и принимающие это решение. Смогут ли системы ИИ применять сложные решения? Понимают ли они вообще концепцию сопутствующего ущерба и принцип пропорциональности, которые могли бы служить оправданием жертв среди гражданского населения пропорционально законному военному преимуществу [Ibid, p. 21]?

Несмотря на неопределенность, так или иначе, все сформулированные выше И. Нвагбаром вопросы касаются юридической и социальной ответственности за применение систем вооружения с использованием ИИ. С одной стороны, оспаривается ответственность государств за серьезные нарушения международного гуманитарного права. С другой стороны, международное уголовное право регулирует индивидуальную уголовную ответственность. Учитывая, что до сих пор исследовательские усилия, направленные на разработку смертоносных автономных систем вооружения, инициировались и финансировались государствами, – вопрос об ответственности начинается с государств [Ibid, p. 21].

Международное гуманитарное право, считает автор, должно применяться ко всем системам вооружений и, таким образом, ответственность государства за нарушение принципов международного гуманитарного права при применении смертоносных автономных систем вооружения возможна. Личная ответственность человека за решения о применении систем вооружений также должна сохраняться, поскольку ответственность не может быть передана машинам [Ibid, p. 22].

Однако практическое применение ответственности является запутанным и рискованным. Для установления индивидуальной уголовной ответственности требуется психологический элемент в той же мере, что и материальные элементы преступления.

Двумя факторами, определяющими психологический элемент преступления, являются «намерение» и «знание». Могут ли смертоносные автономные системы вооружения учитывать знание об основных международных преступлениях и действиях, лежащих в их основе? Могут ли они оценивать и разграничивать ситуации, которые представляют собой международные преступле-

ния, и отличать их от ситуаций, которые таковыми не являются? Если смертоносные автономные системы вооружения не могут понять знание о международных преступлениях, то по умолчанию у них определенно не может быть намерения их совершать. Возникает еще одна философская загадка, которая заключается в том, что если смертоносные автономные системы вооружения могут учитывать сложные знания о международных преступлениях и могут выбирать, иметь намерение их совершать, можно ли действительно говорить, что такие системы вооружений являются автономными или просто предварительно запрограммированными (специалистами-людьми) на то, чтобы иметь возможность оценить основные правовые аспекты международных преступлений? Покажет только время, полагает автор [Ibid, p. 23].

Ряд конкретных вопросов, касающихся юридической ответственности в случае применения систем ИИ в вооруженных конфликтах, продолжают занимать И. Нвагбара: если станет возможным, что смертоносные автономные системы вооружения будут иметь знания о международных преступлениях благодаря своим собственным когнитивным процессам, какие лица возьмут на себя ответственность за их преступления? Специалисты, создавшие такие системы (аппаратное и программное обеспечение)? Несут ли люди ответственность за физическое обслуживание таких систем, а также за разработку и применение таких систем отвечают военные и политические лидеры? [3, p. 23].

Еще один вопрос, касающийся индивидуальной уголовной ответственности за действия смертоносных автономных систем вооружения, заключается в том, какой вид ответственности применяется. Поскольку автономная система принимает решения совершить действие посредством своих автономных когнитивных процессов, она является непосредственным исполнителем. Поскольку люди не принимали участия в принятии автономного решения и не имели полного контроля над этим решением и последующими действиями, юридически было бы невозможно считать людей соисполнителями, косвенными исполнителями или косвенными соисполнителями. Таким образом, ответственность вышестоящего командования (superior responsibility) может стать следующим важным моментом в отношении режима ответственности [Ibid, p. 23].

Первый фактор, который необходимо определить в режиме ответственности вышестоящего командования, заключается в том, обладают ли военные командиры или лица, фактически выпол-

няющие функции военных командиров, эффективным управлением и контролем над силами, совершающими преступление. Это в полной мере касается и смертоносных автономных систем вооружения. В то же время, возможно ли обеспечить эффективное управление автономной системой вооружений? Есть ли в такой автономной системе вооружений компонент, который позволяет осуществлять управление человеком? Если да, то делает ли это такую систему по-настоящему автономной или полуавтономной?

Вторым фактором, связанным с ответственностью такого уровня командования, является осведомленность о совершении преступления. Учитывая автономный и рекурсивный характер смертоносных автономных систем вооружения, следует подчеркнуть, что их внутренний когнитивный процесс, а также процесс принятия решений не только не поддаются точному прогнозированию, но и не открыты для обсуждения с внешними силами [Ibid, p. 24].

Хотя, считает И. Нвагбара, можно установить факт совершения преступления автономной системой, шансы на то, что военное командование должно было знать, что система собирается его совершить, невелики, особенно когда в этот момент военный командир больше не может предотвратить их совершение. И предлагает сконструировать особый режим индивидуальной уголовной ответственности. Такой режим, по его мнению, может логично привести к ответственности политических и военных лидеров, ответственных за разработку и применение смертоносных автономных систем вооружения и стать тяжелым бременем для политических и военных элит стран, показывая им, что именно они будут нести ответственность за авантюры в области военных технологий [3, p. 24].

Заключение

Учитывая, что появление ИИ только начинает открывать новые возможности в военной сфере и сфере международной безопасности, остается неясным, каким образом субъекты международной системы придут к пониманию законности использования ИИ в условиях (военных) конфликтов. Насущная задача сейчас – заложить прочную теоретическую основу, способную максимально охватить практические проблемы, которые провоцирует повсеместное распространение технологий ИИ [2, p. 915, 926].

Государства осознают грозящую ИИ опасность и, тем не менее, не прекращают своих усилий по разработке смертоносных автономных систем вооружения. Более того, они объединяются

для выработки принципов разработки и применения ИИ в военных целях. Так, Франция и Германия подготовили в 2019 г. политическую декларацию «11 руководящих принципов, регулирующих разработку и использование автономных систем вооружения». Хотя такая декларация не является юридически обязательной или окончательным решением – ибо не наносит ущерб будущим обсуждениям, она явно показывает направленность политики – решать вопросы морального, юридического и оперативного плана, препятствующие появлению новых технологий, в том числе в информационной и военной сферах [3, p. 21–22].

Список литературы

1. Загайнов М.Р. Вопросы развития сотрудничества США и России в сфере международной информационной безопасности // Социально-политические науки. – 2024. – Т. 14, № 3. – С. 115–124.
2. Horowitz M., Pindyck Sh., Mahoney C. AI, the International Balance of Power, and National Security Strategy // The Oxford Handbook of AI governance / ed. by Justin B. Bullock, Yu- Che Chen, et. – Oxford: Oxford Univ. Press, 2024. – P. 914–936.
3. Nwagbara I. Artificial Intelligence and International Criminal Law // Artificial Intelligence and the Future of International Law Bridging Rights, Trade, and Arbitration / ed. by A. Poorhashemi. – London: Springer, 2024. – P. 16–27.

УДК 34.096; 341 DOI: 10.31249/iajpravo/2025.03.09

ПРЯЖНИКОВА О.Н.[1] ВЫРАБОТКА ПРАВОВЫХ ПОДХОДОВ К МЕЖДУНАРОДНОМУ РЕГУЛИРОВАНИЮ ТОРГОВЫХ ОПЕРАЦИЙ С ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ НА ПРИМЕРЕ ВТО (Статья)

Аннотация. Рассматриваются вопросы регулирования международной торговли цифровыми технологиями с использованием искусственного интеллекта Соглашением по техническим барьерам в торговле, участниками которого являются члены Всемирной торговой организации. Раскрывается роль Соглашения в создании и продвижении инструментов транспарентности для решения проблем, возникающих в связи с использованием искусственного интеллекта в различных продуктах. Подчеркивается определяемая Соглашением важность установления приоритетности международных стандартов как основы для регулирования искусственного интеллекта.

Ключевые слова: международная торговля; искусственный интеллект; ВТО; Соглашение по техническим барьерам в торговле; транспарентность; международные стандарты.

PRYAZHNIKOVA O.N. Development of Legal Approaches to International Regulation of Trade Operations with AI Using the Example of the WTO (Article)

Abstract. The issues of regulating international trade in digital technologies using artificial intelligence are considered by the Agreement on Technical Barriers to Trade, to which the members of the World Trade Organization are participants. The role of the Agreement in the creation and promotion of transparency tools for solving problems arising from the use of artificial intelligence in various products is

[1] *Пряжникова Ольга Николаевна*, научный сотрудник отдела социологии и социальной психологии ИНИОН РАН.

revealed. The importance of prioritizing international standards as a basis for regulating artificial intelligence, as defined by the Agreement, is emphasized.

Keywords: international trade; artificial intelligence; WTO; Agreement on Technical Barriers to Trade; transparency; international standards.

Для цитирования: Пряжникова О.Н. Выработка правовых подходов к международному регулированию торговых операций с искусственным интеллектом на примере ВТО (Статья) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2025. – № 3. – С. 118–128. – DOI: 10.31249/iajpravo/2025.03.09

Введение

В последние годы международные организации и отдельные страны активно разрабатывают принципы и правила, регулирующие разработку и применение ИИ, стремясь нивелировать различные негативные эффекты от внедрения таких технологий, а именно предвзятость ИИ, сокращение рабочих мест за счет автоматизации, нарушение конфиденциальности и прав потребителей, возникающие моральные дилеммы, обеспечение кибербезопасности.

В результате страны начали формировать политику в сфере ИИ, используя инструменты мягкого права, такие как формирование свода этических принципов и создание соответствующих национальных стратегий. Со временем законодательное регулирование стало касаться конкретных вопросов, а некоторые страны разрабатывают всеобъемлющие законы, контролирующие применение ИИ. Вводимые национальные стандарты служат защите национальных интересов, представляя собой зачастую протекционистский инструмент. В условиях, когда растет число законодательных инициатив на национальном, региональном и международном уровнях, а также в виде двусторонних соглашений, направленных на устранение рисков, связанных с использованием ИИ, возникает проблема фрагментированности правового регулирования. В такой ситуации особое значение приобретает ключевая функция ВТО – предоставлять своим членам возможность быть в курсе последних изменений в сфере регулирования. Обращаясь в нашем обзоре к теме регулирования ИИ в контексте международной торговли, особое внимание мы уделим Соглашению по техническим барье-

рам в торговле (далее – Соглашение по ТБТ), рассмотрев некоторые из реализуемых в его рамках норм и процедур, обеспечивающих развитие международной торговли, в том числе товарами на базе ИИ.

Соглашение по ТБТ вступило в силу 30 лет назад, 1 января 1995 г. Это одно из соглашений, содержащихся в приложениях к Соглашению ВТО. Оно гласит, что страны-участники Соглашения имеют право принимать меры для обеспечения качества экспортируемых товаров или защиты здоровья и жизни людей, окружающей среды, животных и растений при условии недопущения возникновения технических барьеров, препятствующих развитию международной торговли и применяемых в отношении отдельных стран[1]. Соглашение по ТБТ относится к типу многосторонних соглашений ВТО, касающихся торговли товарами (таких как ГАТТ и Соглашение о применении санитарных и фитосанитарных мер). Соглашение по ТБТ включает в себя положения, определяющие специфику подготовки, принятия и применения мер регулирования торговли товарами. При этом оно поощряет гармонизацию регулирования и определяет в качестве приоритета использование международных стандартов. Соглашение содержит подробные положения, применяемые на протяжении всего процесса подготовки, принятия и применения соответствующих мер, что обеспечивает транспарентность всех этапов цикла правового регулирования. Эти положения поэтапно на протяжении многих лет разрабатывались в Комитете по ТБТ[2], что позволило Соглашению по ТБТ стать уникальным многосторонним инструментом для решения проблем регулирования международной торговли[3].

Использование инструментов транспарентности

Соглашение по ТБТ включает три основных инструмента обеспечения транспарентности: 1) участники должны предостав-

[1] Соглашение по техническим барьерам в торговле. – URL: https://wto.ru/about-WTO/WTO-agreements/ (дата обращения: 04.04.2025).

[2] В состав Комитета по техническим барьерам в торговле входят представители от каждого члена. Он собирается по мере необходимости, но не реже чем один раз в год, с тем чтобы предоставить членам возможность провести консультации по любым вопросам, касающимся функционирования Соглашения по ТБТ (ст. 13 Соглашения по ТБТ).

[3] Technical Barriers to Trade: The WTO Agreements Series // World Trade Organization. – Geneva, 2021. – P. 9.

лять уведомления о проектах регламентов (ст. 2.9, 2.10, 3.2, 5.6, 5.7, 7.2); 2) создать информационные центры (для ответов на запросы по поводу вводимых мер от других членов и заинтересованных сторон) (ст. 10.1 и 10.3); 3) обязаны публиковать как предварительные, так и окончательные тексты соответствующих регламентов и стандартов (ст. 2.9.1 и 2.11)[1].

Механизм обеспечения транспарентности Соглашения по ТБТ предусматривает, что его участники должны уведомлять Комитет по ТБТ[2] о вводимых ими мерах регулирования еще на стадии проекта в соответствии со следующей процедурой (рекомендуемый период времени для этапов один – шесть – 60 дней):

1) мера предлагается (ст. 2.9, 5.6);

2) публикуется уведомление о ней (ст. 2.9.1, 5.6.1);

3) уведомление других членов Соглашения через Комитет по ТБТ (ст. 2.9.2, 5.6.2);

4) предоставление по запросу членов копий разрабатываемого технического регламента (ст. 2.9.3, 5.6.3);

5) обсуждение поступающих от членов соглашения комментариев (ст. 2.9.4, 5.6.4);

6) окончание периода комментариев;

7) принятие меры страной-членом;

8) публикация принятого положения (ст. 2.11, 5.8);

9) вступление меры в силу (ст. 2.12, 5.9)[3].

Инструмент раннего уведомления призван помочь правительствам стран и другим заинтересованным участникам международной торговли быть заранее в курсе вводимых правил, связанных с ИИ, и дать возможность своевременно высказывать опасения и задать вопросы относительно планируемого регулирования. Меры регулирования, влияющие на торговлю с другими членами и не соответствующие международным стандартам, после уведомления о них участников Соглашения могут обсуждаться ими на двусторонней основе. Также по их поводу могут поступать комментарии от участников, которые впоследствии могут быть учтены сторо-

[1] Transparency obligations. – URL: https://www.wto.org/english/tratop_e/tbt_e/tbt_notifications_e.htm#draft (дата обращения: 04.04.2025).

[2] Комитет ВТО по техническим барьерам в торговле, состоящий из представителей всех членов ВТО, является органом, ответственным за реализацию Соглашения по ТБТ.

[3] Technical Barriers to Trade: The WTO Agreements Series // World Trade Organization. – Geneva, 2021. – P. 39.

ной, формирующей регуляторные меры. Если информации о вводимых регламентах недостаточно, то участники Соглашения могут поднять возникшие вопросы на заседании Комитета по ТБТ в соответствии со ст. 14 «Консультации и урегулирование споров» Соглашения по ТБТ.

Транспарентность процедур в рамках Соглашения по ТБТ способствует большему пониманию разнообразных подходов к регулированию и способствует разработке более эффективных и скоординированных мер участниками соглашения, т.е. более качественному регулированию товарооборота и снижению торговых издержек.

По данным на июль 2024 г. участники Соглашения по ТБТ подали совокупно за весь период функционирования Соглашения порядка 500 уведомлений о мерах регулирования, связанных с цифровыми продуктами, такими как: Интернет вещей, технология 5G, беспилотные летательные аппараты, автономные транспортные средства, программное обеспечение в различных продуктах и медицинских устройствах на базе ИИ[1]. Цели вводимых участниками международной торговли мер включают предотвращение мошеннических практик и защиту потребителей и информации, стандарты качества, гармонизацию регулирования, защиту здоровья и безопасности человека. Среди наиболее активных участников Соглашения, предоставляющих уведомления в сфере цифровых технологий и ИИ, – США, Бразилия, ЕС, Китай, Мексика, Малайзия, Южная Корея и Япония[2].

Одним из наиболее значимых в сфере ИИ уведомлений стало уведомление о проекте закона Евросоюза об ИИ. 11 ноября 2021 г. Евросоюз уведомил ВТО о «Законе Европейского парламента и Совета, устанавливающем гармонизированные правила в отношении искусственного интеллекта (Закон об искусственном интеллекте)»[3] (Уведомление G/TBT/N/EU/850), который регулирует определение, применение, доступ на рынок, штрафные санкции и другие аспекты технологий ИИ. Этот Закон является первой в

[1] Da Fonseca Azevedo M. Navigating the AI Frontier in International Trade Law: The Role of the WTO's TBT Agreement / World Trade Institute (WTI). – 2024. – P. 16. – (WTI Working paper series: WTI working paper; N 4/2024).

[2] Ibid.

[3] Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). – URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата обращения: 18.04.2025).

истории правовой базой для использования ИИ в Евросоюзе, направленной на усиление контроля Союза за рисками, сопутствующими использованию технологий ИИ, с целью защиты безопасности и основных прав пользователей и компаний[1]. Евросоюз уведомил о том, что системы ИИ, которые считаются явной угрозой безопасности и правам людей, будут запрещены в Европейском союзе. Речь идет о системах ИИ, которые могут манипулировать поведением человека, подавляя свободную волю определенных пользователей (например игрушки, использующие голосовую помощь, поощряющую опасное поведение несовершеннолетних), а также системы ИИ, которые позволяют властям осуществлять «социальный скоринг»[2]. Обсуждение данного Акта происходило на заседаниях Комитета ТБТ в марте, июле, ноябре 2022 г., а также в марте и июне 2023 г.[3]

В апреле 2024 г. впервые член соглашения из группы развивающихся стран в лице Кении уведомил Комитет о регулировании, специфичном для ИИ (Information technology – Artificial Intelligence – Code of Practice for AI Applications: Draft Kenya Standard (DKS 3007:2024), – Уведомление G/TBT/N/KEN/1604[4]. В документе представлен набор рекомендаций, призванных помочь компаниям разрабатывать, продавать или использовать системы ИИ. Рекомендации включают: подходы к укреплению доверия к системам ИИ посредством их прозрачности, объяснимости, контролируемо-

[1] Minutes of the meeting 21–23 June 2023 / Committee on Technical Barriers to Trade. – 2023. – P. 166. – URL: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?FullTextHash=1&MetaCollection=WTO&SymbolList=%22G/TBT/M/90%22+OR+%22G/TBT/M/90/*%22&languageUIChanged=true# (дата обращения: 04.04.2025).

[2] WTO official document number G/TBT/N/ EU/850. – 2021. – 11.11. – P. 1. – URL: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?DataSource=Cat&query=@Symbol=%22G/TBT/N/EU/850%22%20OR%20@Symbol=%22G/TBT/N/EU/850/*%22&Language=English&Context=ScriptedSearches&languageUIChanged=true (дата обращения: 04.04.2025).

[3] См.: European Union – Proposal for a regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts (Id 736). – URL: https://tradeconcerns.wto.org/FR/stcs/details?imsId=736&domainId=TBT (дата обращения: 04.04.2025).

[4] Information technology – Artificial Intelligence – Code of Practice for AI Applications: Draft Kenya Standard (DKS 3007:2024) / Kenya Bureau of Standards. – 2024. – 39 p. – URL: https://members.wto.org/crnattachments/2024/TBT/KEN/24_02705_00_e.pdf (дата обращения: 04.04.2025).

сти; к выявлению типичных сопутствующих угроз и рисков, связанных с системами ИИ, а также к определению возможных методов их смягчения и к оценке доступности, устойчивости, надежности, точности, безопасности, защищенности и конфиденциальности систем ИИ[1].

Помимо положительных эффектов обязательств по обеспечению транспарентности вводимого правового регулирования, которые устанавливает Соглашение по ТБТ, важно отметить, что они могут по существу противоречить институту национальных мер по укреплению кибербезопасности. В соответствии со ст. 2.9.2 и 2.10.1 Соглашения ТБТ страны – участники этого Соглашения обязаны уведомлять о проектах технических регламентов или уже принятых в срочном порядке регламентах в случае особых ситуаций при наличии двух условий: во-первых, когда международный стандарт отсутствует или внутреннее регулирование противоречит соответствующим международным стандартам; во-вторых, когда национальное регулирование может оказать значительное влияние на торговлю с другими участниками. Более того, страны, принимающие национальные технические регламенты, также должны публиковать соответствующее уведомление на ранней стадии соответствующих проектов[2]. Учитывая цели, для которых стандарты кибербезопасности принимаются на национальном уровне (например, для защиты от кибератак), очевидно, что требования транспарентности не могут в особых случаях соблюдаться той или иной страной в целях защиты ее национальной безопасности.

Международные стандарты как основа для регулирования искусственного интеллекта

Международные стандарты играют важную роль в регулировании и согласованности международных торговых операций. Их разработка и использование в области ИИ помогают наметить единые ориентиры для стран мира при формировании мер регулирования в сфере ИИ. Хотя ВТО не разрабатывает международные стандарты, ряд ее соглашений поощряет их использование. Так, Соглашение по ТБТ поощряет своих членов участвовать в гармо-

[1] WTO official document number G/TBT/N/KEN/1604. – 2024. – 19.04. – URL: https://tbt.bsn.go.id/notification_detail/53039 (дата обращения: 04.04.2025).

[2] Oddenino A. Digital standardization, cybersecurity issues and international trade law // Questions of International Law. – 2018. – Vol. 51. – P. 40.

низации регулирования, устанавливая при этом требование использовать в качестве основы для внутренних (национальных) стандартов, технических регламентов и процедур сертификации соответствующие международные стандарты, так как следование им позволяет избежать создания дополнительных барьеров для международной торговли.

В то же время Соглашение ТБТ признает, что могут быть законные причины для того чтобы международный стандарт не использовался в качестве основы для того или иного регламента. Таким образом, странам – участникам Соглашения, в частности из числа развивающихся стран, разрешено при определенных условиях отклоняться от них[1]. Согласно ст. 2.4 Соглашения по ТБТ, когда требуется технический регламент и имеются соответствующие международные стандарты, участники должны использовать их в качестве основы для своего внутреннего регулирования, если только они не окажутся неэффективными, например, из-за географических и климатических факторов или «фундаментальных технологических проблем». По запросу других участников страна, вводящая регламент отличный от действующего, также обязана указать причины неприменения релевантных международных стандартов.

Имея целью гармонизировать технические регламенты для международной торговли, Соглашение по ТБТ настоятельно рекомендует своим участникам принимать участие в разработке и развитии международных стандартов. Статья 4.1 Соглашения по ТБТ требует, чтобы национальные органы по стандартизации принимали и соблюдали приложение 3 Соглашения по ТБТ – «Кодекс добросовестной практики по подготовке, принятию и применению стандартов». В результате принимаемые международные стандарты, в том числе в сфере ИИ, с большей вероятностью будут более инклюзивными, легитимными и актуальными[2]. Ввиду того, что активное участие в разработке международных стандартов в сфере передовых технологий может быть проблематичным для представителей развивающихся экономик из-за ограниченных ресурсов и отсутствия соответствующих знаний, ст. 11.2 Соглашения по ТБТ требует от государств, его подписавших, консультировать участников из развивающихся стран по их запросу и предоставлять им

[1] Trading with intelligence: How AI shapes and is shaped by international trade // World Trade Organization. – 2024. – P. 68.

[2] Ibid.

техническую помощь для участия в работе международных органов по стандартизации.

Одной из особенностей подхода к стандартизации в Соглашении по ТБТ является отсутствие списка соответствующих международных органов по формированию стандартов, чьи регламенты следует использовать. Это делает правила Соглашения по ТБТ применимыми ко всем официальным организациям, функционирующим в данной сфере. При этом Соглашение по ТБТ призывает следовать «Принципам разработки международных стандартов, руководств и рекомендаций» (Principles for the Development of International Standards, Guides and Recommendations)[1] для своих участников при создании стандартов и регламентов. А именно, предполагается соблюдение принципов транспарентности, открытости, беспристрастности, консенсуса, эффективности, релевантности и согласованности. Те же принципы должны применяться в технической работе, делегируемой международными органами по стандартизации. Критерием релевантности международной организации по стандартизации является открытость для участия в ней стран – членов ВТО[2]. В сфере стандартизации ИИ это, прежде всего, такие организации, как Международная организация по стандартизации ИСО (International Organization for Standardization – ISO), Международная электротехническая комиссия (International Electrotechnical Commission – IEC) и Международный союз электросвязи (International Telecommunication Union – ITU).

Вместе с тем по многим возникающим направлениям применения ИИ отсутствует стандартизация, и на практике не так много стран участвуют в разработке стандартов ИИ (особенно это касается развивающихся стран). Учитывая быстрые темпы технологического прогресса, вполне вероятно, что пробелы в стандартизации сохранятся, и это потребует большего сотрудничества между странами, в том числе в виде заключения соглашений о взаимном признании тех или иных регламентов.

Соглашение по ТБТ приветствует использование инструментов нормативной согласованности, а именно заключения соглаше-

[1] Principles for the Development of International Standards, Guides and Recommendations // WTO. – URL: https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm (дата обращения: 04.04.2025).

[2] Da Fonseca Azevedo M. Navigating the AI Frontier in International Trade Law: The Role of the WTO's TBT Agreement / World Trade Institute (WTI). – 2024. – P. 14. – (WTI Working paper series: WTI working paper; N 4/2024).

ний о взаимном признании и оценки соответствия, оговоренных в ст. 6. Эти инструменты могут быть полезны для содействия международной торговле, даже если стандарты, правила и процедуры сертификации между торговыми партнерами различаются или не полностью гармонизированы. Соглашения о взаимном признании, заключаемые между государствами, оптимизируют процедуры оценки соответствия, позволяя торговым партнерам признавать результаты тестирования и сертификации товаров друг друга, тем самым сокращая издержки и ускоряя процедуры распространения продукции. По некоторым оценкам наличие между странами соглашения о взаимном признании увеличивает стоимость экспорта на 15–40%[1]. Возникающий положительный эффект особенно важен в сфере оборота новых высокотехнологичных продуктов, к которым применяются новые нормативные требования, в таких сферах как цифровые стандарты, кибербезопасность, технология 5G, совместимость электронных счетов-фактур и других, связанных с цифровой трансформацией. То, что Соглашение по ТБТ поощряет участников полагаться на соглашения о взаимном признании и оценку соответствия (ст. 2.7 и ст. 6), создает возможность избежать ненужного дублирования процедур сертификации и тем самым снижает барьеры для торговли продуктами на базе ИИ[2].

Заключение

В заключение отметим, что различные органы ВТО организуют тематические дискуссии по темам, связанным с торговлей ИИ, для обмена опытом и передовыми практиками в данной области. Комитет по ТБТ, со своей стороны, недавно провел ряд тематических сессий[3] по проблемам цифровизации и связанным с ней мерам регулирования с целью улучшения глобального сотрудничества между странами – участниками Соглашения в этих областях. На тематических сессиях обсуждались проблемы торговли нематериальными цифровыми продуктами, включая ИИ, кибербе-

[1] Trading with intelligence: How AI shapes and is shaped by international trade // World Trade Organization. – 2024. – P. 69.

[2] Ibid.

[3] Например, см.: Thematic Session on Regulatory Cooperation between Members on Cybersecurity // WTO, Technical Barriers to Trade. – 2023. – 20.07. – URL: https://www.wto.org/english/tratop_e/tbt_e/tbt_2006202315_e/tbt_2006202315_e.htm (дата обращения: 04.04.2025).

зопасность, вопросы оценки соответствия продуктов, продаваемых через процедуры электронной торговли, цифровые решения для проведения оценки соответствия и использования цифровых технологий и инструментов в процессах регулирования торговли[1].

Следует подчеркнуть, что ВТО может внести значимый вклад в формирование торговой политики в отношении цифровых продуктов на базе ИИ и обеспечение кибербезопасности, играя роль ключевой «площадки» для международного сотрудничества и поддерживая важную работу международных органов по стандартизации. Соглашение по ТБТ, в свою очередь, продвигает сотрудничество в сфере регулирования и помогает избежать нормативной фрагментации, которая создает барьеры для торговли цифровыми товарами, что способствует решению некоторых проблем и нивелирует риски, связанные с разработкой, использованием и товарооборотом цифровых продуктов и продуктов на базе ИИ. Благодаря продвижению принципов транспарентности и следованию международным стандартам, Соглашение по ТБТ с высокой вероятностью гарантирует, что процесс регулирования не создаст дискриминационных технических барьеров в международной торговле продуктами с использованием ИИ, при этом защищая право стран реализовывать их цели в соответствии с государственной политикой.

[1] Ibid. – P. 67.

УДК 34.096; 342 DOI: 10.31249/iajpravo/2025.03.10

АЛФЕРОВА Е.В.[1] **ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ: ПРАВОВОЙ ПОТЕНЦИАЛ И РИСКИ ПРИМЕНЕНИЯ (Обзорная статья)**

Аннотация. В обзорной статье представлены исследования российских и зарубежных ученых в области внедрения технологий искусственного интеллекта в различных областях государственного (публичного) управления. Внимание сконцентрировано на перспективных направлениях и преимуществах применения искусственного интеллекта в целях повышения эффективности и результативности деятельности органов государственной управления, качестве и открытости работы публичных органов и государственных служащих по реализации ими своих должностных обязанностей и функций. Рассматриваются виды потенциальных рисков, которые могут возникнуть при использовании этих технологий, некоторые проблемы их правового предупреждения.

Ключевые слова: государственное управление; государственные служащие; цифровые технологии; искусственный интеллект; правовое регулирование искусственного интеллекта; риски применения искусственного интеллекта.

ALFEROVA E.V. Artificial Intelligence in Public Administration: Legal Potential and Application Risks (Review article)

Abstract. This review article presents research by Russian and foreign scientists on the development of the concept of digital governance and points of view on various issues of the introduction of artificial intelligence technologies in various fields of public administration. Attention is focused on promising areas and advantages of using artificial intelligence in order to increase the efficiency and effectiveness of

[1] *Алферова Елена Васильевна*, ведущий научный сотрудник, завотделом правоведения ИНИОН РАН, кандидат юридических наук.

the activities of public administration bodies, the quality and openness of the work of civil servants in the implementation of their official duties and functions. The types of potential risks that may arise when using these technologies and some problems of their legal prevention are considered.

Keywords: public administration; civil servants; digital technologies; artificial intelligence; legal regulation of artificial intelligence; risks of using artificial intelligence.

Для цитирования: Алферова Е.В. Искусственный интеллект в государственном управлении: правовой потенциал и риски применения. (Обзорная статья) // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 4: Государство и право. – Москва, 2025. – № 3. – С. 129–146. – DOI: 10.31249/iajpravo/2025.03.10

Введение

Технологии ИИ находят распространение во всех сферах государственного управления, таких как образование, здравоохранение, социальное обеспечение, охрана окружающей среды, правоохранительная деятельность, нормотворчество, транспорт, IT-сфера и др. На развитие систем ИИ направлены Национальная стратегия развития искусственного интеллекта на период до 2030 г., утвержденная Указом Президента РФ от 10.10.2019 № 490 (ред. от 15.02. 2024 г.). Искусственный интеллект, согласно п. 17.1 Национальной стратегии, определяется как одна из самых важных технологий, доступных человеку. Уже сегодня благодаря ИИ происходит рост мировой экономики, ускорение инноваций во всех областях науки, повышение качества жизни населения, доступности медицинской помощи, качества образования, производительности труда и качества отдыха[1].

Достижения и риски внедрения технологий ИИ в различных сферах общественной жизни актуализируют внимание ученых-правоведов к вопросам их правового регулирования и проблемам внедрения этих технологий[2]. Анализ законодательства показывает,

[1] Перспективные направления правового регулирования искусственного интеллекта: монография / под ред. А.В. Минбалеева. – Саратов, 2023. – С. 11.

[2] См.: Комплексное исследование правовых и этических аспектов, связанных с разработкой и применением систем искусственного интеллекта / под. ред. В.Б. Наумова. – 2022. – 366 с.; Залоило М.В. Искусственный интеллект в праве. – 2021. – 132 с.; Правовое регулирование применения цифровых технологий в го-

что государственное управление в области ИИ развивается в двух направлениях: 1) формирование нового режима правового регулирования ИИ; и 2) применение ИИ при выполнении государственных функций. Оба эти сегмента важны и требуют пристального изучения, в том числе в целях поиска ответов на вопросы о том, кто будет нести ответственность за сбой в работе ИИ[1], соответствуют ли алгоритмы функционирования ИИ принципу верховенства закона[2], каковы уровень зрелости технологий ИИ и эффекты от применения методов ИИ в государственном управлении и др.[3]

Как отмечают большинство исследователей, технологии ИИ, применяемые в государственном управлении, открывают новые возможности, однако их внедрение в деятельность органов публичной власти и управления, работу государственных служащих сопряжено как с появлением сложных технологических новаций, увеличением объема должностных функций и расширением «цифровых» обязанностей, так и определенными цифровыми рисками[4].

сударственном управлении / под ред. М.Б. Добробабы. – Саратов, 2024. – 156 с.; Научное технологическое развитие, цифровизация, искусственный интеллект и право // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2024. – № 4. – С. 9–128; Artificial Intelligence and the Law Cybercrime and Criminal Liability / ed. by Dennis J. Baker, Paul H. Robinson. – 2021. – 265 p.; Kumar S., Kumar Verma A., Mirza A. Digital Transformation, Artificial Intelligence and Society: Opportunities and Challenges. – 2024. – 193 p.; Artificial Intelligence and the Future of International Law Bridging Rights, Trade, and Arbitration / ed. by Abbas Poorhashemi. – 2024. – 61 p.; Legal Aspects of Autonomous Systems: A Comparative Approach / ed. by Dário Moura Vicente, Rui Soares Pereira, Ana Alves Leal. – 2024. – 382 p.; AI and Law How Automation Is Changing the Law / eds. Aurelia Tamò-Larrieux, Clement Guitton, Simon Mayer. – 2025. – 195 p. and others.

[1] Digital Governance: Confronting the Challenges Posed by Artificial Intelligence / ed. K. Prifti, E. Demir, J. Krämer, K. Heine, E. Stamhuis. – 2024. – P. 12.

[2] Burgess P. AI and the Rule of Law: The Necessary Evolution of a Concept. – 2024. – P. VII–IX.

[3] Косоруков А.А. Технологии искусственного интеллекта в современном государственном управлении // Социодинамика. – 2019. – № 5. – С. 26–27.

[4] Поярков Р.А. Искусственный интеллект как инструмент оптимизации процессов принятия управленческих решений в системе государственной службы РФ // Общество: политика, экономика, право. – 2025. – № 2. – С. 140–141; Digital Governance: Confronting the Challenges Posed by Artificial Intelligence. Op. cit. – P. 12, и др.

Концепция цифрового управления

Для того чтобы воспользоваться преимуществами цифровых технологий, в том числе ИИ, и снизить связанные с ними риски, ключевым становится вопрос развития концепции управления. Несмотря на ряд идей и определений этой концепции, общее определение остается неясным. Исследователи признают, что она расплывчата и широка, ее трудно применять на практике, содержит мало положений по конкретным структурам, процессам и задействованным субъектам. Однако с аналитической точки зрения использование концепции управления, как полагают авторы книги «Цифровое управление: решение проблем, связанных с искусственным интеллектом» – Эсра Демир, Юлия Кремер, Костина Прифти, Клаус Хайне и Эверт Стамхейс, является ценным. В целом *концепция управления* (*the concept of governance*) означает «управление с помощью сетей» и, соответственно, охватывает взаимодействие между широким кругом участников. Концепция управления отличается от *концепции государственного управления* (*the concept of government*) и является более широкой, поскольку включает в себя негосударственных субъектов (non-state actors). Тем не менее использование и понимание этой концепции варьируются в зависимости от контекста[1].

С развитием технологий необходимость контролировать технологические нововведения привела к появлению *концепции цифрового управления* (*the concept of digital governance*). Роль цифрового управления заключается в обеспечении реализации функций субъектов («акторов») и использовании механизмов управления цифровыми технологиями в целях извлечения преимуществ и снижения рисков, с ними связанных. Таким образом, концепцию цифрового управления, по мнению авторов, можно определить как «практику разработки и внедрения политики, процедур и стандартов для надлежащей разработки, внедрения и использования цифровых технологий»[2].

Концепцию цифрового управления в первую очередь необходимо оценивать с точки зрения ее нормативности. Цифровое управление может содержать руководящие принципы (инструкции) и рекомендации, которые частично совпадают с норматив-

[1] Digital Governance: Confronting the Challenges Posed by Artificial Intelligence. Op. cit. – P. 4–5.

[2] Ibid.

ным правовым регулированием в сфере цифровизации. Это совпадение связано с нормативными моделями цифрового управления, которые относятся к системе актов, разрабатываемых и применяемых общественными или государственными институтами в целях регулирования поведения соответствующих субъектов. Другими словами, системы цифрового управления содержат множество нормативных моделей. Таким образом, ценность цифрового управления заключается в том, чтобы избежать «дублирования», т.е. цифровое управление может предложить структуру, объединяющую пути регулирования, которые в противном случае могли бы действовать независимо или вступать в противоречие, когда они касаются одного и того же цифрового явления. Если сосредоточить внимание на цифровом управлении, возможно, удастся избежать или (по крайней мере) смягчить разрушительные последствия технологий ИИ, возникающие в результате их разработки, внедрения и использования.

Управление в цифровую эпоху, по мнению некоторых исследователей, можно рассматривать как комплекс изменений, в центре которых находятся ИТ-технологии и обработка информации, приводящие к необходимости реорганизация государственного управления, где появляются новые и развиваются прежние государственные услуги, формируются «малые миры» (small worlds) (так называемые «агентства-бутики», которые узко специализированы и не дублируют функции других). Это предполагает «создание более крупных и всеобъемлющих управленческих блоков..., сквозной реорганизации процессов, устранения ненужных шагов, затрат на соблюдение требований, проверок и формуляров [и] создание более “гибкого” правительства, способного быстро реагировать на изменения в социальной среде»[1]. По мнению Р. Кеннеди, основные компоненты этой «цифровой» деятельности – интерактивный поиск и предоставление информации, которая имеет основополагающее значение для дальнейшего развития; реорганизация, ориентированная на интересы и потребности человека; комплексное предоставление услуг, «однократные запросы» (ask-once processes); хранение данных; реинжиниринг комплексных услуг; гибкие процессы управления; устойчивое развитие и изменения, связанные с цифровизацией. Изменения в ИТ становятся «по-настоящему трансформирующими». Основными компонентами

[1] Kennedy R. The Rule of Law and Algorithmic Governance // the Cambridge Handbook of the Law of Algorithms / ed. by Woodrow Barfield. – 2021. – P. 212.

цифрового управления являются электронное предоставление услуг и электронное правительство; веб-платформа; вычислительная техника общего назначения; новые формы автоматизированных процессов; радикальное устранение посредничества; активное использование потоковых каналов; содействие изократическому управлению и переход к управлению по принципу «открытой книги»[1].

Роль искусственного интеллекта в государственном управлении: вопросы его правового регулирования

О применении ИИ в деятельности органов публичной власти и управления, работе государственных служащих пишут государствоведы, правоведы, политологи, социологи и ученые других научных направлений. Как отмечается в их исследованиях, многие страны уже внедрили технологии ИИ для выполнения государственных задач и повышения эффективности реализации государственных функций, борются за лидерство в этой области. Среди таких странвыделяются Китай, США, а также Евросоюз[2]. Правительства и законодатели разных стран, полагает Джемин Ли, уже осознали преимущества применения ИИ, в том числе для решения своих государственных задач, и присоединились к общемировой тенденции: технологии ИИ все шире применяется в целях реализации функций и компетенций органов государственной власти. Персональные данные, базы данных и алгоритмы все чаще используются в государственном управлении и процессе принятия решений, их распространение в публичной сфере оказывает значительное влияние, как положительное, так и отрицательное[3].

С точки зрения Б.Н. Комахина, доктора юридических наук, профессора, положительная роль ИИ в государственной управленческой деятельности государственных служащих заключается в следующем: 1) повышается эффективность этой деятельности при

[1] Ibid.

[2] Катанандов С.Л., Ковалев А.А. Технологическое развитие современных государств: искусственный интеллект в государственном управлении // Государственное и муниципальное управление. Ученые записки. – 2023. – № 1. – С. 177; Ли Яо. Особенности нормативно-правового регулирования генеративного искусственного интеллекта в Великобритании, США, Евросоюзе и Китае // Право. Журнал Высшей школы экономики. – 2023. – Т. 16, № 3. – С. 252–255; Jemin Lee. Artificial Intelligence and International Law. – 2022. – P. 18.

[3] Jemin Lee. Op. cit. – P. 18–19.

анализе данных; 2) автоматизируются рутинные процессы и высокозатратные этапы управленческой деятельности (обработка заявлений и различных документов, заполнение форм, управление базами данных и составление планов и др.); 3) растет уровень обслуживания граждан и взаимодействия с ними; 4) улучшаются процессы принятия решений, прогностическая аналитика; 5) изменяется структура кадров, открываются возможности для профессионального развития и обучения в новых областях; 6) появляются более эффективные услуги. Примерами являются электронное правительство и онлайн-платформы для связи с государственными органами и др.; 7) повышается прозрачность государственных процессов, например при помощи систем, которые отслеживают целевое использование бюджетных средств при реализации государственных проектов; 8) оптимизируется процесс распределения ресурсов и минимизируется коррупционная составляющая, улучшаются процессы распределения ресурсов, эффективно управляющие финансами и охватывающие те области, которые нуждаются в первоначальной помощи[1].

Исследуя вопросы классификации приложений ИИ, включая системы цифровой безопасности и финансового анализа, так называемые «проактивные» услуги, «умные» системы в сфере адаптивного обучения, прокторинга, а также здравоохранения, беспилотного транспорта, управления в сфере миграции и др., А.А. Косоруков, старший преподаватель факультета государственного управления МГУ им. М.В. Ломоносова, кандидат политических наук, указывает, что наиболее важным и широко востребованным направлением применения ИИ является комплексное решение административных задач в сфере оказания государственных услуг гражданам и организациям, в том числе обеспечение своевременного и релевантного реагирования на их запросы, прогнозирование потребностей различных групп населения или отдельных лиц и эффективное использование ресурсов[2].

Искусственный интеллект в государственном управлении также применяется государственными служащими при приняти решений, организации, и проведении государственных закупок,

[1] Комахин Б.Н. Совершенствование деятельности государственных служащих в условиях интеграции искусственного интеллекта: плюсы и минусы // Вестник Московского ун-та МВД России. – 2025. – № 1. – С. 75–76.

[2] Косоруков А.А. Технологии искусственного интеллекта в современном государственном управлении // Социодинамика. – 2019. – № 5. – С. 46.

например в целях повышения эффективности налоговой системы и др. Помимо достижения целевых показателей в деятельности ведомств технологии ИИ препятствуют внедрению «серых» схем в государственных закупках и сфере налогообложения, позволяют снизить вероятность организации преступных сговоров и способствовать раскрытию фактов мошенничества на государственной службе. То есть, результатом применения ИИ может стать повышение эффективности функционирования системы государственного управления в целом[1].

Перспективными областями применения ИИ в государственном управлении, по мнению Р.А. Пояркова из Среднерусского института управления филиала РАНХ и ГУ, могут стать: автоматизация обработки обращений граждан с использованием интеллектуальных систем анализа текста; внедрение предиктивной аналитики для прогнозирования социально-экономических показателей и оптимизации управленческих решений; создание интеллектуальных систем поддержки принятия решений для государственных служащих; использование ИИ для выявления потенциальных рисков и нарушений в сфере государственных закупок; применение технологий машинного обучения для оптимизации внутренних административных процессов и документооборота. Реализация этих направлений, полагает автор, может осуществляться через создание пилотных проектов на базе отдельных ведомств, разработку специализированных программных решений отечественными компаниями, формирование центров компетенций по внедрению ИИ в государственном секторе и организации системы переподготовки служащих для работы с новыми технологиями. Ключевыми компонентами внедрения предиктивной аналитики на основе ИИ в систему государственной службы РФ становятся: нейронные сети для прогнозирования временных рядов социально-экономических показателей; алгоритмы кластеризации для выявления групп схожих явлений и процессов; системы распознавания аномалий для раннего выявления отклонений от нормального развития ситуации; рекомендательные системы для формирования оптимальных управленческих решений[2].

[1] Там же.

[2] Поярков Р.А. Искусственный интеллект как инструмент оптимизации процессов принятия управленческих решений в системе государственной службы РФ // Общество: политика, экономика, право. – 2025. – № 2. – С. 80.

Рассматривая роль ИИ в публичном управлении и его правовое развитие в Российской Федерации, Т.А. Полякова, доктор юридических наук, профессор, заведующая сектором информационного права и международной информационной безопасности Института государства и права РАН, и Н.А. Троян, кандидат юридических наук, старший научный сотрудник указанного сектора, отмечают, что в ближайшей перспективе в России запланирован ряд масштабных проектов, связанных с внедрением ИИ в публичное управление[1]. Среди них, например, проект «Цифровое государственное управление» в рамках программы «Цифровая экономика Российской Федерации»[2], направленный на применение инновационных технологий в цифровых публичных сервисах и технологической трансформации инфраструктуры правительства. Также активно прорабатывается проект создания цифрового профиля как совокупности сведений о гражданах и юридических лицах, содержащихся в информационных системах, посредством регистров, реестров, кадастров и перечней персонифицированной информации. Приоритетным направлением признается цифровая трансформация публичного сектора посредством формирования единого федерального информационного ресурса[3], а также единого федерального информационного регистра сведений о населении[4], системы идентификации и аутентификации на основе биометрических данных[5] и др. Вместе с тем, по мнению ученых, в

[1] Полякова Т.А., Троян Н.А. Правовые вопросы использования технологий искусственного интеллекта в информационном обществе и в государственном управлении // Правовое государство: теория и практика. – 2024. – № 3. – С. 85–93.

[2] См.: Паспорт национального проекта «Национальная программа “Цифровая экономика Российской Федерации”», утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7 [Электронный ресурс]. – URL: https://digital.gov.ru (дата обращения: 21.04.2025).

[3] См.: Распоряжение Правительства РФ от 04.06.2017 № 1418-р «Об утверждении концепции и плана мероприятий (“дорожной карты”) по формированию и ведению единого федерального информационного ресурса, содержащего сведения о населении Российской Федерации».

[4] Федеральный закон от 08.06.2020 № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации».

[5] Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодатель-

России необходимо решить проблемы повышения эффективности использования технологий ИИ при оказании публичных услуг, а также устранить барьеры «информационного отличия» различных субъектов. Сохраняется необходимость достижения баланса интересов публичных органов власти и общества в контексте применения технологий ИИ, что, в свою очередь, должно способствовать формированию механизмов адаптации регулирования ИИ на перспективный период[1].

Ученые не только выявляют разновекторные направления применения технологий ИИ, но изучают тенденции и перспективы развития комплексного нормативного правового регулирования в этой сфере, в том числе выделяют следующие подходы и направления:

– сочетание различных методов в регулировании использования ИИ (правового, этического, технического и проч.);

– гарантии безопасности человека и его прав при использовании ИИ;

– сочетание комплексного концептуального регулирования ИИ с особенностями и потребностями незамедлительного решения наиболее острых проблем по отдельным технологиям ИИ (в сфере беспилотного транспорта, телемедицины, навигации, а также обработки больших данных и т.п.);

– правовая неопределенность и неоднозначность восприятия систем ИИ и роботов и др.;

– решение этических проблем при использовании ИИ, а также в сфере робототехники и др.[2]

В связи с развитием законодательства в сфере ИИ актуализируется проблема совершенствования концепции верховенства закона применительно к ИИ. Может ли верховенство закона – в том виде, в каком оно понимается в настоящее время и было задумано в прошлом – применяться к ИИ, контролировать его и ограничивать? – задает вопрос Пол Бёрджесс, автор книги «Искусственный интеллект и верховенство закона: необходимая эволюция

ные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации».

[1] Полякова Т.А., Троян Н.А. Указ. соч. – С. 90–91.

[2] Перспективные направления правового регулирования искусственного интеллекта. Указ соч. – С. 54–56.

концепции»[1]. Размышляя о «недалеком будущем» ИИ, в котором эти технологии будут использоваться для принятия решений органами государственной власти, автор выделяет три гипотетические ситуации, в которых ИИ мог бы использоваться при осуществлении власти: во-первых, при принятии административных решений; во-вторых, при создании вторичного (делегированного) законодательства и, в-третьих, при разработке первичного законодательства. В связи с этим рассматривается вопрос о том, может ли верховенство закона, в том виде, в каком оно понимается в настоящее время и было задумано в прошлом, – применяться к действиям ИИ. Другими словами, способен ли принцип верховенства закона и формы защиты, которые он призван обеспечить при осуществлении «власти» ИИ, ограничить эту «власть». П. Бёрджесс доказывает, что различные способы, с помощью которых обществом понимается верховенство закона, являются несоответствующими средствами для ограничения осуществления «власти» ИИ, и по этой причине концепция должна развиваться, чтобы соответствовать новым вызовам, которые ставит ИИ[2].

Риски и угрозы внедрения искусственного интеллекта в государственное управление

При использовании ИИ в контексте публичного управления и принятия соответствующих управленческих решений технические новации могут способствовать возникновению различных опасных ситуаций, которые создают опции для произвольного поведения. На это указывают практически все исследователи темы внедрения ИИ в государственном управлении. Однако комплексного подхода к пониманию и рассмотрению проблемы правового регулирования безопасности ИИ, нарушения этими технологиями закона в юридической литературе не прослеживается. Авторы книги «Цифровое управление: решение проблем, связанных с искусственным интеллектом» предлагают объединить социально-правовой подход применения закона к функционированию технологий ИИ с базовыми понятиями о системной безопасности – инженерной традиции, опирающейся как на научные данные, так и на реальную практику, которая рассматривает безопасность с тех-

[1] Burgess P. AI and the Rule of Law: The Necessary Evolution of a Concept. – 2024. – P. 3–5.

[2] Ibid.

нологической, системной и институциональной точек зрения. Результатом этого подхода является лексический и аналитический методы, которые позволяют государственным организациям выявлять места, где могут возникнуть возможности для произвольного поведения в государственных системах ИИ (public AI systems). На основе этого, с их точки зрения, могут быть разработаны законодательные и технологические меры по предотвращению, смягчению или устранению системных угроз и, таким образом, защитить граждан от произвольного осуществления властных полномочий[1].

С точки зрения Д.А. Репина, доктора социологических наук, ведущего научного сотрудника Института проблем передачи информации имени А.А. Харкевича РАН, среди ключевых угроз применения ИИ в государственном управлении в России – неправомерное использование персональных данных, алгоритмическая предвзятость, снижение контролируемости при принятии автоматизированных решений, потенциальная уязвимость к кибератакам. По мнению исследователя, некорректное или непродуманное применение технологий ИИ может привести к негативным социально-экономическим и политическим последствиям, т.е. стать деструктивным фактором в контексте государственной безопасности и достижения национальных целей развития России[2]. Автор предлагает классифицировать риски и угрозы, возникающие в процессе внедрения технологий ИИ в систему государственного управления, по следующим ключевым группам: 1) риски, связанные с гарантиями прав и свобод граждан; 2) недостаточно высокая степень доверия со стороны населения к ИИ-технологиям; 3) частичная эффектность ИИ или ошибки в принятии решений; 4) недостаточная квалификация государственных служащих в сфере ИИ-технологий; 5) угрозы и вызовы для национальной безопасности, киберугрозы (утечка конфиденциальной информации, манипуляции с государственными данными, потенциальный взлом в системах критически важных инфраструктурных объектов)[3].

Сочетается с вышеназванной классификацией рисков и вызовов их перечень, представленный Б.Н. Комахиным. По его мне-

[1] Digital Governance: Confronting the Challenges Posed by Artificial Intelligence. Op. cit. – P. 184.

[2] Репин Д.А. Технологии искусственного интеллекта как фактор совершенствования государственного управления: вызовы и угрозы // Экономика и управление. – 2025. – Т. 31, № 2. – С. 140–141.

[3] Там же. – С. 142.

нию, вызовы (риски), связанные с интеграцией ИИ в государственное управление, могут возникнуть в таких сферах, как: 1) этическая и правовая; 2) дискриминация; 3) доверие общества; 4) кадровое обучение государственных служащих, работающих с ИИ и их информированность о потенциальных рисках при использовании ИИ; 5) рабочие места. Так как ИИ способен эффективно выполнять человеческие функции, это создает риск увеличения безработицы в определенных областях; 6) человеческий фактор. Искусственный интеллект может упустить нюансы, которые свойственны только человеку (эмпатию и эмоциональный интеллект); 7) техническая. Как и любая технология, ИИ подвержен сбоям и ошибкам, возникающим в результате перегрузок, поломок или отключения электроэнергии. Ошибочные алгоритмы приводят к неправильным решениям и негативным последствиям[1].

Интересные позиции зарубежных ученых относительно вызовов и рисков применения ИИ в государственном управлении приводит в своем обзоре С.И. Коданева, ведущий научный сотрудник отдела правоведения ИНИОН РАН, кандидат юридических наук. Государственное управление с помощью ИИ в зарубежной научной литературе рассматривается как многоуровневая проблема, характеризующаяся системным сопротивлением из-за огромного количества вовлеченных лиц, скорости изменений и понимания неизбежности технологической трансформации. Автор приводит трехуровневую классификацию барьеров для внедрения ИИ в государственном управлении:

1) макроуровень требует нормативной трансформации определения прав и обязанностей как граждан, так и государственных чиновников, повышения их квалификации;

2) мезоуровень испытывает потребность в разработке новых способов измерения, мониторинга и оценки входных данных, обрабатываемой информации, полученных результатов и результатов воздействия на социум, что подразумевает разработку показателей эффективности деятельности государственных органов, качества услуг и оценки рисков;

3) микроуровень нуждается в устранении противоречий между легитимностью решений, предложенных ИИ, свободой усмотрения чиновников при оценке, использовании или отмене этих

[1] Комахин Б.Н. Указ соч. – С. 76–77.

решений и правами граждан и бизнеса, которые могут быть затронуты предложенными решениями[1].

Есть и так называемые «ловушки» ИИ, которые могут стать препятствием для внедрения ИИ в госуправление:

– ловушка фрейминга – неспособность смоделировать социальную систему целиком, включая общие социальные критерии, такие как справедливость;

– ловушка переносимости – неспособность понять, как перепрофилирование алгоритмических решений, разработанных для одного социального контекста, может вводить в заблуждение, быть неточным или иным образом наносить вред при применении к другому контексту;

– ловушка формализма – неспособность объяснить полный смысл социальных понятий, таких как справедливость, которые не могут быть включены в математические модели;

– ловушка волнового эффекта – неспособность понять, как внедрение технологии в существующую социальную систему изменяет поведение людей и уже сложившиеся ценности;

– ловушка солюционизма – неспособность признать возможность того, что лучшее решение проблемы может быть достигнуто без использования технологии[2].

Еще одну «ловушку» можно усмотреть в том, что «культура управленческого обновления с помощью искусственного интеллекта в государственном управлении предлагается с чрезмерно оптимистичной точки зрения, которая сводит проблемы управления к техническим аспектам»[3].

Внедрение ИИ в государственной сфере лежит в основе создания новой модели государственного управления, однако «цифровые инструменты в управлении могут стать слишком технократичными и это поставит под угрозу неприкосновенность частной жизни индивида, усилит неравенство граждан и территорий»[4].

---

[1] Коданева С. И Перспективы и риски внедрения искусственного интеллекта в государственном управлении // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2021. – № 1. – С. 136–137.

[2] Там же.

[3] Катанандов С.Л., Ковалев А.А. Указ. соч. – С. 181–182.

[4] Кайсарова В.П., Кайсаров А.А. Ценностно-ориентированный подход в государственном управлении как базис исследований искусственного интеллекта // Управление бизнесом в цифровой экономике: 7-я Междунар. конф. – Санкт-Петербург, 2024. – С. 375.

Важный аспект угроз технологий ИИ заметила также Ли Яо (Институт сравнительного правоведения при Китайском политико-правовом университете). По ее мнению, технологии ИИ влияют в целом на традиционную культуру и национальный суверенитет. Риски заключаются в том, что в базовой структуре данных, если говорить о генеративном ИИ, ныне преобладают англоязычные данные, и выходной контент неизбежно имеет иное понятие об истории и культуре неанглоязычных стран, таких как Китай и Россия, и порой генерирует искаженную информацию. В этом случае население может подсознательно изменить свое долгосрочное понимание традиционной культуры и национальных особенностей после длительного получения такой информации, содержащей ценностные предубеждения. Если генеративный ИИ будет использоваться в когнитивной войне на национальном уровне, то это создаст угрозу подрыва национального суверенитета[1].

Существенным видом риска применения ИИ в государственном управлении, как отмечалось выше, признаются *угрозы* и *вызовы верховенству закона*, как основному механизму борьбы с произволом в государственных системах ИИ. Вызовы для права нормативного, казуистического и морального характера «предупреждают, что верховенство права может быть заменено на “верховенство технологии” (‘rule of technology’), привести к формам антиутопии. Приложения машинного обучения ставят под сомнение состязательность – фундаментальный элемент верховенства права. Иными словами, применение систем ИИ в государственном управлении может быть фактором, подрывающим верховенство закона»[2].

Приложения ИИ опосредуют задачи или работу человека и, таким образом, могут привести к непредсказуемому его поведению при использовании или проектировании систем ИИ. Исследование такого поведения с социально-технической точки зрения содержит систематическую оценку вызовов и возможностей для обеспечения верховенства закона в условиях растущей автоматизации и расширения процесса принятия решений. *Во-первых*, существует общая угроза того, что технический компонент подменит

[1] Ли Яо. Особенности нормативно-правового регулирования генеративного искусственного интеллекта в Великобритании, США, Евросоюзе и Китае // Право. Журнал Высшей школы экономики. – 2023. – Т. 16, № 3. – С. 249.

[2] Digital Governance: Confronting the Challenges Posed by Artificial Intelligence / ed. K. Prifti, E. Demir, J. Krämer, K. Heine, E. Stamhuis. – 2024. – P. 191.

собой, частично или полностью, функции институтов в практике государственного управления. В этой ситуации верховенство закона отходит на второй план. *Во-вторых*, верховенство закона как институциональное явление оказывает влияние как на поведение людей, так и на форму и функции ИИ. *В-третьих*, ограничения влияния верховенства закона вытекают из характера применяемых технических средств и от того, как люди используют как технические, так и институциональные средства. В итоге субъекты, реализующие в своей деятельности принцип верховенство закона, например должностные лица органов государственной власти и управления, государственные служащие, зависят от субъектов из других областей общественной практики и знаний, например от разработчиков приложений ИИ. Тем не менее верховенство закона как фундаментальный принцип должно связывать параметры и спецификации, формирующие технический артефакт, и, следовательно, обусловливать практику разработки приложений ИИ, а также деятельность вовлеченных в это субъектов[1].

Заключение

Анализ исследований ученых позволяет констатировать, что:

1) эффективное применение ИИ в сфере государственного управления зависит от успешности использования технологий ИИ в различных сферах человеческой деятельности и в вопросах безопасности; это требует от государства пристального внимания к проблеме в целом, а также активной адаптации и внедрения наиболее результативных разработок на базе ИИ в свою деятельность. Данные технологии обладают возможностью значительно увеличить результативность государственного управления[2];

2) перспективы внедрения ИИ в процессы государственного управления существенно связаны с потенциалом и общим вектором цифровизации государственного механизма[3];

3) влияние практик ИИ на государственное управление попрежнему остается весьма неопределенным, возможности госу-

[1] Ibid. – P. 194–195.

[2] Косоруков А.А. Указ соч. – С. 43–57.

[3] Там же.

дарственных органов в этой связи выходят за рамки общепринятых границ и в значительной степени зависят от контекста[1];

4) изменение динамики государственного управления с помощью методов ИИ требует защиты граждан от произвольного использования властных полномочий государством при посредничестве государственных систем ИИ[2];

5) применение ИИ в государственном управлении – комплексная задача, для решения которой необходим не только технический потенциал автоматизации (цифровизации), но и ряд таких факторов, как политические, экономические, нормативные, демографические, социальной приемлемости и др.[3];

6) несмотря на высокий потенциал для внедрения технологий ИИ в государственной сфере и растущее число стран, делающих на это ставку в процессе собственной модернизации, ИИ для государственных нужд все еще составляет область исследований, в которой сегодня недостаточно данных и методик по всесторонней диагностике этических и правовых проблем, связанных с интенсивным применением этих сложных технологий[4];

7) для внедрения предиктивной аналитики на основе ИИ в систему государственной службы РФ необходимо создать специализированную отечественную платформу ИИ для обработки разнородных данных, разработать систему объяснимого ИИ, создать специализированные центры разработки ИИ-решений, сформировать размеченные датасеты (структурированный набор обработанных и разложенных по понятным категориям данных), разработать стандарты интеграции с государственными информационными системами, создать программы подготовки профильных специалистов, разработать протоколы безопасности, внедрить систему оценки эффективности[5];

8) верховенство закона как фундаментальный принцип должен связывать параметры и спецификации технологий ИИ, прак-

[1] Digital Governance: Confronting the Challenges Posed by Artificial Intelligence. Op. cit. – P. 273; Kennedy R. Op. cit. – P. 209–233.

[2] Ли Яо. Указ соч. – 245–267.

[3] Поярков Р.А. Указ. соч. – С. 78–83;

[4] Катанандов С.Л., Ковалев А.А. Указ соч. – С. 174–182.

[5] Поярков Р.А. Указ. соч. – С. 78–83.

тики разработки и применения технологий ИИ, а также деятельность вовлеченных в эту работу субъектов[1];

9) ИКТ и алгоритмы могут поддерживать верховенство закона, обеспечивая доступ к юридическим текстам и повышая прозрачность судебной системы[2];

10) внедрение технологий ИИ существенно трансформирует отношения между гражданами и государством, государством и бизнесом, гражданином и бизнесом, отношения в системе государственного управления в целом. Права граждан нуждаются в особенной и эффективной защите в условиях потенциально негативного воздействия используемых государством и бизнесом технологий ИИ в социальной сфере[3];

11) эра искусственного интеллекта уже наступила и требует соответствующего нормативно-технического и нормативно-правового регулирования[4].

[1] Burgess P. AI and the Rule of Law: The Necessary Evolution of a Concept. Op. cit. – P. 3–15.

[2] Ibid.

[3] Перспективные направления правового регулирования искусственного интеллекта: монография / под ред. А.В. Минбалеева. – 2023. – С. 42–43.

[4] Там же.

УДК 34.096 DOI: 10.31249/iajpravo/2025.03.11

РЯБЦЕВА Е.В.[1] ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В МЕДИЦИНЕ: ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ И БЕЗОПАСНОСТИ (Обзор)

Аннотация. В данном обзоре представлены новые исследования, рассматривающие вопросы применения искусственного интеллекта в медицине и проблемы правового регулирования отношений, возникающих в связи с расширением внедрения технологий искусственного интеллекта в сферу здравоохранения. Анализируется французское и европейское законодательство с точки зрения обеспечения баланса между интересами пациентов и развитием искусственного интеллекта в медицине. Показаны преимущества и риски использования искусственного интеллекта в различных областях медицины. На основании анализа действующего законодательства раскрываются различные подходы к установлению юридической ответственности за вред, причиненный интеллектуальными роботами.

Ключевые слова: искусственный интеллект; здравоохранение; правовое регулирование; медицинское страхование; робот-компаньон; юридическая ответственность.

RYABTSEVA E.V. Application of Artificial Intelligence in Medicine: Legal Regulation and Security Issues (Review)

Abstract. This review presents new research examining the use of artificial intelligence in medicine and the problems of legal regulation of relations arising from the expansion of the introduction of artificial intelligence technologies in the healthcare sector. The article ana-

[1] © *Рябцева Екатерина Владимировна*, доцент кафедры теории права, государства и судебной власти Российского государственного университета правосудия им. В.М. Лебедева, кандидат юридических наук, доцент, эксперт Совета судей РФ.

lyzes French and European legislation in terms of ensuring a balance between the interests of patients and the development of AI in medicine. The advantages and risks of using artificial intelligence in various fields of medicine are shown. Based on the analysis of current legislation, various approaches to establishing legal liability for harm caused by intelligent robots are revealed.

Keywords: artificial intelligence; healthcare; legal regulation; medical insurance; companion robot; legal responsibility.

Для цитирования: Рябцева Е.В. Применение искусственного интеллекта в медицине: вопросы правового регулирования и безопасности (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4: Государство и право. – 2025. – № 3. – С. 147–158. – DOI: 10.31249/iajpravo/2025.03.11

Введение

Развитие искусственного интеллекта, его интеграция в прикладные отрасли медицинской науки закономерно создают основу для значимых изменений в здравоохранении. Ученые полагают, что «проникновение» технологий ИИ в практическую медицину несет в себе положительный потенциал, который может существенно повысить уровень здравоохранения, качество и доступность медицинской помощи [2, с. 35]. В то же время возникает ряд проблем, связанных с обеспечением безопасности персональных данных пациентов, к которым имеет доступ ИИ, и с юридической ответственностью за вред, причиненный роботами, используемыми в медицинской деятельности, и др. Решение этих проблем посредством правового регулирования использования ИИ позволяет, с одной стороны, максимально гарантировать защиту прав пациентов, с другой – снять необоснованные препятствия для развития искусственного интеллекта в медицине.

В настоящее время опубликовано значительное количество работ, посвященных разным аспектам применения ИИ в здравоохранении как одного из перспективных направлений развития современного общества. Комплексные исследования в данной сфере являются важной и неотъемлемой частью развития современной медицины. Остановимся кратко на некоторых их них.

Искусственный интеллект, здравоохранение и право

Книга с таким названием [3] представляет собой комплексное исследование – коллективную монографию, редакторами которой являются Гильем Джулиа, старший преподаватель частного права и уголовных наук в университете Сорбонна Париж-Норд (Франция), и Энн Фошон, декан факультета права, политических и социальных наук этого же Университета, и Рашед Канавати, исследователь в области компьютерных наук в названном Университете.

В монографии анализируются различные аспекты применения ИИ в медицине, в том числе для диагностики тех или иных заболеваний, прогнозирования развития здравоохранения, популяризации здорового образа жизни с помощью цифровых сервисов, использования роботов для ухода и помощи больным и др., рассматриваются проблемы правового регулирования использования ИИ в медицине.

Предложенная в исследовании модель применения ИИ в медицине, по мнению редакторов книги, направлена на реализацию современной персонализированной медицины и может способствовать определению «терапевтической стратегии, которую следует применять для каждого пациента» [3, p. 17–18].

Для выражения мнения по этическим вопросам, возникающим при использовании большого объема данных, редакторы работы обратились к «концепции точной медицины» (concept of precision medicine), основанной на том, что «каждый пациент определенным образом становится уникальным случаем» [Ibid, p. 19].

По мнению авторов, переход от «массовой лечебной медицины» к «персонализированной медицине» актуализирует некоторые проблемные вопросы, связанные с гарантиями обеспечения квалифицированной медицинской помощи. Вместе с тем рассмотрение пациента как уникального субъекта лечения было всегда неотъемлемой частью медицинской деятельности. Клятва Гиппократа напоминает о степени, в которой врач «допущен в частную жизнь пациентов». В связи с этим в книге приводят перечень обязанностей по отношению к пациентам, предусмотренный п. 32–55 Французского кодекса медицинской этики (French code of medical ethics; принят Ассоциацией врачей Франции в 1975 г. (в ред. 1995 г.)), подтверждающий особый статус пациента в медицинском праве. Кроме того, Французский кодекс медицинской этики предусмат-

ривает обязанность врача «лично обеспечить пациенту добросовестную, современную помощь на основе приобретенных научных знаний и при необходимости привлечение для оказания помощи компетентных специалистов» [Ibid, p. 19]. Этот общий лейтмотив соблюдения этических норм в отношении пациентов при использовании ИИ сохраняется в монографическом исследовании при анализе различных вопросов темы, таких как использование ИИ в медицинском страховании, юридическая ответственность роботов, применяемых в медицине и т.д.

Использование искусственного интеллекта и обеспечение безопасности персональных данных пациентов. Обеспечение безопасности персональных данных пациентов при использовании ИИ поднимает проблему нехватки медицинских ресурсов и безопасности персональных данных пациентов. Один из авторов монографии – Энн Каммиллери (Anne Cammiller), профессор публичного права Университете Сорбонна Париж-Норд, провела анализ активно используемых в настоящее время цифровых приложений в области здравоохранения, которые при правильном использовании способствуют должному функционированию государственной и частной медицины и безопасности обрабатываемых данных о здоровье. Однако для гарантии их целостности требуется создание мощных стратегий кибербезопасности для обеспечения устойчивости приложений [Ibid, p. 4–6].

В книге приводятся примеры киберпреступлений в медицине. Например, WannaCry – крайне вредоносная вирусная программа, совершившая кибератаку на британскую систему здравоохранения в 2017 и 2020 гг., привела к краже медицинских данных более 2300 человек. В 2021 г. Франция пострадала от киберкражи данных, затронувшей более 1,4 млн пациентов из AP – HP (Assistance Publique – Hôpitaux de Paris). Эти данные включали «личность, номер социального страхования и контактные данные пациентов, прошедших тестирование, а также личность и контактные данные медиков, лечивших их, характеристики и результаты проведенных тестов». В последующем были созданы специальные программы для защиты персональных данных пациентов, например приложение Stop COVID и т.д. [Ibid].

Использование искусственного интеллекта в медицинском страховании как одно из направлений политики государства в области здравоохранения. Отдельная тема в книге посвящена применению ИИ в медицинском страховании как одному из направлений политики здравоохранения во Франции. На основе специальных

алгоритмов разрабатываются приложения, которые используются для поддержания здорового питания, лучшего сна, контроля физической активности и т.д. Новые маркетинговые стратегии ориентируются на здоровье в смысле благополучия, а не нацеливаются на конкретное заболевание. Такие стратегии используются в области медицинского страхования и направлены на внедрение технологий «самоактуализации»[1].

Новый рынок медицинского страхования в стране опирается на распространение цифровых устройств, побуждающих страхователей ежедневно придерживаться «здорового образа жизни». Данные устройства не только представлены как новый сегмент рынка страхования, но и оказывают положительное влияние на укрепление здоровья населения.

По мнению Э. Каммиллери, во Франции наблюдается переход от «электронного здравоохранения» (информационно-коммуникационные технологии, применяемые в здравоохранении) к «мобильному здравоохранению» (здравоохранение на мобильных устройствах), которое основано на обеспечении доступа не только к данным застрахованного лица, но и к его мобильному устройству, подключенному к специальным программам, ориентированным на здоровый образ жизни застрахованных лиц [Ibid, p. 46–47].

Страхование здорового образа жизни дает возможность тем, кто ведет такой образ жизни, платить меньше страховых взносов.

Проблемы юридической ответственности в связи с использованием роботов, наделенных искусственным интеллектом, в медицине. Значительная часть работы посвящена вопросам юридической ответственности роботов, наделенных искусственным интеллектом и применяемых в сфере оказания медицинских услуг. Авторы подробно проанализировали данную проблему и делают вывод о том, что с одной стороны, робот-компаньон заботится о человеке, опекает его; с другой стороны – устройство является интеллектуальным роботом, способным к самообучению. Гильем Джулия предлагает ввести юридическую ответственность за вред, причиненный роботом-компаньоном (companion robot): законодательно закрепить доктринальное различие между хранителем структуры (формы и внутренней конструкции), т.е. производителем (manufacturer) робота и хранителем-опекуном (guardian) пове-

[1] *Самоактуализация* – стремление человека к полному раскрытию своего потенциала, максимальному использованию своих способностей и возможностей. URL: https://psychology.academic.ru/ (дата обращения: 04.04.2025).

дения робота. Так, пользователь считается хранителем поведения робота, в то время как его производитель остается хранителем структуры робота [Ibid, p. 75–80]. Преимущество такого подхода, по мнению Г. Джулии, заключается в том, чтобы возложить опеку над роботом и, следовательно, бремя его ремонта – на производителя робота-компаньона, а не на его пользователя, когда повреждение является результатом ошибки конструкции, а не ошибки использования [Ibid, p. 84].

Применительно к проблеме ответственности за вред, причиненный роботом-компаньоном, и во французском, и в европейском законодательстве были созданы два специальных режима ответственности. Первый относится к дорожно-транспортным происшествиям, второй – к неисправным товарам. Первый вид режима представлен специальной схемой компенсации для потерпевших в результате дорожно-транспортных происшествий, появившийся вместе со знаменитым «Законом Бадинтера» 1985 г., который расширил права жертв ДТП. Согласно этому акту, перевозчик, как правило, не может возложить вину за происшествие на пассажира. В подтверждении данного вывода Кассационный суд Франции постановил, что «электрическая коляска, медицинское устройство, предназначенное для перевозки человека с инвалидностью, не является наземным механическим транспортным средством» [Ibid, p. 96–100].

Хотя описанный правовой режим ответственности, касающийся ДТП, не может быть применен к роботам-компаньонам, однако два его элемента можно было бы применить – страховое обязательство и понятие вовлеченности. Г. Джулия полагает, что было бы целесообразно также обязать производителей робота-компаньона оформить страховку для покрытия риска использования самообучающегося робота [Ibid, p. 98–101].

Второй вид правового режима ответственности за возмещение вреда предусматривает ответственность за причинение вреда неисправным товаром. Производителями роботов-компаньонов фактически являются: производители материального носителя и соединительной части, разработчики алгоритма и программного обеспечения. Кроме того, в случае ущерба, причиненного неисправным товаром, который является частью другого продукта, закон предусматривает солидарную ответственность производителя составной части и лица, осуществившего сборку частей в единый объект. Это положение облегчает возмещение ущерба, причиненного роботом-компаньоном [Ibid, p. 102–103].

Европейское законодательство устанавливает две презумпции ответственности за причинение вреда: презумпцию дефектности товара, вызвавшего ущерб, и презумпцию причинно-следственной связи между дефектом товара и ущербом. Система ответственности, вызванная дефектным товаром, не требует доказательства вины производителя такого товара; она, тем не менее, требует доказательства дефекта указанного товара и причинно-следственной связи между таким дефектом и ущербом, понесенным жертвой. Преимущество такого правового регулирования заключается в том, что оно учитывает трудности доказывания, с которыми сталкивается потерпевший «из-за определенной технической или научной сложности», что часто будет иметь место в случае ущерба, причиненного интеллектуальным роботом [Ibid, p. 104]. По мнению авторов, совершенствование правового регулирования ИИ и включение в правоотношения роботов должно проходить постепенно [Ibid, p. 110].

Искусственный интеллект в здравоохранении: применение, риски, этические и социальные последствия

Данный обзор практики применения ИИ под названием «Искусственный интеллект в здравоохранении: применение, риски, этические и социальные последствия [4] подготовлен группой экспертов для европейского парламента и его сотрудников в целях повышения эффективности работы клиницистов, улучшения диагностики и лечения, а также оптимизации распределения человеческих и технических ресурсов. Его авторы – Карим Лекадир (Karim Lekadir), директор «Лаборатории искусственного интеллекта в медицине» в Университете Барселоны; Джанлука Квальо (Gianluca Quaglio), член экспертной группы «Будущее науки и Технологии» Европейского парламента; Анна Целиудис Гармендия (Anna Tselioudis Garmendia), преподаватель Школы общественного здоровья, медицинского факультета Имперского колледжа Лондона; Кэтрин Галлин (Catherine Gallin), преподаватель факультета математики и компьютерных наук Университета Барселоны, член Лаборатории искусственного интеллекта в медицине. В этом по жанру в справочно-информационном материале рассматриваются основные клинические, социальные и этические риски, связанные с использованием ИИ в здравоохранении: потенциальные ошибки врачей, причиняющие вред пациентам; предвзятость и усиление неравенства в отношении здоровья; отсутствие прозрачности и

доверия; уязвимость к хакерским атакам и нарушениям конфиденциальности данных и др.

В области клинической практики в работе рассматриваются как реализованные, так и планируемые проекты внедрения ИИ в различные области медицины – радиологию, кардиологию, неотложную медицину, хирургию, прогнозирование заболеваний, адаптивные вмешательства, уход на дому и психическое здоровье и др. Что касается биомедицинских исследований, то в работе раскрывается потенциальный вклад ИИ в клинические исследования, разработку лекарств, клинические испытания.

При этом обращается внимание и на трудности, связанные с ИИ в медицине. Отмечено, что в последнее время было разработано множество медицинских инструментов ИИ, однако на пути к их внедрению, интеграции и использованию в реальных клинических условиях существует множество препятствий, как то: ограниченное качество данных, их структура и возможность взаимодействия между разными клиническими центрами и электронными медицинскими картами; потенциальные изменения в отношениях между врачом и пациентом в связи с внедрением ИИ; расширенный и недостаточно регулируемый доступ к данным пациентов; отсутствие клинической и технической интеграции и функциональной совместимости инструментов искусственного интеллекта с существующими клиническими рабочими процессами и электронными системами здравоохранения и др.

Искусственный интеллект для медицины: прогресс, проблемы и перспективы

Еще одним интересным научным исследованием, посвященным искусственному интеллекту в медицине, является статья, подготовленная группой китайских ученых – «Искусственный интеллект для медицины: прогресс, проблемы и перспективы» [5]. В ней описан не только положительный опыт использования ИИ и перспективы его дальнейшего внедрения в медицину, но и обозначены различные, в том числе правовые и этические, проблемы в рассматриваемой теме.

Так, по мнению авторов, применение ИИ в медицине поднимает этические и правовые вопросы и создает проблему для защиты конфиденциальности и прав пациентов. Приложения ИИ собирают персональные данные пациентов, что требует соблюдения правил защиты конфиденциальности для минимизации риска

несанкционированного доступа со стороны злоумышленников. Невыполнение этого требования может нарушить право пациентов на информацию во время диагностики их здоровья и лечения. Следовательно, необходимы эффективные рамки регулирования и политики, которые решают этические проблемы, вопросы конфиденциальности, прозрачности алгоритмов и безопасности пациентов [5, p. 230–231].

Также авторы отмечают, что с быстрым развитием крупных языковых моделей, таких как ChatGPT и Claude в 2023 г., соответствующие правила часто обновлялись в крупных организациях. Например, администрация киберпространства Китая опубликовала «Временные меры по управлению генеративными службами ИИ», сосредоточившись на управлении политически и юридически чувствительным контентом, на оценке и отслеживании его рисков.

Авторы статьи указывают на то, что, несмотря на значительную привлекательность технологий ИИ в медицинских исследованиях, их практическое внедрение по-прежнему сталкивается с препятствиями. Первое из них связано с нормативными правовыми актами. В действующих нормативных правовых актах отсутствуют стандарты для оценки безопасности и эффективности систем ИИ. Чтобы преодолеть эту трудность, Управление по санитарному надзору за качеством пищевых продуктов и медикаментов США разработало рекомендации оценки систем ИИ. В первом руководстве системы ИИ классифицируются как «продукты общего оздоровления», которые слабо регулируются до тех пор, пока устройства предназначены только для общего оздоровления и представляют низкий риск для пользователей. Во втором руководстве обосновывается использование реальных фактических данных для оценки эффективности систем ИИ. И, наконец, в руководстве разъясняются правила адаптивного проектирования в клинических испытаниях, которые будут широко использоваться при оценке рабочих характеристик систем ИИ. Вскоре после опубликования этих рекомендаций платформа медицинской визуализации Arterys стала первой системой углубленного обучения, которая может помочь кардиологам диагностировать сердечные заболевания.

Вторым препятствием является обмен данными. Для эффективной работы системы ИИ должны постоянно обучаться на основе данных клинических исследований. Однако, как только система ИИ будет внедрена после первоначального обучения с использованием исторических данных, продолжение предоставления дан-

ных становится решающим вопросом для дальнейшего развития и совершенствования системы.

Сравнительное исследование нормативно-правового регулирования искусственного интеллекта в здравоохранении

В этой части обзора кратко остановимся на информационно-справочном издании «Глобальный атлас регулирования искусственного интеллекта», подготовленного коллективом авторов под редакцией А.В. Незнамова, в котором представлен сравнительный анализ законодательства 43 стран в области ИИ, в том числе в здравоохранении [1]. Для примера возьмем две страны. Так, в работе описывается новое законодательство в области медицинского страхования в Тайване, которое предполагает, что пациенты владеют смарт-картами «Карточка IC национального медицинского страхования» (National Health Insurance IC card), хранящими достаточно большой массив информации, начиная от контактных данных, даты рождения и заканчивая данными о посещениях врача, диагнозах, расходах на посещение врача, выписанных лекарствах. Данная информация заносится в специальную информационную сеть и используется для развития технологий ИИ в здравоохранении, при условии, что будут применены принципы анонимизации и защиты персональных данных [1, с. 72].

В Малайзии приняты специальные законы и ведомственные акты, которые регулируют сферу применения медицинских продуктов и услуг на основе использования ИИ. В стране регулирование медицинских устройств осуществляется Управлением по медицинским устройствам Малайзии в соответствии с положениями Закона Малайзии «О медицинских устройствах» 2012 г. (MDA 2012) и соответствующих подзаконных актов. В соответствии с положениями этого Закона любой инструмент, аппарат, приспособление, машина, программное обеспечение и материал на базе ИИ, которые обладают способностью диагностировать, предотвращать, контролировать, лечить заболевание или травму, исследовать, заменять или модифицировать, поддерживать анатомическую целостность или физиологический процесс организма, вероятно, охватываются термином «медицинское устройство». Положения Закона 2012 г. также регулируют различные требования правил классификации группировки и регистрации медицинского устройства. Управление медицинского оборудования Малайзии уполномочено в соответствии с законом MDA 2012 г.

лицензировать и выдавать разрешение на использование различных медицинских устройств [1, с. 247–250].

Заключение

Анализ научных публикаций, представленных в рассмотренном обзоре, позволяет сделать некоторые выводы относительно особенностей внедрения ИИ в медицину в современных условиях.

1. В сфере здравоохранения осуществляется интеграция разнообразных подходов ИИ при анализе большого объема данных о состоянии здоровья пациентов, что способствует переходу от «массовой лечебной медицины» к «персонализированной медицине».

2. Использование информационных технологий, в частности телемедицины, позволяет обеспечить доступность и своевременность медицинской помощи.

3. С помощью ИИ можно проводить точную и быструю диагностику заболеваний, анализировать большие данные, прогнозировать заболевания и повышать эффективность работы, обучения и переподготовки кадров, повышать результативность медицинских исследований и дистанционной диагностики, а также выявлять генетические заболевания и т.д.

4. Одно из направлений развития ИИ – применение ИИ в медицинском страховании. На основе специальных алгоритмов разработаны приложения, которые используются для поддержания здорового питания, лучшего сна, контроля физической активности и т.д. Новые маркетинговые стратегии ориентируются на здоровье в смысле благополучия, а не нацеливаются на конкретное заболевание. Такие стратегии используются в области медицинского страхования и направлены на внедрение технологий «самоактуализации».

5. Современные исследования ИИ выявляют основные клинические, социальные и этические риски, связанные с использованием ИИ в здравоохранении: потенциальные ошибки и причинение вреда пациентам; риск предвзятости и усиления неравенства в отношении здоровья; отсутствие прозрачности и доверия; а также уязвимость к хакерским атакам и отсутствие эффективных гарантий защиты конфиденциальности и прав пациентов.

6. В сравнительных исследованиях, посвященных ИИ, раскрывается содержание законов различных государств, которые регулируют этические проблемы, вопросы конфиденциальности,

прозрачности алгоритмов и безопасности пациентов, обеспечения конфиденциальности их данных.

Список литературы

1. Глобальный атлас регулирования искусственного интеллекта: Вектор БРИКС / под ред. А.В. Незнамова. – Москва, 2024. – 377 с.
2. Привалов С.А. Технологии искусственного интеллекта в сфере обеспечения права на охрану здоровья, доступную и качественную медицинскую помощь: перспективы и проблемы регулирования // Вестник Саратовской гос. юрид. акад. Сер. Право, 2021. – № 4 (141). – С. 34–43.
3. AI, Healthcare and Law / eds. by Guilhem Julia, Anne Fauchon, Rushed Kanawati. – London; New York: Wiley & Sons, Inc., 2024. – P. 17–18.
4. Artificial Intelligence in Healthcare. Applications, Risks, and Ethical and Societal Impacts / K. Lekadir, G. Quaglio, A. Tselioudis Garmendia, C. Gallin. – 2022. – 69 p. – URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729512/EPRS_STU(2022)729512_EN.pdf(дата обращения: 21.04.2025).
5. Artificial Intelligence for Medicine: Progress, Challenges, and Perspectives / Fei Jiang, Yong Jiang, Hui Zhi, Yi Dong, Hao Li, Sufeng Ma, Yilong Wang, Qiang Dong, Haipeng Shen, Yongjun Wang // The Innovation Medicine. – 2023. – Vol. 1, N 2. – P. 230–243. – URL: https://radensa.ru/wp-content/uploads/2024/05/230.full_.pdf?ysclid=m9k2d4if3t904719927 (дата обращения: 07.04.2025).

УДК 34.096 DOI:10.31249/iajpravo/2025.03.12

ГРОГОЛЬ А.Г.[1] «АЛГОРИТМИЧЕСКАЯ» МЕДИЦИНА: НАПРАВЛЕНИЯ ВНЕДРЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ПРОБЛЕМЫ ЦИФРОВОГО БУДУЩЕГО ЗДРАВООХРАНЕНИЯ (Обзор)

Аннотация. Данная работа представляет собой обзор книги зарубежных авторов и отражает их попытку поиска эффективных механизмов имплементации технологий искусственного интеллекта в такую жизненно важную сферу общественной жизни, как здравоохранение. Рассматриваются современный правовой опыт Франции по внедрению технологий искусственного интеллекта в сферу здравоохранения, правовые и этические вопросы, возникающие в «алгометрической» медицине, а также проблемы ответственности субъектов, связанных с разработкой и функционированием искусственного интеллекта, защиты персональных данных пациентов и др. Представлены результаты исследований создания экосистемы для внедрения искусственного интеллекта в медицинскую практику.

Ключевые слова: искусственный интеллект; здравоохранение; медицина; правовое регулирование, персональные данные; алгоритмы, диагностика заболеваний; медицинское страхование.

GROGOL A.G. “Algorithmic” Medicine: Areas of Artificial Intelligence Implementation and Problems of the Digital Future of Healthcare (Review)

Abstract. This work is a review of a book by foreign authors and reflects their attempt to find effective mechanisms for the implementation of artificial intelligence technologies in such a vital area of public life as healthcare. The article examines the current legal experience of

[1] *Гроголь Анастасия Георгиевна,* младший научный сотрудник отдела правоведения ИНИОН РАН.

France in the implementation of artificial intelligence technologies in the field of healthcare, legal and ethical issues arising in “algometric” medicine, as well as issues of responsibility of subjects related to the development and operation of artificial intelligence, protection of personal data of patients, etc. The results of research on the creation of an ecosystem for the introduction of artificial intelligence into medical practice are presented.

Keywords: artificial intelligence; healthcare; medicine; legal regulation, personal data; algorithms, diagnosis of diseases; medical insurance.

Для цитирования: Гроголь А.Г. «Алгоритмическая» медицина: направления внедрения искусственного интеллекта и проблемы цифрового будущего здравоохранения (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 3: Государство и право. – 2025. – № 3. – С. 159–170. – DOI:10.31249/iajpravo/2025.03.12

Введение

В обзоре представлены научные статьи из Университета Сорбонна-Париж-Норд, включенные в монографию «Программные приложения для здравоохранения: Искусственный интеллект, здравоохранение и право» (“Healthcare Applications. In AI, Healthcare and Law”) исследователей: Филиппа Батифулье (Philippe Batifoulier), профессор; Селин Блауд-Рей (Céline Bloud-Rey), старший преподаватель, директор Института судебных исследований; Анн Каммиллери (Anne Cammilleri), профессор; а также Николас Da Силва (Nicolas da Silva), кандидат педагогических наук в Люксембургском университете, Томас Лефевр (Thomas Lefèvre), доктор медицинских наук, профессор и др.).

В центре внимания авторов – вопросы влияния искусственного интеллекта на сферу здравоохранения и развитие таких его направлений, как «алгоритмическая медицина», охватывающая ИИ-диагностику заболеваний, персонализированную медицину, автоматизацию и алгоритмизацию медицинских задач, система структурирования данных о пациенте, онлайн-доступ к медицинским услугам и др.

Термин *алгоритмическая медицина* (*algorithmic medicine*) определяется как совокупность инструментов и систем, основанных на алгоритмах компьютерной обработки, внедренных в медицину [2, p. 13]. Однако помимо ИИ и сопутствующих ему техноло-

гий ключевым признается здоровье, определяемое ВОЗ как состояние полноценного физического, психического и социального благополучия. Следовательно, толкование данного термина не ограничивается наличием болезни или недуга[1].

Особое внимание в книге уделяется так называемым технологиям «повседневности», включая мобильные приложения, цифровые платформы по мониторингу текущего здоровья пациентов, предупреждению вреда здоровью, а также иным цифровым технологиям в сфере здравоохранения.

Авторы утверждают, что сегодня, с учетом широкого применения ИИ при проведении операций, диагностики, профилактики и при прогнозировании заболеваний, невозможно обойти цифровой скрининг – набор диагностических процедур, направленных на выявление заболеваний пациента и электронную обработку и хранение данных. Современное поколение стало непосредственным участником «медицинского искусственного интеллекта» (Medical AI), понимаемого как совокупность технологий по получению, визуализации, медицинских результатов и увеличения объема и способов хранения медицинских данных [2, p. 13–14].

Концепция «Закон для цели» (“Goal Law”) в правовом регулировании ИИ

Все системы, действующие на основании ИИ, как подчеркивает С. Блауд-Рей, должны содержать набор математически выверенных, надежных алгоритмов, который позволил бы анализировать проблемы не только с технической, но и с юридической точки зрения. Закон, в условиях внедрения ИИ в различные сферы деятельности, в том числе в здравоохранение, следует воспринимать «как цель, т.е. в качестве государственного инструмента для грамотного законодательного закрепления способов сбора, обработки, структурирования, форматирования данных». Законодатель, разрабатывая нормативно-правовой акт, должен определить цель и предвидеть результат его реализации, социальные, этические и технические последствия применения [2, p. 15].

По мнению С. Блауд-Рей, особую важность приобретает «закон для цели», поскольку интересы, преследуемые законодателем,

[1] Preamble to the Constitution of the World Health Organization. Available online on the WHO website. – URL: https://www.who.int/about/governance/constitution (дата обращения: 01.04.2025).

могут спровоцировать конфликт ценностных ориентировок. Принятие такого закона, безусловно, подразумевает определенную иерархию в целях, которые должны быть достигнуты, что предполагает формулировку суждения о конкретных оценочных категориях, выбранных законодателем в качестве обязательных [Ibid].

Совмещая «медицинский искусственный интеллект» и концепцию «закон для цели» законодательные органы Франции приняли ряд специальных нормативных правовых актов. Так, Закон Франции N 2019–774 от 24.07.2019 г. «Об организации и преобразовании системы здравоохранения» (LOI n° 2019–774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, OTSS) был принят в качестве глобальной стратегии в области искусственного интеллекта, в котором законодатель акцентировал внимание на двух четко определенных целях: 1) данные о состоянии здоровья должны подлежать оценке и систематизации. В рамках продолжения данной тенденции президентом Франции был инициирован проект по созданию Центра медицинских данных (Health Data Hub), задача которого – реализация французской стратегии в области продвижения ИИ; 2) цифровые технологические новации должны соответствовать сохранению высокого уровня защиты частной жизни [2, p. 16–17].

Алгоритмический подход, основанный на взаимодействии «врач – пациент»

Статья 17 Закона Франции N 2021–1017 от 02.08.2021 г. «О биоэтике» (La loi n°2021–1017 du 2 août 2021 sur la bioéthique en France)[1] регулирует использование медицинских технологий, предназначенных для алгоритмической обработки данных медицинским работником. Согласно п. I указанной статьи Закона «О биоэтике» на специалиста (медицинского работника) возлагается обязательство предоставлять информацию о применении алгоритмической обработки с использованием ИИ в процессе получения и интерпретации медицинских результатов пациенту. Пункт II данной статьи содержит обязательство медицинского работника информировать пациента об участии ИИ в анализе данных о его состоянии здоровья. Пункт III обязывает разработчиков доступно

[1] La loi n°2021–1017 du 2 août 2021 sur la bioéthique en France. –. URL: https://www.legifrance.gouv.fr/jorf/id/JORFARTI000043884399 (дата обращения: 03.04.2025).

объяснять пациентам деятельность медицинского работника при применении алгоритмов ИИ в работе с их медицинскими данными. Пункт IV рассматриваемой статьи предусматривает прерогативу Высшего органа здравоохранения Франции (High Authority for Health), а также Национальной комиссии по информатике и свободам (The Commission nationale de l'informatique et des libertés, CHIL) на определение типа и характеристик медицинских устройств, изделий, которые могут использоваться и применяться в работе с персональными данными пациента:

1) медицинский работник, решивший использовать устройство алгоритмической обработки данных пациента для профилактики, диагностики или оказания ему помощи, должен убедиться, что пациент был проинформирован о применении ИИ для анализа его личных медицинских данных и предупредить о возможных последствиях применения ИИ;

2) медицинские работники должны быть в равной мере, как и пациент, информированы об использовании механизмов обработки данных о пациентах, а также иметь свободный доступ к ним с согласия пациента;

3) разработчики алгоритмического механизма обработки медицинских данных должны позаботиться о доступности и объяснимости его функционала для медработников и пациентов.

Таким образом, законодатель поспособствовал соблюдению и сохранению достоверности информации о пациенте при проведении алгоритмической обработки массива медицинских данных [2, p. 21–23].

Использование программного приложения (application) в сфере здравоохранения

Размышляя над данным вопросом, Э. Каммиллери определяет термин «программное приложение» как «ограниченную область обработки, для которой написано программное обеспечение», или как «программное обеспечение или набор программ, предназначенных для облегчения использования при осуществлении определенной задачи». Использование таких приложений в области здравоохранения представляет собой огромный вклад, позволяющий пациентам улучшить свое здоровья путем самоконтроля.

В последнее время, как отмечает автор, количество поисковых интернет-заявок в различных направлениях здравоохранения и медицины возросло. Среди 50 лучших приложений для здраво-

охранения интернет-пользователи предпочитают поисковую систему Google AllergoBox (приложение для лечения аллергии), которое помогает людям определить характер аллергии, подобрать правильный повседневный рацион, согласующийся с диетическими потребностями клиента. Медицинское приложение Gluci Check позволяет отслеживать потенциальный риск развития диабета. Кроме того, в верхней части списка находится приложение Santé.fr (официальное приложение для предоставления государственных услуг в сфере здравоохранения) [3, p. 33–35].

Риски возникновения вреда здоровью в результате использования цифровых сервисов

Различные программные приложения медицинского сектора служат вспомогательным средством поддержания здоровья не только для докторов, но и для пациентов. Тем не менее такое преимущество нередко используется для кибератак, поскольку обеспечение кибербезопасности либо вообще не предусмотрено приложениями, либо находится в зачаточном состоянии. Так, лишь в некоторых городах Франции функционируют центры передового опыта в области кибербезопасности, которые создают условия для устойчивого развития соответствующей информационной экосистемы на территориях, включая здравоохранение [3, p. 44].

19 октября 2022 г. Европейский парламент и Совет ЕС приняли Регламент (2022/2065) «О цифровых услугах» (Regulation on a Single Market For Digital Services)[1], который предусматривает механизм реагирования на возникновение угроз в данной сфере (ст. 36). Согласно ст. 34 этого Регламента, при использовании ИИ учитываются принципы человеческого достоинства, свободы, плюрализма средств массовой информации и прав детей, предусмотренные в ст. 24 Хартии основных прав, принятой ЕС 2008 г. [3, p. 44–46].

Применение технологий ИИ в области медицинского страхования

Нововведением в практическом применении ИИ в сфере здравоохранения, как подчеркивают Ф. Батифулье и Н. da Силва,

[1] Regulation on a Single Market For Digital Services. – URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj (дата обращения: 06.04.2025).

является особая система медицинского страхования с применением механизмов ИИ. Такие электронные информационные инструменты направлены на стимулирование клиентов вести здоровый образ жизни, более выгодный с точки зрения общественного здравоохранения [1, p. 53].

Частные страховые компании в медицинском секторе (коммерческие и некоммерческие) стали предлагать услуги расширенного спектра, направленные на поддержание общего здоровья страхователей. К таким онлайн-продуктам автор относит: мониторинг питания, стимулирование отказа от курения, поддержку физической активности, управление стрессом и др. Это достигается за счет развития цифровых технологий и распространения электронных устройств, считывающих базовые показатели здоровья пациентов. Они основаны на алгоритмах, которые используются медицинскими страховщиками для оптимизации решений и управления поведением страхователей. Так, компании коммерческого и некоммерческого страхования через различного рода приложения сравниваются по критерию «здоровой полезности», изобретая каждый раз новые функции, например при фиксации ежедневно производимых шагов, мониторинге веса и др. Такие приложения следят, чтобы клиент сжигал достаточное количество калорий или поддерживал форму. Их можно также применять для соблюдения здорового питания, повышения качества сна и т.д. [Ibid].

Новые маркетинговые стратегии демонстрируют достижения позитивных маркеров и показателей уровня здоровья, т.е. благополучных медицинских результатов, однако, как замечают авторы, совершенно не нацелены на выявление новых заболеваний. В то время как одни частные страховые компании стремятся предоставить экспертные оценки состояния здоровья для принятия решения об объеме вреда ввиду нездоровых привычек пациента, подлежащего финансированию, страховщику, другие – усилить уровень человеческой осмотрительности с помощью технологий «самооценки» (self-esteem technology) своего здоровья. Ф. Батифулье и Н. да Силва отмечают, что поощрение здорового поведения (которое должно быть принято во внимание страхователями) также выгодно для страховщиков, поскольку это позволяет совершать расходы, подлежащие покрытию, снизить риск банкротства и выполнять долговые обязательств [1, p. 53].

Ф. Батифулье и Н. да Силва полагают, что такой обновленный рынок медицинского страхования опирается прежде всего на

распространение цифровых устройств и технологий, побуждающих страхователей придерживаться здорового образа жизни. Такая тенденция выступает не только новым сегментом, но и решает важнейшую задачу по обеспечению общественного здравоохранения. Принимая во внимание возможность влиять на сознание клиентов через агитацию к ЗОЖ, страховщики отказались от части личной выгоды в пользу общественного благополучия [Ibid]. Так, по их мнению, развитие рынка медицинского страхования осуществляется в «высших интересах» пациента. От страховщика больше не ожидают, что он будет оплачивать последствия заболевания, а, скорее, ожидают, что он будет выполнять задачу помощника или ментора пациента для поддержки «наилучших повседневных практик» (best daily practices).

Таким образом, использование ИИ в области медицинского страхования для повышения человеческого интеллекта направлено на развитие рынка самостоятельной количественной оценки (self-quantification market) состояния здоровья человека. Несмотря на то что такие нововведения в медицинском страховании представляются как комплекс индивидуальных и коллективных мер по укреплению здоровья, они также влияют на изменение формы и формата бизнес-модели страховщиков, позволяя им повышать свой деловой престиж и стать защитниками общих интересов. В этом смысле, как указывают Ф. Батифулье и Н. да Силва, использование ИИ в области медицинского страхования является средством, доступным для страховых компаний в целях увеличения прибыли и повышения своего делового престижа [1, p. 53–55].

Примером такого подхода служит программа Vitality, разработанная Generali во Франции в 2016 г. Эта программа на момент ее внедрения в сферу страхования здорового образа жизни стала наиболее распространенной. В этой программной системе, первоначально введенной в Южной Африке (ЮАР), а в последствии заимствованной другими странами, компании, придерживающиеся стратегии заключения коллективных договоров о медицинском страховании (с работниками определенной организации) или о пенсионном обеспечении, а также участники этих договоров могут воспользоваться специальной программой, в рамках которой все действия, направленные на сохранение или улучшение здоровья, вознаграждаются в виде премий, бонусов или иных поощрений. Каждый участник обязуется зафиксировать индивидуальный план достижения прогрессивного ЗОЖ: количество шагов, предприни-

маемых в день, покупки фруктов и овощей, профилактические визиты к врачу и т.д. [1, p. 56–58].

Также авторы анализируют деятельность швейцарской страховой компании Helsana, которая, следуя примерам наилучшей бизнес-практики, ввела аналог такой бонусной системы в форме накопления «профилактических» баллов (prevention points) с помощью шагомера, встроенного в качестве приложения на смартфоне. Особенностью такой программы стала возможность конвертации накопленных балов в ваучеры, которые можно было обналичить либо пожертвовать на благотворительность в Швейцарский Красный Крест или Фонд Теодоры. Эти программы являются дополнением к коллективным договорам о медицинском страховании, которые работодатель заключает для своих сотрудников, но не напрямую с сотрудниками на индивидуальной основе.

Таким образом, новые методы медицинского страхования направлены на побуждение страхователей придерживаться поведения, которое считается лучшим для индивидуального и общественного здоровья. Приложения для электронного здравоохранения представлены на рынке не только как коммерческие продукты, но и как средство участия в достижении общей цели – улучшения здоровья населения [1, p. 61–63].

Образование экосистемы цифровых данных для анализа и разработки алгоритмов

Размышляя над термином «экосистема данных» (data ecosystem), Т. Лефевр полагает, что это понятие ввиду своего полиморфного характера отлично подойдет для описания совокупности различных систем электронных данных – в общем, о состоянии здоровья, в частности о применении ИИ. Автором выделяется особый актор – Google, который за последнее десятилетие увеличил и укрепил свое влияние настолько, что стал, пожалуй, единственным «игроком», диктующим условия и непосредственно формирующим цифровую экосистему данных. Так, компания Google, создавая и развивая экосистему данных, аккумулирует информацию, ориентируясь на отдельно взятого человека (независимо от его профессиональных и гражданских прерогатив), на основании собранных данных об используемых им цифровых услугах, электронных приложениях, поисковых запросах и иных цифровых следах, оставленных на пространстве сети Интернет [4, p. 72].

По мнению Т. Лефевр, именно сфера здравоохранения с наибольшей силой сопротивляется широко распространяющейся цифровой революции, по крайней мере, в большинстве различных форм охраны и защиты сферы здравоохранения. Одной из главных причин, на которые ссылается профессор, выступает отсутствие экономического содержания в понятии «здоровье». Автор убежден, что термин «здоровье» не является товаром (good) с точки зрения экономической выгоды [Ibid].

Т. Лефевр приводит также и иные причины повышенной сопротивляемости сферы здравоохранения влиянию современных технологий: сложность нормативно-правового регулирования, дисбаланс частных и публичных источников финансирования, затруднения, возникающие при определении субъекта ответственности. Это происходит потому, что большинство компаний частного сектора предпочитают избежать возможных юридических рисков в целях сохранения имиджа компании. Перечень названных причин повышенной резистентности не является исчерпывающим, и Т. Лефевр предлагает оперативное решение правовой неопределенности, устранение пробелов в правовом регулировании в области здравоохранения и применения технологий ИИ в этой сфере. По его мнению, между активно развивающимися цифровыми технологиями и различными сложившимися в процессе функционирования институтами здравоохранения существуют противоречия и даже конфронтация [Ibid].

Цифровизация здравоохранения изнутри

Данный подход, по мнению Т. Лефевра, заключается в попытке объяснить причину цифровизации здравоохранения. Технологии ИИ используются не только в качестве оцифровки данных, но и как способ их администрирования, хранения в электронных информационных системах. В данном случае распространение цифровизации в сфере здравоохранения происходит от источника (медицинских данных), который, будучи переведенным в дигитализированный формат, нуждается в применении других технологий по администрированию, хранению и обеспечению доступа к данным для пациентов и медицинских работников [4, p. 73–74].

Например, во Франции административное «пилотирование» данными (administrative piloting) открывает путь к более легкому и слаженному управлению здравоохранением. Французская программа медицинской информатизации PMSI (Programme de

médicalisation du système d'information) была внедрена в больницах сначала на локальном уровне, а после удачной апробации была интегрирована в объединенную национальную систему. Такой успех достигнут благодаря деятельности Французского технического агентства по предоставлению информации о больничном уходе (ATIH, Technical Agency for Information on Hospital Care), в чью компетенцию входит определение продолжительности пребывания пациента в больнице и др.

В дальнейшем на федеральном уровне появилась еще одна программа применения ИИ в здравоохранении. Французская национальная система данных о здравоохранении (SNDS, Système national des données de santé n.d.) ставит своей целью совершенствование и развитие баз данных о потреблении медицинских услуг. Тем не менее важно отметить, что все базы данных и функционирующие на основе программ информационные системы претерпевают множество изменений, дополнений и правок [Ibid].

Таким образом, здравоохранение во Франции включает в себя два аспекта. С одной стороны, внедрение информационных технологий (например для оцифровки данных и их анализа, для получения данных из дополнительных обследований), с другой – внедрение медико-административных систем данных, изначально разработанных для управления деятельностью [Ibid].

Заключение

Анализ содержания рассматриваемой книги подтверждает, что это – комплексное и динамичное исследование, раскрывающее различные аспекты применения ИИ в сфере здравоохранения и такие важные вопросы, как правовые и этические нормы, регулирующие функционирование ИИ в медицине, перспективы практического использования ИИ для повышения качества диагностики и лечения серьезных заболеваний, обеспечения конфиденциальности цифровых данных через «сберегающие» алгоритмы ИИ, ответственности разработчиков ИИ и др. Особое внимание авторы сосредоточили на процессах трансформации рынка медицинского страхования под влиянием ИИ, перехода его на новый аппарат суждений и ценностных ориентиров.

Книга раскрывает механизмы и особенности страхования здоровья, основанные на сборе и анализе данных о действиях пациентов с использованием цифровых сервисов и подключенных устройств, в целях поддержания здорового образа жизни во Фран-

ции. Подчеркивается, что, хотя такие модели могут стимулировать ЗОЖ и снижать затраты на здравоохранение, они также несут в себе риски дискриминации и усиления социального неравенства.

Список литературы

1. Batifoulier P., Da Silva N. Behavioral Insurance: The Latest Trick of Capitalism? // Healthcare Applications. In AI, Healthcare and Law / eds G. Julia, A. Fauchon, R. Kanawati. – 2024. – P. 53–70.
2. Bloud-Rey C. Introduction // Healthcare Applications. In AI, Healthcare and Law / eds G. Julia, A. Fauchon, R. Kanawati. – 2024. – P. 13–27.
3. Cammilleri A. Healthcare Applications // Healthcare Applications. In AI, Healthcare and Law / eds G. Julia, A. Fauchon, R. Kanawati. – 2024. – P. 31–51.
4. Lefèvre T. Artificial Intelligence and Health: Description of the Ecosystem Required for an Effective Use of AI // Healthcare Applications. In AI, Healthcare and Law / eds G. Julia, A. Fauchon, R. Kanawati. – 2024. – P. 71–98.

НОВЫЕ КНИГИ НА ПОЛКАХ ФУНДАМЕНТАЛЬНОЙ БИБЛИОТЕКИ ИНИОН РАН

УДК 34.096, 342 DOI: 10.31249/iajpravo/2025.03.13

ЕРЕМИНА Е.А.[1] РЕЦЕНЗИЯ НА КНИГУ: КОНСТИТУЦИОННЫЕ ВЫЗОВЫ В АЛГОРИТМИЧЕСКОМ ОБЩЕСТВЕ / под ред. Х.-В. Миклица, О. Полличино, А. Райхмана, А. Симончини, Дж. Сартора и Дж. де Грегорио.
EREMINA E.A. [Book review]. – Book review: Constitutional Challenges in the Algorithmic Society / ed. by Hans-W. Micklitz, Oreste Pollicino, Amnon Reichman, Andrea Simoncini, Giovanni Sartor and Giovanni De Gregorio. – Cambridge: Cambridge University Press, 2022. – 330 p.

Ключевые слова: алгоритмы; алгоритмическое общество; искусственный интеллект; конституционное право; основные права и свободы; цифровые платформы.

Keywords: algorithms; algorithmic society; artificial intelligence; constitutional law; fundamental rights and freedoms; digital platforms.

Для цитирования: Еремина Е.А. [Рецензия] // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4: Государство и право. – 2025. – № 3. – С. 171–183. – Рец. на кн.: Constitutional Challenges in the Algorithmic Society = Конституционные вызовы в алгоритмическом обществе / ed. by Hans-W. Micklitz, Oreste Pollicino, Amnon Reichman, Andrea Simoncini, Giovanni Sartor and Giovanni De Gregorio = под ред. Х.-В. Миклиц, О. Полличино, А. Райхмана, А. Симончини, Дж. Сартора и Дж. де Грегорио. – Cambridge: Cambridge University Press, 2022. – 330 p. – DOI: 10.31249/iajpravo/2025.03.13

[1] © *Еремина Елизавета Анатольевна*, доцент кафедры предпринимательского права факультета «Высшая школа финансового права и государственного аудита» Института правоведения ФГАОУ ВО «Российский государственный гуманитарный университет», кандидат юридических наук.

Появление новых технологий всегда бросало вызов социальному, экономическому, правовому и идеологическому укладу. Конституционное право в не меньшей степени подвержено влиянию подобных изменений, поскольку государство обязано формулировать соответствующий правовой ответ. Развитие оборота цифровых данных и алгоритмического анализа, использование предиктивной аналитики с последующей манипуляцией поведением пользователей или без нее, представляют уникальные проблемы для конституционного права, как на законодательном, так и на теоретическом уровнях.

Данные проблемы разбирают авторы сборника трудов «Конституционные вызовы в алгоритмическом обществе» (Cambridge univ. press, 2022), вышедшего в свет под редакцией Х.-В. Миклица (H.-W. Micklitz), профессора экономического права в Центре передовых исследований Роберта Шумана Европейского университетского института; О. Полличино (O. Pollicino), профессора конституционного права Университета Боккони и члена Исполнительного совета Европейского агентства по основным правам; А. Райхмана (A. Reichman), профессора конституционного права Университета Хайфы; А. Симончини (A. Simoncini), профессора конституционного права в Университете Флоренции; Дж. Сартора (G. Sartor), профессора правовой информатики Университета Болоньи и профессора правовой информатики и теории права Европейского университетского института; Дж. Де Грегорио (G. De Gregorio), научного сотрудника Центра социально-правовых исследований Оксфордского университета. В подготовке проекта приняли также участие 25 ученых-юристов и практиков из различных стран.

Представленный сборник трудов является результатом двухлетней работы исследовательской группы IACL «Алгоритмическое государство, рынок и общество» и посвящен исследованию конституционных проблем, порождаемых алгоритмическим обществом.

Авторы сборника «Конституционные вызовы в алгоритмическом обществе» полагают, что с развитием информационных технологий и формированием алгоритмического общества появились новые угрозы соблюдению прав и свобод личности, а также принципам демократии. Отмечается, что границы юрисдикций нарушаются, а прежние доктрины и процедуры, разработанные еще в докибернетическую эпоху, не всегда способны фиксировать нарушения прав в соответствующие временные рамки. Все это требует либо корректировки пределов конституционно-правового регули-

рования, в контексте подчинения цифровых платформ конституционному праву, либо пересмотра соотношения публичного и частного правового регулирования.

Исследователи в своих статьях обращаются к наиболее актуальным проблемам современного права и пытаются показать, как изменились внутривластные отношения в алгоритмическом обществе, каковы новые нормы материального и процессуального права, защищающие людей и демократические ценности, как частные лица могут воздействовать на инновационные компании и какие требуется сформулировать правовые стимулы, чтобы обеспечить подотчетность цифровых платформ, и др.

Главная цель, которую поставил перед собой исследовательский коллектив – выстроить таксономию (систему) конституционных вызовов алгоритмического общества, акцентируя внимание на конкретных проблемах.

Целью обусловлена и структура книги, которая состоит из введения и трех частей, разделенных в свою очередь на главы.

В первой части рассматриваются вызовы, стоящие перед основными конституционными правами и демократическими ценностями в алгоритмическом обществе. В частности, подчеркивается то, как стремительное использование алгоритмов в различных областях, включая правосудие, полицию и общественное благосостояние, может привести к предвзятым и ошибочным решениям, усилению неравенства, подрыву базовых конституционных прав, в том числе права на частную жизнь и свободы слова.

Вторая часть посвящена правовому регулированию и политике в сфере алгоритмического общества. Обозначаются проблемы непрозрачности и предвзятости как самих алгоритмических систем, так и субъектов, участвующих в регулировании этих технологий.

В третий части фокус внимания сосредоточен на роли и обязанностях частных субъектов в контексте различий их конституционного статуса и возможных угроз. Подчеркивается, что частный сектор является значимым субъектом, выполняющим функции, отражающие, в некоторой степени, публичные полномочия.

Введение, кроме вступительной части, состоящей из краткой характеристики работы, включает статью редакторов издания О. Полличино и Дж. Де Грегорио, посвященную роли конституционного права в алгоритмическом обществе.

Авторами подчеркивается, что в цифровой экономике данные и информация являются основными активами. И, хотя технологии оказывают положительное влияние на все общество, они

также приводят к новым конституционным вызовам, прежде всего непрозрачности и отсутствию подотчетности в сфере алгоритмических технологий, так называемой «алгократии» – власти алгоритмов (p. 3–4).

О. Полличино и Дж. Де Грегорио указывают, что технологии ИИ могут способствовать совершенствованию обеспечения соблюдения правовых норм, а также повышению эффективности оказания государственных услуг. Но современные вызовы побуждают законодателей к соблюдению баланса между рисками и инновациями при создании правовой базы. В этих условиях доктрина горизонтального эффекта (the horizontal effect doctrines) и новые материальные и процессуальные права представляются перспективными средствами правовой защиты (p. 16–17). В связи с этим следует согласиться с позицией авторов, полагающих, что основной задачей конституционных демократий может стать ограничение усиления власти цифровых платформ, что предполагает определение конституционных рамок, в которых государственная и частная власть будут связаны гарантиями и процедурами.

Первая часть сборника «Алгоритмы, свобода и основные права» открывается главой «Основные права и верховенство закона в алгоритмическом обществе», написанной профессорами конституционного права Университета Флоренции А. Симончини (A. Simoncini) и Э. Лонго (E. Longo). Прежде всего они приводят слова выдающегося немецкого и американского философа, представителя Франкфуртской школы, Герберта Маркузе, который размышлял о влиянии технического прогресса на состояние и реализацию прав и свобод в современном обществе (p. 28–29). Авторы, развивая его мысль, отмечают, что одной из наиболее очевидных областей, где эта проблема находит свое воплощение, становится государственная и личная безопасность. Как следствие этого процесса происходит увеличение государственного и частного надзора в сочетании с растущими угрозами политическим и гражданским правам и свободам (p. 29).

Наиболее значительные проблемы, по их мнению, возникают из-за растущей мощности алгоритмов, основанных на аналитике больших данных при машинном обучении, используемых для автоматизации принятия решений. Для устранения данной проблемы часть ученых и политиков призывают ввести ограничения в отношении IT-компаний, поскольку антимонопольное законодательство не подходит для этой цели. Другие требуют установления процессуальных гарантий, которые бы позволили индивидам ос-

паривать решения алгоритмов, повлекших существенные последствия для их жизни (p. 30).

А. Симончини и Э. Лонго полагают, что, учитывая все технологические риски, необходимо создать «гибридное» конституционное право, которое не только направлено на защиту основных прав человека, но и выражает эту необходимость на языке технологий. Одной из предлагаемых авторами мер должны стать требования к образованию специалистов в сфере технологий, которые должны были бы привить им понимание необходимости защиты персональных данных, человеческого достоинства и защиты свободы (p. 41).

Глава «Неотъемлемое право на надлежащую правовую процедуру в эпоху искусственного интеллекта: ограничение договорного перехода в сторону автоматизированного судопроизводства» подготовлена профессором права Бруклинской школы права Ф. Паскуале (F. Pasquale).

Автор поднимает важнейшую проблему множественности случаев ошибок автоматизированного вынесения судебных и административных решений на основе неверных данных, ложных фактических предположений и ошибочного правоприменения и отмечает, что растущее использование автоматизированных систем создает потенциальные риски для соблюдения права на надлежащую правовую процедуру.

В этой статье Ф. Паскуале пытается понять, почему правовые ценности должны сдерживать усилия по «ускорению» дел с помощью статистических методов и машинного обучения и указывает на необходимость увязывания дебатов о надлежащей роли автоматизации правоприменения с требованиями к принятию обоснованных решений (p. 55–56).

Следующая статья – «Конституционные проблемы в эпоху эмоционального искусственного интеллекта» – подготовлена профессором права Левенского католического университета П. Валке (P. Valcke), научным сотрудником Австралийского национального университета Д. Клиффордом (D. Clifford) и научным сотрудником Левенского католического университета В.К. Дессерсом (V.K. Dessers).

В своей Декларации о манипулятивных возможностях алгоритмических процессов от февраля 2019 г. Комитет министров Совета Европы предупреждает о растущей способности машинного обучения не только предсказывать выбор, но и влиять на эмоции, мысли и даже действия индивидов (p. 57).

«Эмоциональный искусственный интеллект» и «эмпатические медиа» – это новые понятия, используемые для обозначения субдисциплины «эмоциональные вычисления» и технологий, способных анализировать эмоциональную жизнь пользователей и соответствующе реагировать на нее. Авторы подчеркивают, что, несмотря на серьезные споры относительно их точности, внедрение технологий эмоционального искусственного интеллекта получает все более широкое распространение во многих сферах, как государственного управления, так и в частном секторе, что порождает опасности, исходящие от использования алгоритмических инструментов, способных не только контролировать экономическим выбором индивидов, но и манипулировать их социальным и политическим поведением (p. 59).

П. Валке, Д. Клиффорд и В.К. Дессерс рассматривают некоторые юридические и этические проблемы, связанные с появлением эмоционального ИИ и его манипуляционного потенциала, а также пытаются выработать рекомендации по совершенствованию законодательства. Основное внимание в этой главе уделяется европейской правовой базе и использованию эмоций в коммерческих целях, хотя некоторые замечания также актуальны в контексте внедрения ИИ в государственном секторе или политике.

Научный сотрудник Европейского университетского института М. Катандзарити (M. Catanzariti) стал автором следующей главы в сборнике – «Алгоритмическое право: производство законов с помощью данных или производство данных с помощью закона?».

Эта глава логично разделена на четыре части, в которых описываются общие черты и различия между сущностью правовой бюрократии и алгоритмами, рассматривается связь между моделью законотворчества, основанной на данных и алгоритмической рациональностью, разбираются различные мнения в рамках социально-правового подхода к алгоритмическому регулированию, а также подвергается критике идея создания законов с помощью данных как продукта правовой культуры. М. Катандзарити рассматривает проблему соответствия алгоритмической рациональности с веберовской концепцией юридической рациональности. Утверждается, что алгоритмическое наблюдение упрощает реальность, вычисляя вероятность наступления определенных фактов на основе повторяющихся действий, а алгоритмы формируют человеческое поведение. Сила алгоритмов в значительной степени заключается в предсказании социального поведения. Вместе с тем автор

ставит под сомнение идею о том, что техническое невмешательство может достичь цели алгоритмической нейтральности и объективного принятия решений (p. 78).

С. Кастетс-Ренар (C. Castest-Renard), профессор частного права Университета Оттавы – автор статьи «Права человека и алгоритмическая оценка воздействия для прогонстической деятельности полиции» обращается к исследованию роли систем алгоритмизированного принятия решений (Algorithmic Decision Systems, ADS), используемых в области уголовного правосудия и прогностической деятельности полиции. Правоохранительные органы используют такие системы для предупреждения преступной деятельности и распределения полицейских ресурсов. С их помощью определяются места наиболее вероятного совершения преступлений в определенный промежуток времени, а также выявляются потенциальные жертвы или правонарушители на основе разнообразных данных.

Однако С. Кастетс-Ренар подчеркивает одну из самых важных и критических проблем алгоритмизации права – подобные системы нарушают основные права и гарантии уголовного судопроизводства. Это ставит вопросы о принятии этических норм для укрепления конституционных прав (p. 102), а также об использовании алгоритмизированной оценки воздействия (Algorithmic Impact Assessment) для снижения рисков, связанных с использованием автоматизированных систем принятия решений (Automated Decision (-making / -support) System, ADS) (p. 105).

Автор справедливо отмечает, что конституционные права должны подкрепляться не только этическими принципами, но и конкретными практическими инструментами, учитывающими риски при принятии решений в профилактической работе полиции. Он указывает на необходимость для европейского законодателя обращения к опыту Канады и принятия акта, аналогичного Канадской директиве об автоматизированном принятии решений и политики (AIAs) (p. 110). В очерке подчеркивается, что данная политика должна реализовываться на уровне регулирования всего Европейского союза, а не отдельных государств-членов.

Вторую часть сборника «Правовое регулирование и политика» открывает статья профессора конституционного права Хайфского университета А. Райхмана (A. Reichman) и профессора философии права Болонского университета и Европейского университетского института Дж. Сартора (G. Sartor) «Алгоритмы и регулирование».

Авторы подробно рассматривают юридические дебаты о перспективах и ограничениях «алгоритмизации» или «механизации» права и государственного управления, включая использования систем ИИ и машинного обучения. По мнению А. Райхмана и Дж. Сартора, закон и его принципы способны сочетаться с инновациями на основе применения ИИ, а действия могут быть более эффективными. Однако соблюдение мер предосторожности все же необходимо. Так, человеческое присутствие незаменимо, в особенности если речь заходит об апелляции к сочувствию и состраданию, ценностным суждениям и способности реагирования на непредвиденные обстоятельства. Авторы указывают на потенциальные сценарии, связанные с рисками применения ИИ («технорегулирования» или формулирование конкретных предписаний с помощью ИИ), которые могут привести к потере контроля над нормативной базой, лежащей в основе социального поведения.

Тема взаимовлияния новых технологий, политики и правовой сферы продолжена в главе «Искусственный интеллект, управление и этика: глобальные перспективы». Ее подготовили А. Дейли (A. Daly), профессор права Университета Стратклайда, Т. Хагендорф (T. Hagendorff), преподаватель медиа и технологий Университета Тюбингена, Ли Хуэй (L. Hui), ассоциированный научный сотрудник Шанхайского института естественных наук, М. Манн (M. Mann), старший преподаватель криминологии Университета Дикина, В. Марда (V. Marda), старший специалист по программам британской правозащитной орагнизации «АРТИКЛЬ19», Б. Вагнер (B. Wagner), доцент кафедры технологий и политики Делфтского технологического университета, и Уэйн Вэй Ван (W.W. Wang), доктор философии в области компьютерных юридических исследований в Университете Гонконга.

Авторы дают характеристику существующим представлениям о соответствии систем ИИ этическим стандартам и правовому регулированию в Австралии, Китае, Европейском союзе, Индии и Соединенных Штатах Америки. Особый акцент сделан на изучении процесса формирования подходов в сфере управления и этики ИИ мировыми лидерами в рассматриваемой области – Китаем и США, а также Евросоюзом, который потенциально может занять ведущие позиции в данной сфере. В работе констатируется, что в последние годы США начали догонять Китай и Европейский союз в вопросе правовых инициатив в данной отрасли. Важно, что в своей статье авторы не обошли стороной и другого, не менее существенного игрока, Индию, которая остается в стороне с отсутст-

вием четко сформулированного набора этических принципов в отношении ИИ. В свою очередь опыт Австралии демонстрирует, что страны подобные ей могут быть «последователями», но не «лидерами», поскольку они перенимают принципы и подходы, сформулированные другими странами. Отмечается, что форма и содержание норм, регулирующих использование искусственного интеллекта, должны оцениваться с позиции их эффективности в независимости от того – являются ли они нормами мягкого права, или императивными нормативными установлениями.

П. ван Кляйненбройгель (P. Van Cleynenbreugel), профессор европейского права Льежского университета, подготовил исследование «Нормативно-правовая база Европейского союза в алгоритмическом обществе: перспективный путь вперед или сотворение конституционного кошмара?», в котором отмечается, что процесс принятия алгоритмических решений ставит перед законодателями и регулирующими органами фундаментальную задачу – найти новые способы обеспечения соблюдения закона операторами и контролерами алгоритмических систем. Одним из способов справиться с ростом масштабов автоматизации принятия решений является введение дополнительных обязательств. П. ван Кляйненбройгель тщательно разбирает суть и особенности проектного регулирования, направленного на включение юридических требований в спецификации технологий, основанных на применении искусственного интеллекта. Представляется, что спецификации должны быть запрограммированы / закодированы в существующих или недавно разработанных алгоритмах (p. 202). Исследователь подробно рассматривает предпосылки для создания более развитой нормативной базы с учетом конституционного права ЕС, а также потенциальные трудности на этом пути. Он подчеркивает, что для развития законодательства и проектного регулирования в сфере ИИ требуется также политическая воля.

Глава «Что в коробке? Юридическое требование объяснимости при принятии решений с помощью вычислений в государственном управлении» подготовлена Х.П. Олсеном (H.P. Olsen), профессором юриспруденции Копенгагенского университета, и Т.Т. Хильдебрандтом (Th.T. Hildebrandt), профессором компьютерных наук Копенгагенского университета.Авторы отмечают, что применение технологий ИИ для поддержки процессов принятия решений, в том числе в сфере государственного управления, имеет множество преимуществ: быстрое реагирование, высокая экономическая эффективность, согласованность в принятии решений и

др. Однако оно же вызывает ряд проблем, среди которых предвзятость в процессе принятия решений, отсутствие прозрачности и устранение дискреционных полномочий человека (p. 220). Если подобные вызовы не подкреплены соответствующими средствами правовой защиты, то они могут препятствовать разработке эффективных систем из-за чрезмерно консервативного подхода. Авторы выражают справедливые опасения, связанные с внедрением систем автоматизированного принятия решений (Automated decision-making, ADM), которые связаны со страхами потери контроля над машиной ввиду излишнего доверия к ней, невозможности быть понятым другим человеком в случае замены всех юридических процессов алгоритмами, а также использования некорректных данных, которые могут привести к ложным решениям и нарушению закона (p. 221).

Для решения обозначенных проблем авторы предлагают сосредоточить внимание при внедрении ADM на требовании обоснованности, присущего административному праву (p. 221). Несомненным достоинством данной работы является тот факт, что в отличие от большей части современной литературы, в которой основное внимание уделяется контексту защиты персональных данных, авторы предлагают учитывать устоявшиеся традиции административного права. Отталкиваясь от датского законодательства, исследователи проводят сравнение с другими юрисдикциями Европы.

Системному осмыслению проблем, стоящих перед алгоритмическим обществом, посвящена *Третья часть* коллективного труда «Роли и обязанности частных субъектов», которую открывает глава «Обязанности компаний в алгоритмическом обществе», подготовленная Х.-У. Миклитцем (Hans-W. Micklitz), профессором экономического права и сотрудником Европейского университетского института, и А.Э. Вильянуэвой (A.A. Villanueva).

В данном исследовании внимание привлекает обращение к тому уровню регулирования, на котором частные лица и государства сотрудничают для обеспечения баланса между свободой компаний в ведении бизнеса за пределами государственных границ и, также ответственности государств. Авторы отмечают, что Европейский парламент уже поставил вопрос о создании независимого органа, наделенного полномочиями по проведению контроля и принятия надлежащих мер реагирования в случае возникновения рисков. Создание такого агентства могло бы обладать полномочиями в области мониторинга и надзора за соблюдением основных

прав в области окружающей среды, трудовых прав, прав потребителей и т.д. (p. 279).

Вместе с тем остается нерешенным фундаментальный вопрос об ответственности транснациональных компаний за границей. Исследователи указывают, что законодательство находится только на стадии формирования. Несомненно, имеется политическая воля, гражданское участие для его реализации, а компании применяют внутренние корпоративные стратегии по снижению рисков своей деятельности. Тем не менее проблемы с соблюдением законодательства и судебные тяжбы все же возникают.

С. Гэйрат (S. Gijrath), профессор права Лейденского университета, продолжает поднятую в статье выше в главе «Закон о защите прав потребителей как инструмент регулирования искусственного интеллекта». Исследователь отмечает, что возникновению алгоритмического общества способствуют два фактора: растущие возможности в области машинного обучения и доступность анализа данных с помощью алгоритмов. Возникает вопрос, как в данных условиях государство должно реагировать на новые технологии на цифровых платформах?

Использование ИИ способствует созданию платформами взаимозависимости спроса между участниками рынка, порождающей сетевые эффекты на цифровых платформах, и может привести к потенциально опасным для потребителей ситуациям. Европейская политика строится на том, что чтобы системы ИИ были прозрачными, отслеживаемыми и гарантировали человеческий надзор (p. 283).

С. Гэйрат предпринимает смелую попытку выяснить, насколько частное право может быть пересмотрено в сфере прав потребителей, чтобы служить инструментом регулирования искусственного интеллекта для предотвращения возможных неблагоприятных последствий. Вместо нисходящего регулирования последствий применения ИИ для защиты человеческого достоинства он предлагает рассмотреть подход «снизу вверх», направленный на расширение прав и возможностей потребителей на этапах управления взаимными транзакциями на цифровых платформах. Автор предлагает меры по совершенствованию законодательства о защите прав потребителей, в том числе в рамках предоставления потребителям права запрашивать исправления и удаления результатов непосредственно у производителей контента, а также путем совершенствования института защиты персональных данных, обрабатываемых ИИ и др.

В статье «Когда Алгоритм не является полностью надежным. Сотрудничество между технологиями и людьми в борьбе с разжиганием ненависти», написанной Ф. Казароза, научным сотрудником Европейского университетского института, ставится под сомнение целесообразность абсолютного доверия алгоритмам, с учетом их влияния на наши личные решения, а также их возможности в модерации контента. Исследовательница справедливо указывает на два направления влияния алгоритммов на принятия решений индивидами. Во-первых, результаты поисковых запросов, сформированные алгоритмами, могут определять решения человека, влиять на его интерпретацию искомой информации и дальнейшее принятие решений (p. 330). Во-вторых, следует принимать во внимание роль самих цифровых компаний, устанавливающих эти переменные, и тем самым влияющих на выбор пользователя. Всё это свидетельствует о более децентрализованном распределении полномочий и, как следствие, о стремлении к созданию системы подотчетности и ответственности.

Как представляется, особенно важным является то, что Ф. Казароза предупреждает о рисках чрезмерной цензуры, нарушения принципа свободы слова, а также предвзятого принятия решений в отношении меньшинств. Еще большую угрозу она видит в рисках разжигания ненависти (p. 302). Автор обращает внимание на то, что ИТ-компании, формируя коммуникационную экосистему, также предоставляют возможности для загрузки вредоносного контента. Стремительный рост количества высказываний, разжигающих ненависть, провоцирует все большее вмешательство государственных институтов с целью ограничения таких действий в Интернете.

Для преодоления коллизий национального правового регулирования и расширения возможности привлечения международных ИТ-компаний к этому процессу Комиссия ЕС использует подход совместного регулирования, при котором общие правила определяются государством совместно с IT-компаниями, что стимулирует их следовать им при условии отсутствия ответственности за несоблюдение обязательств. Это позволяет снизить риски чрезмерных блокировок, а также удаления легального контента.

Заключительная глава «Смарт-контракты и автоматизация частных отношений» подготовлена профессорами частного права Университета Боккони П. Сирена (P. Sirena) и Ф.П. Патти (F.P. Patti).

Авторы отмечают, что современные исследования влияния технологий на частное право, в том числе в области алгоритмических решений, цифровых платформ и технологий блокчейн, указывают на серьезные изменения в сфере свободы предпринимательства. Так, подчеркивается, что цифровые компании больше не являются только участниками рынка: они способны осуществлять контроль за условиями продажи товаров и услуг, зачастую сопротивляясь соблюдению обязательных норм (р. 315). Исходя из этого, исследователи предпринимают попытку рассмотреть технологические платформы блокчейна и смарт-контрактов как форму частной власти.

Резюмируя, следует отметить, что данный коллективный труд представляет собой основательное обобщение знаний о конституционных вызовах основным правам личности, демократии, роли политики и правового регулирования, а также трансформации правового положения частных субъектов в условиях повсеместной алгоритмизации и внедрения технологий в различные сферы общественной жизни. Заслуга авторов заключается еще и в том, что на протяжении всего исследования им удалось подчеркнуть важность сочетания таких ключевых характеристик, как статика и динамика права. Все рассматриваемые вопросы имеют фундаментальное значение не только для развития теории права, отдельных его отраслей, но и представляют несомненную пользу в области прикладных юридических наук. Немаловажным является и тот факт, что большинство исследователей, представивших свое видение – ученые из европейских университетов, а соответственно представители стран, где в настоящее время активно формулируются регулятивные механизмы в отношении цифровых платформ, что позволяет им давать оценку, основанную на возможно и предварительной, но все же апробированной нормативно-правовой базе.

УДК 34.096; 341.1/8 DOI: 10.31249/iajpravo/2025.03.14

САЛЬНИКОВА А.К.[1] РЕЦЕНЗИЯ НА КНИГУ: МОНТАСАРИ Р. КИБЕРПРОСТРАНСТВО, КИБЕРТЕРРОРИЗМ И МЕЖДУНАРОДНАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ЧЕТВЕРТОЙ ПРОМЫШЛЕННОЙ РЕВОЛЮЦИИ: УГРОЗЫ, ОЦЕНКА И ОТВЕТНЫЕ МЕРЫ.
SALNIKOVA A.K. [Book review]. – Book review: Montasari R. Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses. – Cham: Springer NATURE Switzerland AG, 2024. – 270 p.

Ключевые слова: киберпространство; искусственный интеллект; кибертерроризм; терроризм; права человека; дипфейки.
Keywords: cyberspace; artificial intelligence; cyberterrorism; terrorism; human rights; deepfakes.

Для цитирования: Сальникова А.К. [Рецензия] // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. Государство и право. – 2025. – № 3. – С. 184–191. – Рецензия на книгу: Montasari R. [Монтасари Р.] Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses = Киберпространство, кибертерроризм и международная безопасность в условиях Четвертой промышленной революции: угрозы, оценка и ответные меры. – Cham: Springer NATURE Switzerland AG, 2024. – 270 p. – DOI: 10.31249/iajpravo/2025.03.14

Книга Резы Монтасари, старшего преподавателя кафедры криминологии Университета Суонси (Уэльс, Великобритания), имеющего докторскую степень в области цифровой криминалистики, представляет собой комплексное междисциплинарное ис-

[1] *Сальникова Анастасия Кирилловна*, младший научный сотрудник Центра междисциплинарных исследований ИНИОН РАН.

следование ключевых вопросов, связанных с кибертерроризмом, киберпространством, национальной и международной безопасностью. Как отмечает сам автор в аннотации к книге, в ней критически рассматриваются сложные взаимосвязи между киберпространством, кибертерроризмом, национальной и международной безопасностью и технологией ИИ. В этих целях раскрываются двойственная природа этих элементов, их потенциал как для полезного и конструктивного, так и для вредоносного применения в контексте современных киберугроз. Автор исследует мотивы, методы и последствия кибертерроризма, оценивает международные усилия по противодействию кибертерроризму, показывает прогресс в выработке единого подхода к реагированию и устранению сохраняющихся проблем и разногласий между государствами, представляет практические стратегии, направленные на выявление террористических атак и реагирование на них. Много внимания Р. Монтасари уделяет анализу эффективности, сильных и слабых сторон реагирования на кибератаки и векторы для совершенствования стратегий их предупреждения и борьбы с ними.

Книга состоит из введения и четырех разделов: раздел I – «Понятие терроризма и контртеррористические стратегии»; раздел II – «Пространство кибертерроризма», посвящен изучению современной природы кибертерроризма неизбежности его угрозы национальной безопасности; раздел III – «Противодействие терроризму с помощью технологических ресурсов»; раздел IV – «Искусственный интеллект и национальная и международная безопасность». Целями данного исследования является изучение различных вопросов, связанных с киберпространством и искусственным интеллектом: рассматриваются актуальные проблемы, связанные с темой исследования, вопросы трансформации терроризма ввиду массового распространения новых технологий и усилия международного сообщества по противодействию терроризму, обосновывается необходимость правовой регламентации регулирования новых технологий, а также представление практических рекомендаций специалистам.

Война в Ираке, которой посвящена глава 2 «Раскрытие государственных преступлений: критический анализ войны в Ираке и ее глобальных последствий» раздела I, служит, по словам автора, важнейшей отправной точкой данного исследования. В этой главе освещаются хитросплетения международной политики, вопросы ответственности государств и долгосрочные последствия военных вмешательств. Война в Ираке 2003 г. рассматривается как одно из

самых спорных политических решений за последние десятилетия (p. 19). В контексте общей темы данной работы в этой главе через анализ событий конкретного конфликта, его причин, действий мировых лидеров изучается само явление терроризма, обозначаются тенденция роста его масштаба, а также долгосрочные негативные последствия. Оценивая эти события, Р. Монтасари считает уместным дать понятие государственного преступления как действия или бездействия государства, которые нарушают внутреннее и международное законодательство, права человека или систематически наносят ущерб своему собственному населению или населению другого государства. Война в Ираке квалифицируется как агрессивная война, нарушающая Устав ООН.

Интерес представляет также исследование проблем, связанных с гуманитарной интервенцией, ее мотивами, которые в значительной степени обусловлены предполагаемой угрозой терроризма и оружия массового уничтожения в Ираке. Кроме того, обсуждаются общие итоги и долгосрочные последствия этого важного события (p. 19–26).

Следующая глава 3 раздела I – «Оценка эффективности контртеррористических стратегий Великобритании и альтернативных подходов» – содержит анализ положений законодательных актов Великобритании, принятых в целях противодействия терроризму. Великобритания сталкивается с постоянной проблемой противодействия терроризму. Объединенный центр анализа терроризма (JTAC), работающий под эгидой Службы безопасности MI5, присвоил текущему национальному уровню террористической угрозы наименование «существенный», что указывает на вероятную террористическую атаку. Понятие терроризма, как оно определено в Законе Великобритании о терроризме 2000 г., охватывает акты насилия или угрозы насилия, направленные на оказание влияния на правительство или запугивание широкой общественности с целью достижения конкретных политических, религиозных или идеологических целей. Такие действия могут быть связаны с угрозой или причинением серьезного насилия отдельным лицам, причинением существенного имущественного ущерба или выводом из строя электронных систем. Ученые также дают академическое определение терроризма, охарактеризовав его как тактику, которая вселяет страх и использует «принудительное политическое насилие». Это часто рассматривается как рассчитанная и демонстративная практика, включающая «прямые насильственные действия», лишенные «юридических или моральных ограничений» (p. 28).

Цель этой главы – изучение эффективности контртеррористических стратегий Великобритании и анализ альтернативных подходов, основанных на фактических данных, критическая оценка текущей практики борьбы с терроризмом, применяемой Соединенным Королевством, с учетом спорных вопросов, связанных с их эффективностью. В частности, основное внимание уделяется британскому механизму борьбы с терроризмом, известному как Антитеррористическая стратегия Соединенного Королевства, разработанная в 2003 г., последняя редакция которой была принята в 2023 г. Р. Монтасари раскрывает ключевые направления Стратегии – «предотвращать, преследовать, защищать и готовиться» (prevent, pursue, protect и prepare). Особой критике подвергается такое ее направление, как «предотвращать» (prevent) за стигматизацию мусульман, непрозрачность механизмов контроля, недостаток независимости. При этом на основе всестороннего изучения текущей практики в главе обозначены основные проблемы и предложены конкретные рекомендации, направленные на достижение баланса между жесткими мерами безопасности и защитой индивидуальных прав, подчеркивается необходимость увеличения прозрачности деятельности ответственных органов государственной власти, а также достижения большей открытости.

Отдельное внимание в главе 4 «Понимание и оценка роли женщин в борьбе с терроризмом» раздела I автор уделяет рассмотрению феномена женщин в терроризме. Р. Монтасари опровергает устоявшийся миф, заключающийся в понимании положения женщин в терроризме исключительно как жертв, а также утверждает, что традиционный подход, который делит женщин на «жертв» и «преступниц», слишком упрощает реальность. Чтобы глубже понять мотивы совершения ими определенных действий, необходимо отказаться от жестких категорий и рассматривать их участие в терроризме как многофакторное явление. Так, рассматривается устоявшийся стереотип, в соответствии с которым роль женщин в терроризме сводится лишь к пассивному участию: жены или матери террористов, принимающих участие лишь из-за мужей и сыновей, или женщины, неспособной к принятию решений самостоятельно. Далее автор, опираясь на пул современных исследований, описывает трансформированные модели участия женщин в террористических актах: они стали активными участницами и не только исполнительницами, а организаторами, идеологами и, в исключительных случаях, лидерами террористических группировок. В качестве практических примеров рассматривается практический

опыт нескольких террористических организаций. Резюмируя проведенный анализ, автор приходит к выводу о необходимости отказа от представления женщин в терроризме исключительно в качестве жертв, а также о необходимости изучения терроризма в целом, как многосубъектного состава преступления, принимая во внимание изменяющееся положение женщин и занятие ими более активных позиций.

В следующем разделе II – «Пространство кибертерроризма» – содержится две главы: «Современный кибертерроризм: тенденции, методы противодействия и последствия пандемии» (гл. 5) и «Изучение неизбежности угрозы национальной безопасности со стороны кибертерроризма» (гл. 6). В данных главах Р. Монтасари рассматривает феномен кибертерроризма и его потенциальные последствия как новой формы террористической деятельности в условиях быстро меняющегося технологического ландшафта. В рамках исследования автор оценивает «привлекательность» кибертерроризма, а именно: высокую анонимность, низкий порог входа, а также широкое распространение цифровых технологий. Данные аспекты являются серьезным вызовом для органов национальной безопасности. Так, значительный массив преступлений и на сегодняшний день остается нераскрытым ввиду невозможности деанонимизировать лицо, совершившее преступление или способствовавшее его совершению. В рамках исследования автор достигает одной из поставленных задач – оценки реального уровня угрозы кибертерроризма для национальной безопасности. Автор приходит к выводу о том, что наличествует сложная взаимосвязь между технологическим прогрессом, уязвимостями систем и воспринимаемой угрозой кибертерроризма, а также вероятность становления кибертерроризма в качестве наиболее эффективного способа совершения преступлений и насильственных актов.

Раздел III анализируемой монографии «Использование технологий для противодействия кибертерроризму» состоит из четырех глав, 7–10, в которых рассматриваются следующие вопросы: 1) влияние интернет-технологий на радикализацию терроризма и трансформацию его привычных форм. Так, медиапространство и Интернет в целом создали благоприятную среду для распространения, вербовки и организации террористической деятельности; 2) машинное обучение и методы глубокого обучения в борьбе с кибертерроризмом; 3) этические, юридические, технические и операционные проблемы, связанные с применением машинного обучения в борьбе с кибертерроризмом; 4) решение этических,

юридических, технических и оперативных проблем в борьбе с терроризмом с помощью машинного обучения: рекомендации и стратегии (p. 109–220).

Показательно то, что в этом разделе Р. Монтасари раскрывает содержание понятия «новый терроризм», ключевыми характеристиками которого, по его мнению, выступают: высокая степень технологичности, децентрализованность, идеологическая гибкость, массовое психологическое воздействие. «Новый терроризм» для реализации целей деятельности активно использует новые технологии и цифровые платформы, в первую очередь для пропаганды и вербовки, а также социальные сети, блокчейн-технологии, технологии шифрования.

Кроме того, в этом разделе рассматриваются вопросы: 1) баланса интересов: обеспечение безопасности в обществе посредством технологий распознавания лиц и умных камер и соблюдение прав человека, в том числе на частную жизнь; 2) ответственности. С точки зрения современного уровня научно-технологического развития, как уже было отмечено выше, в большинстве случаев нет возможности деанонимизировать лицо, совершившее преступное посягательство. В связи с этим вопрос несения уголовной или административной ответственности в части субъектного состава, остается неразрешенным; 3) юрисдикция. Кибертерроризм представляет наибольшую опасность, в первую очередь за счет «удаленного» формата совершения преступления: объект и субъект преступления зачастую находятся на территории разных государств. Поэтому так актуальна консолидация усилий мирового сообщества и сотрудничество государств, в том числе в вопросе раскрытия и расследования преступлений, а также выдачи информации о совершенном акте. Систематическое рассмотрение технических, операционных, этических и правовых барьеров создает основу для разработки сбалансированных стратегий, обеспечивающих как повышение уровня безопасности, так и защиту фундаментальных прав человека.

Заключительный раздел IV – «Искусственный интеллект и национальная и международная безопасность» – охватывает три главы (гл. 11–13). В главе 11 – «Двойная роль искусственного интеллекта в онлайн-дезинформации: критический анализ» – раскрывается многогранная роль ИИ в сфере онлайн-дезинформации. В частности, рассматривается потенциал методов ИИ для создания высокореалистичной дезинформации и эффективного ее распространения среди широкой аудитории на платформах социальных

сетей. Более того, автор, характеризуя использование ИИ как средства борьбы с таким пагубным явлением, одновременно анализирует связанные с этим проблемы и этические затруднения. Для решения этих сложных проблем Р. Монтасари предлагает комплексный набор рекомендаций, направленных на их устранение и подчеркивает, что этические соображения должны быть неотъемлемой частью разработки и внедрения инструментов искусственного интеллекта, принимая во внимание непреднамеренные негативные последствия, которые могут возникнуть в результате их использования. Рассматривая многогранные проблемы, связанные с дезинформацией, генерируемой искусственным интеллектом, автор вносит значительный вклад в академическую дискуссию, а за счет формулирования практико-ориентированных рекомендаций создает основу для разработки эффективных правительственных стратегий.

В главе 12 – «Решение проблем, связанных с подделкой документов в Соединенном Королевстве: юридические и технические выводы с рекомендациями» – Р. Монтасари подчеркивает, что быстрое развитие технологий глубокого машинного обучения (DML) и ИИ за последнее десятилетие ознаменовало начало новой эры – эры цифровых инноваций. Ярким последствием стало возникновение «дипфейк-эры», рост дезинформационных рисков и угроз, превращающихся в механизм влияния и на обыденную жизнь граждан, и на политическую арену. В контексте Великобритании констатируется отсутствие комплексного законодательства, регулирующего «дипфейк-контент», а также непредвиденность скорых политических изменений в этой сфере.

Интерес у читателя может вызвать углубленный анализ этических и юридических проблем, связанных с подделкой порнографических материалов. Кроме того, в главе рассматриваются далеко идущие последствия подобной дезинформации и та роль, которую технология подделки может сыграть в усилении ее разрушительного и вредоносного воздействия. В конце главы Р. Монтасари призывает объединить усилия ученых и законодателей по реформированию законодательства в условиях внедрения ИИ и повышению цифровой грамотности для эффективного устранения потенциальных угроз, создаваемых новыми технологиями.

В завершающей главе 13 – «Влияние технологии распознавания лиц на фундаментальное право на неприкосновенность частной жизни и соответствующие рекомендации» – дается критический анализ влияния распознавания лиц на такое фундаментальное

право человека, как неприкосновенность частной жизни. С этой целью автор описывает многомерные аспекты технологии распознавания лиц (FRT), оценивает ее достоинства и присущие ей ограничения. Признавая многочисленные преимущества FRT, Р. Монтасари подчеркивает важность сбалансированного подхода, его потенциал для повышения безопасности и обеспечения гарантий соблюдения права на неприкосновенность частной жизни. По итогам этого всестороннего анализа автор предлагает ряд рекомендаций, направленных на защиту фундаментального права на неприкосновенность частной жизни в контексте внедрения системы распознавания лиц. Результаты исследования показывают, что по мере дальнейшего развития сферы применения биометрических технологий на первый план выходят такие требования, как повышение точности, прозрачности и создание надежной правовой базы. Кроме того, полученные результаты подчеркивают необходимость тщательной интеграции технологий и этики, что имеет первостепенное значение для обеспечения конфиденциальности личности.

Таким образом, можно заключить, что монография Р. Монтасари «Киберпространство, кибертерроризм и международная безопасность в эпоху Четвертой промышленной революции» представляет собой важный вклад в изучение киберугроз, кибертерроризма и роли технологий – особенно искусственного интеллекта – в обеспечении национальной и международной безопасности в эпоху Четвертой промышленной революции. Значение данной книги также состоит в ее междисциплинарном подходе, выявлении новых вызовов в сфере кибербезопасности и терроризма, а также практических рекомендациях и примерах противодействия современным угрозам. Благодаря этому данный труд становится настольным руководством для специалистов и государственных деятелей, стремящихся обеспечить безопасность в эпоху цифровой трансформации.

УДК 34.096 DOI: 10.31249/iajpravo/2025.03.15

ГЛОТОВ С.А.[1] РЕЦЕНЗИЯ НА КНИГУ: ГАЛЯШИНА Е.И., АНТОНЯН Е.А., БОГАТЫРЕВ К.М. ЗАЩИТА ОТ ЗЛОУПОТРЕБЛЕНИЯ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ И НЕЙРОТЕХНОЛОГИЯМИ В АСПЕКТЕ МЕДИАБЕЗОПАСНОСТИ: монография / отв. ред. Е.И. Галяшина. – МОСКВА: ПРОСПЕКТ, 2025. – 272 с.

GLOTOV S.A. Book review: Galyashina E.I., Antonyan E.A., Bogatyrev K.M. Protection from abuse of artificial intelligence and neurotechnologies in the aspect of media security: monograph / ed. by E.I. Galyashina. – Moscow: Prospekt, 2025. – 272 p.

Ключевые слова: Интернет; нейронет; искусственный интеллект; нейросети и нейротехнологии; медиакоммуникации и кибербезопасность; специальные правовые режимы; этапы и перспективы развития нейронета; правовые акты ООН и законодательство Российской Федерации в области кибербезопасности.

Keywords: Internet; neuronet; artificial intelligence; neural networks and neurotechnologies; media communications and cybersecurity; special legal regimes; stages and prospects of the neuronet development; UN legal acts and the legislation of the Russian Federation in the field of cybersecurity.

Для цитирования: Глотов С.А. [Рецензия] // Социальные и гуманитарные науки, отечественная и зарубежная литература. Сер. Государство и право. – 2025. – № 3. – С. 192–200. – Рец. на кн.: Галяшина Е.И., Антонян Е.А., Богатырева К.М. Защита от злоупотребления искусственным интеллектом и нейротехнологиями в аспекте медиабезопасности / отв. ред. Е.И. Галяшина. – Москва: Проспект, 2025. – 272 с. – DOI: 10.31249/iajpravo/2025.03.15

[1] *Глотов Сергей Александрович*, ведущий научный сотрудник отдела правоведения ИНИОН РАН, доктор юридических наук, профессор.

Коллективная монография, авторами которой являются ученые Московского государственного юридического университета имени О.Е. Кутафина (МГЮА) – доктора юридических наук, профессора Елена Игоревна Галяшина и Елена Александровна Антонян и кандидат юридических наук Константин Михайлович Богатырев, посвящена актуальной проблематике, которая все больше охватывает умы теоретиков и практиков в различных отраслях знаний, включая представителей юридической науки, – искусственному интеллекту, нейротехнологиям и праву. Это благо или зло в нашей цифровой жизни? – задаются они вопросом и полагают, что ИИ – «джин, выпущенный из бутылки», способный выполнить любое наше желание. Однако результат может быть совсем не тем, что мы хотим получить; кроме того, никто не знает, что этот «джин» наделает, когда станет «свободным» (с. 5).

Авторы приводят пример деятельности лаборатории «Наносемантика» С.И. Ашманова применительно к системе нейросети Chat GPT, так как последняя, обученная только лишь редактировать или дополнять текст, внезапно показала свойства, которые не только не программировались, но даже и не ожидались от нее (например навыки переформатирования текста, решения математических задач и т.д.). Неслучайно в п. 8 Национальной стратегии развития искусственного интеллекта на период до 2030 г., утвержденной Указом Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024), говорится: «…алгоритмы работы нейронных сетей крайне сложны для интерпретации, и, следовательно, результаты их работы могут быть подвергнуты сомнению и отменены человеком. Отсутствие понимания того, как искусственный интеллект достигает результатов, является одной из причин низкого уровня доверия к современным технологиям искусственного интеллекта и может стать препятствием для их развития…».

«Создание универсального (сильного) искусственного интеллекта, способного, подобно человеку, решать различные задачи, мыслить, взаимодействовать и адаптироваться к изменяющимся условиям, является сложной научно-технической проблемой, решение которой находится на пересечении различных сфер научного знания – естественно-научной, технической и социально-гуманитарной. Решение этой проблемы может привести не только к позитивным изменениям в ключевых сферах жизнедеятельности, но и к негативным последствиям, вызванным социальными и технологическими изменениями, которые сопутствуют развитию технологий искусственного интеллекта» (п. 9 Национальной страте-

гии). Свои мнения о решении указанных проблем высказывают и юристы различной специализации. Так, авторами рецензируемой книги проводится углубленный криминологический анализ возможных злоупотреблений ИИ и нейротехнологиями в процессе медиакоммуникации, их причин и инструментов осуществления, а также исследуются направления предупреждения и меры профилактики. Это позволило им определить и раскрыть основные концептуальные подходы к уголовно-правовому регулированию общественных отношений, складывающихся в процессе применения ИИ в рассматриваемой области (с. 9).

Заметим, что на самом деле Е.И. Галяшина, Е. А, Антонян и К.М. Богатырёв несколько выходят за рамки криминологической тематики в сфере ИКТ и искусственного интеллекта и обращаются к более широкому кругу правовых вопросов. Так, глава 1 посвящена вопросам нейротехнологий и ИИ как элементам современного информационного пространства России. Здесь авторы справедливо утверждают, что ИИ и нейротехнологии решают «самые разнообразные задачи – от обороны и разведки до управления экономикой (прогнозирования экономических кризисов, оптимизации самостоятельных систем и принятия решений). Большое внимание уделяется вопросам обеспечения информационной безопасности (противодействию взлому и неправомерному доступу к данным, использованию ИИ в ущерб государственным интересам)» (с. 10, 11–30). Действительно, сегодня ИИ проявляет себя весьма негативно в различных сферах государственной и общественной жизни. К 2025 г., например, количество выявленных дипфейков в мире достигло 8 млн, что в 16 раз больше, чем в начале 2023 г. Так, всплеск числа фальшивых сообщений, сгенерированных с помощью нейросетей на выборах в Европарламент в 2014 г. составил в Болгарии – 3000%, Португалии – 1700%, Бельгии – 800%. В России уже 60% россиян сталкиваются с фейковыми новостями как минимум раз в неделю, а 66% признаются, что хотя бы раз верили дезинформации[1].

В целях исследования основных компонентов и видов ИИ (узкий, общий, сверхинтернет) и нейротехнологий ученые МГЮА используют «Дорожную карту развития “сквозной” цифровой технологии “Нейротехнологии и искусственный интеллект”», утвер-

[1] См.: Бевза Д. Дипфейк шагает по планете // RJ RU. – 2025. – 8 апр. – URL: https://rg.ru/2025/04/08/dipfejk-shagaet-po-planete.html?ysclid=mao13ijcex754 63576 (дата обращения: 29.04.2025).

жденную Минцифры России (с. 13–14). Подчеркивается, что Российская Федерация более оперативно стала реагировать на вызовы времени в области ИИ и нейротехнологий, в том числе путем принятия ряда законодательных актов, среди которых выделяются федеральные законы: от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных"»; от 31.07.2020 № 258-ФЗ (ред. от 08.08.2024, с изм. и доп., вступившими в силу 05.01 2025) «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», положивших начало формированию правового регулирования технологии ИИ в Российской Федерации, ускоренному внедрению результатов развития цифровых технологий в практической жизни (применению ИИ, больших данных, распределительных реестров и т.д.).

На обретение технического лидерства, по мнению авторов, оказывает заметное влияние использование таких технологий, как:

- компьютерное зрение;
- рекомендательные системы и интеллектуальные системы поддержки принятия решений;
- распознавание и синтез речи;
- обработка естественного языка (NLP);
- нейроинтерфейсы и нейростимуляторы и др. (с. 17–18).

Их внедрение осуществляется по разным каналам (с помощью, например, государственных фондов и федеральных органов власти, госзаданий), в том числе с помощью программы «Цифровая экономика Российской Федерации», утвержденной Правительством РФ.

К основным направлениям дальнейшего развития ИИ и нейротехнологий Е.И. Галяшина, Е.А. Антонян, К.М. Богатырёв предлагают отнести их интеграцию в социально-экономическое развитие страны, разработку стандартов их безопасной и эффективной деятельности, а также развитие и совершенствование механизмов правового регулирования.

Частью информационного пространства, и довольно важной, признается медиасреда, существующая в традиционной форме (коротковолновые радиостанции, СМИ, частные периодические издания и т.д.), и в новом, «цифровом» формате (сайты СМИ, ин-

тернет-издания, хостинги, стриминг-сервисы, мессенжеры, форумы, почтовые сервисы, облачные хранилища, поисковые сервисы, тематические сайты и т.п.).

Социальные сети «ВКонтакте», «Одноклассники», системы мгновенного обмена сообщениями – мессенджеры Telegram, WhatsApp, Viber и иные ресурсы играют сегодня важнейшую роль в жизни общества, личности, формируют зачастую повестку их деятельности. «Люди, – как замечают авторы, – не полностью осознают все принципиальные возможные последствия их применения. Взаимодействие через цифровые средства массовой коммуникации (СМК) позволяет не только приятно проводить время, но и нередко столкиваться с пропагандой, недостоверной информацией, фейками, диффамацией, кибермошенниками, незаконным контентом; “сливом” персональных данных, взломом и кражей личных данных, записей (аккаунтов) и т.д. Поэтому вопрос информационной безопасности (и особенно – медиабеопасности в цифровой среде) стоит довольно остро» (с. 23).

Это действительно так и подтверждается множеством фактов, в том числе втягиванием детей в так называемое дроперство – мошеннические схемы, связанные с обналичиванием с помощью подростков денежных средств с карт клиентов. Жертвами этих мошеннических схем стали уже в 2023–2024 гг. 170 тыс. детей, а сумма мошеннических сделок с их помощью превысила 75 млрд рублей. Сегодня у детей на руках 16 млн банковских карт, и их число будет расти ради незначительного обогащения под воздействием ИКТ и других факторов; подростки и далее будут становиться соучастниками преступлений, если со стороны и государства и общества не будут предприниматься более ответственные меры по противодействию данному негативному явлению[1].

На этом сосредоточивается внимание и в Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 г., утвержденной Указом Президента РФ от 17.05.2023 № 358, и других нормативно-правовых актах.

[1] Александрова Н. Карты детям не игрушки // Московский комсомолец. – 2025. – 4 апр. См. также: Рекомендации по нормативному регулированию использования искусственного интеллекта, включая этические стандарты для исследования и разработок. Принята на пятьдесят пятом пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ (Постановление № 55–23 от 14.04. 2023).

Оценивая перспективы развития ИКТ и ИИ, авторы прогнозируют, что на смену децентрализованному компьютер-ориентированному Интернету вещей Web 3.0, деятельность которого напрямую связана с ИИ, приходит Web 4.0 – нейронет, в котором взаимодействуют «человек – человек», «человек – машина», с помощью новых нейрокомпьютерных интерфейсов, в дополнение традиционным методам, а сами компьютеры станут нейромаршрутными (похожими на мозг) на основе гибридных цифроаналоговых архитектур (с. 27). Нейронет сегодня означает уже не только нейросеть, но и коммуникационную сферу следующего поколения, основанную на нейроинтерфейсах и новых протоколах опосредованного или взаимодействия между людьми, коллективами искусственными автономными системами работы с данными и объектами реального мира.

Приблизительные временные рамки этапов развития нейронета, с точки зрения Е.И. Галяшиной, Е.А. Антонян и К.М. Богатырёва, следующие.

Первый этап (2015–2020) – возникновение первых нейрочатов, социальных сетей на основе интерфейсов «мезо-компьютер» для людей с нарушениями речи и опорно-двигательного аппарата. Нейронет проявляет себя, прежде всего, в таких областях деятельности, как медицина, безопасность и развлечения.

Второй этап (2020–2030) – появление двух прототипов нейронета, его прологов – интернет-биометрических вещей (устройств, считывающих физиономические параметры человека) и Web2.0 t практик, использующих биометрическую инфраструктуру. Это также создание системы взаимосвязанных порталов открытых сообществ не только в сфере медицины и развлечений, но и в спорте, образовании, услугах, продвижение ИИ и ИКТ на территории, значительное увеличение мощности интерфейсов.

Третий этап (2030–2040) – дальнейшее развитие нейронета как в отдельных отраслях, так и по более широкому полю деятельности, создание коммуникационной среды, основанной на протоколах прямого взаимодействия. Первые системы типа протокола передачи мыслей HTTP-2 – создание нейроколлективов. Возможно появление «экзокротека» – «внешнего мозга», «искусственной» части психики, поддерживаемых машинами и синхронизируемых с естественной психикой, создание внешней памяти, проведение сложных вычислений и т.д. и даже создание искусственного опыта.

Четвёртый этап (после 2040 г.) – нейронет, выйдя за пределы очагов его использования, захватывает область коммуника-

ций целиком и превращает в массовый инструмент и цивилизационную инфраструктуру (с. 28–30).

Следует отметить, что пока это только один из прогнозов развития ИИ, Интернета, нейростетей, их трансформации. По мнению Е.И. Галяшиной, Е.А. Антонян, К.М. Богатырёва, активный процесс их быстрого развития вызван экономическими, социальными, политическими и иными факторами. Сегодня достижения ИКТ и нейросети можно наблюдать в медицине, технике, образовании, культуре.

Например, Венский университет прикладного искусства зачислил в качестве студента нейросеть. Киберобучающийся по имени Флинн будет проходить обучение по программам цифрового искусства, он уже прошел все необходимые испытания собеседования, тест на профпригодность и даже представил портфолио, которое экзаменаторы назвали впечатляющим. Заведующая кафедрой Лиз Хаас заявила, что нет никаких письменных требований, согласно которым студентом может быть только человек. «Это очевидно, потому что ранее никто об этом не задумывался», – заявила она. Разработчики Флинна утверждают, что полученные данной нейросетью в процессе обучения вместе со студентами и преподавателями знания помогут отточить его внутренние алгоритмы. Для занятий Флинну потребуется ноутбук или планшет, через который будет осуществляться передача информации и ее обработка. Эксперимент с «киберстудентом» имеет своей целью доказать, что ИИ является новым типом художественного средства, не подменяющим человека, а помогающим ему в творческой работе[1].

Значительное внимание в книге, в главе 3, авторы уделяют теме регулирования нейротехнологий и ИИ в контексте обеспечения национальной безопасности Российской Федерации. Для этого они анализируют правовые акты ООН и Совета Европы в области ИИ, ИКТ, в том числе рамочные соглашения об этике ИИ – Рекомендации об этических аспектах искусственного интеллекта (ЮНЕСКО, 2021); Рамочную конвенцию Совета Европы об искусственном интеллекте, правам человека, демократии и верховенстве права (2024); Рекомендацию Парламентской ассамблеи Совета Европы (ПАСЕ) № 2184, Резолюцию 2344 «Интернет – мозг – компьютер: новые права и новые угрозы основам свободы» (2020, ПАСЕ).

[1] Подробнее см.: Кожевников А. Алгоритм с зачеткой // Российская газета. – 2025. – 8 апр.

Далее приводится краткая характеристика нормативно-правовых актов Российской Федерации, регулирующих ИИ и нейротехнологии, а также Кодекса этики в сфере искусственного интеллекта (2021), подготовленного совместно Альянсом «Россия в сфере искусственного интеллекта», Аналитическим центром при Правительстве РФ и Минкультом России. Документ подписали на Первом международном форуме «Этика искусственного интеллекта: начало доверия» первые 20 компаний – лидеров в области ИИ, в том числе Яндекс, Сбер, МТС, Ростелеком, Высшая школа экономики, Росатом и Сколково[1]. Важность развития института этики ИИ и необходимость увеличения числа подписантов Кодекса отражены в поручении Президента РФ по итогам конференции «Путешествие в мир искусственного интеллекта» от 16.12.2021 № Пр-2371. В соответствии с п. 1г Правительству РФ поручено принять меры по увеличению числа российских и иностранных организаций, присоединившихся к Кодексу этики в сфере искусственного интеллекта. В настоящее время к Кодексу присоединились более 180 подписантов[2].

Е.И. Галяшина, Е.А. Антонян, К.М. Богатырёв предполагают, что с развитием законодательства положения, регулирующие функционирование ИИ и нейротехнологий, будут включаться в такие нормативные правоые акты, как Конституция РФ (например, в целях закрепления на конституционном уровне новой категории прав – нейроправ), Уголовный кодекс РФ (введение новых составов преступлений), Гражданский кодекс РФ (например определение прав и результатов ИИ или их субъектности), Федеральный закон «Об информации, информационных технологиях и о защите информации» и т.д. (с. 48)

Новые возможности нейротехнологий рассматриваются в главе 4. Речь идет о нейроинтерфейсах, нейропрогнозировании, нейростимуляции; анализе возможных злоупотреблений нейротехнологиями и противодействии этому.

[1] Кодекс для ИИ. В России определились, что этично в сфере искусственного интеллекта. – 2021. – URL: https://secretmag.ru/cifrovaya-ekonomika/kodeks-dlya-ii-v-rossii-opredelilis-chto-etichno-v-sfere-iskusstvennogo-intellekta.htm (дата обращения: 12.05.2025).

[2] Кодекс этики в сфере искусственного интеллекта. – URL: https://economy.avo.ru/main/-/asset_publisher/cwir6q331Q6n/content/kodeks-etiki-v-sfere-iskusstvennogo-intellekta (дата обращения: 12.05.2025).

Указанная выше проблематика заслуживает отдельного детального анализа, поскольку создание и применение новых технологий, особенно в таких чувствительных сферах как ИИ и нейросети, нейронета порождают целый ряд правовых вопросов, проблем.

В заключение работы авторы констатируют, что разработка и поддержание отечественных систем ИИ и нейроинтерфейсов является обязательным условием технологического суверенитета страны, вопросом национальной безопасности. Ученым важно продолжать исследовать проблематику когнитивного суверенитета отдельных пользователей, соблюдения прав и свобод человека и гражданина, нахождения компромисса и обеспечения интересов отдельных социальных групп и общества в целом. Именно медиасредства становятся не просто местом столкновения множества разнонаправленных интересов, но и площадкой для осмысления и оценки (как позитивной, так и негативной) описанных технологий, результатов их применения (с. 115–116).

И здесь важную роль играет право, гибкое этичное регулирование, различные экспериментальные режимы, так называемое «мягкое право», положения которого закрепляются законом.

УДК 343, 34.096 DOI: 10.31249/iajpravo/2025.03.16

АЛФЕРОВ О.Л.[1] РЕЦЕНЗИЯ НА КНИГУ: АНИЩЕНКО В.Н., ВЫБОРНЫЙ А.Н., ХАБИБУЛИН А.Г. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПРОТИВОДЕЙСТВИИ КРИМИНАЛЬНЫМ УГРОЗАМ ФИНАНСОВОЙ БЕЗОПАСНОСТИ РОССИИ (ТЕОРИЯ, МЕТОДОЛОГИЯ И ПРАКТИКА) / Московский государственный университет имени М.В. Ломоносова, Высшая школа государственного аудита. – Москва, 2024. – 376 с.
ALFEROV O.L. Book review: Anishchenko V.N., Vyborny A.N., A.G. Khabibulin. Artificial Intelligence in Countering Criminal Threats to Russia's Financial Security (Theory, Methodology, Practice) / Lomonosov Moscow State University, Higher School of Public Audit. – Moscow, 2024. – 376 p.

Ключевые слова: искусственный интеллект; криминальные угрозы; финансовая безопасность; органы финансового расследования; программные инструменты и технологии.

Keywords: artificial intelligence; criminal threats; financial security; financial investigation agencies; software tools and technologies.

Для цитирования: Алферов О.Л. [Рецензия] // Социальные и гуманитарные науки, отечественная и зарубежная литература. Сер. Государство и право. – 2025. – № 3. – С. 201–208. – Рец. на кн.: Анищенко В.Н., Выборный А.Н., Хабибулин А.Г. Искусственный интеллект в противодействии криминальным угрозам финансовой безопасности России (теория, методология, практика) / Московский государственный университет имени М.В. Ломоносова, Высшая школа государственного аудита. – Москва, 2024. – 376 с. – DOI: 10.31249/iajpravo/2025.03.16

Данный монографический труд написан тремя представителями профессорско-преподавательского состава кафедры эконо-

[1] *Алферов Олег Леонидович*, ведущий редактор отдела правоведения ИНИОН РАН.

мических и финансовых расследований Высшей школы государственного аудита Московского государственного университета имени М.В. Ломоносова – В.Н. Анищенко, доктором технических наук, профессором, А.Г. Хабибулиным, доктором юридических наук, профессором и А.Н. Выборным, кандидатом экономических наук, член-корреспондентом РАЕН. Посвящен он проблемам создания искусственных интеллектуальных систем противодействия криминальным угрозам финансовой безопасности России, реализуемых в правоохранительных органах, а также комплексному изучению теоретико-методических основ исследования данных проблем, прежде всего обеспечения финансовой безопасности и защиты финансового суверенитета страны. Исходной базой при подготовке монографии, и это следует подчеркнуть, стали: 1) научные труды российских и зарубежных ученых, международных и российских институтов и организаций по проблемам противодействия преступности и коррупции в сфере финансов и обеспечения финансовой безопасности; 2) политические и стратегические официальные документы РФ, соответствующие нормативные правовые акты, судебные решения, статистические данные, проанализированные авторами в контексте рассматриваемой темы. Интерес представляют также практические рекомендации, методологические приемы и подходы, которые могут быть использованы при разработке законодательных и иных нормативных правовых актов федерального значения, в целях создания условий для повышения уровня финансовой безопасности России в современных условиях. Важно отметить, что при исследовании многих вопросов финансовой безопасности России в книге выявляются и описываются потенциальные возможности использования в органах финансового расследования искусственных интеллектуальных информационно-аналитических систем. Такой подход обусловлен, по словам авторов, прежде всего высокой общественной опасностью, латентностью и масштабностью преступности экономической направленности в России, большой территориальной спецификой страны, значительным количеством хозяйствующих субъектов, постоянным усложнением внешнеэкономических связей и отношений (с. 355). Такие системы характеризуются как основное средство информационно-аналитического обеспечения оперативно-служебной деятельности органов финансового расследования. Их применение рассматривается как сложная мультиотраслевая задача, решение которой предусматривает реализацию комплекса взаимосвязанных мер организационного, правового, образовательного, научно-тех-

нического, кадрового, материального и финансового характера, направленных на обеспечение и повышение эффективности финансовых расследований (там же).

В целях комплексного раскрытия роли и места систем искусственного интеллекта (далее – СИИ) в противодействии криминальным угрозам финансовой безопасности России и строится структура работы, объемной по своему содержанию и количеству глав – 13, в которых последовательно исследуются: ключевые экономико-правовые аспекты противодействия угрозам финансовой безопасности России (гл. I); роль и место СИИ в противодействии этим угрозам (гл. II); теоретические основы, цели, задачи, функции и основные принципы построения такой системы искусственного интеллекта (СИИ) (гл. III); теоретико-методологические аспекты ее функционирования (гл. IV) и организационно-техническая структура ИИС органов финансовых расследований (далее – ОФР) (гл. V); общесистемные программно-аппаратные платформы информационно-аналитических комплексов ИИС ОФР (гл. VI) и их информационные ресурсы (гл. VII); прикладные средства информационно-аналитического обеспечения ИИС ОФР (гл. VIII); прикладные программные инструменты и технологии ИИС ОФР (гл. IX); базы данных и системы управления ими в ИИС ОФР (гл. X); обеспечение функционирования ИИС ФР (гл. XI) и вопросы эффективности работы ИИС ФР (гл. XII); анализ эволюции и направлений развития ИИС ФР) (гл. XIII).

Так как ключевым понятием в данной монографии является термин «искусственный интеллект», авторы делают ряд принципиальных пояснений относительно его лингвистического и смыслового содержания. По их мнению, сложилось образное искаженное представление о функционировании электронных машин в современной литературе, получившее обозначение «искусственный интеллект», которое, считают они, более корректно именовать «искусственная интеллектуальная система» (с. 30–31). В отличие от выражения «искусственный интеллект», термин «искусственная интеллектуальная система» представляется более точным, поскольку прилагательное «интеллектуальная» отражает факт отношения данной системы к человеческому интеллекту, в том числе как объект, созданный благодаря интеллекту человека, и как формализованное модельное отражение отдельных функциональных свойств интеллектуальной деятельности человека, по своей природе строго неформализуемых (с. 31).

Искусственные интеллектуальные системы – *системы*:

– созданные человеком или являющиеся результатом интеллектуальной и иной деятельности человека;

– имеющие отношение к интеллекту человека, выраженные как в использовании результатов интеллектуальной деятельности человека, так и в обеспечении реализации в автоматическом режиме некоторых формализуемых утилитарных элементов интеллектуальной деятельности специалистов;

– реализующие некоторое конечное множество алгоритмизируемых, рутинных функций человеческого интеллекта;

– образованные некоторым комплексом, как правило электронных средств, связанных между собой непосредственно или посредством телекоммуникационных систем, в том числе электронных, в основе функционирования которых лежит реализация взаимосвязанного множества различного рода алгоритмов, соответствующих функциональной принадлежности системы (с. 68–69).

В целях раскрытия темы монографии авторы, опираясь на Стратегию национальной безопасности РФ, утвержденную Указом Президента РФ от 02.07.2021 г. № 400, и законодательство РФ, концентрируют свое внимание на основных направлениях развития науки и технологий, характеристике государственной инновационной политики РФ, погружаются в историю инновационной активности промышленных предприятий разных форм собственности, а также в историю и современную практику развития правовых отношений, опосредующих инновационную деятельность в стране (с. 32–47).

Еще одним важным ключевым термином в данном исследовании является выражение «финансовая безопасность», которая рассматривается как основа гарантии финансовой независимости и суверенитета страны, условие стабильности и эффективности жизнедеятельности общества и первостепенный государственный приоритет в развитии российской экономики. Под финансовой безопасностью России, по мнению авторов, целесообразно понимать феномен отсутствия внешних и внутренних угроз безопасности Российской Федерации, имеющих финансовую природу, или источником которых является внутренняя и внешняя сферы финансов, способность причинять существенный или недопустимый вред России (с. 57). Подчеркивается, что неэффективное государственно-правовое воздействие на указанные финансовые сферы – реальные, виртуальные и криминальные финансы – может привести к утрате финансового суверенитета страны (с. 65).

Следует отметить, что, начиная с главы II, В.Н. Анищенко, А.Н. Выборный и А.Г. Хабибулин переходят к исследованию СИИ как искусственных интеллектуальных систем (ИИС), противостоящих криминальным угрозам финансовой безопасности России. Масштабность использования новых средств производства и телекоммуникации проявляются: 1) в повсеместном оснащении всех предприятий реального и финансового секторов экономики высокопроизводительными комплексами средств автоматизации, новейшими электронными средствами информатизации и оптико-электронными средствами телекоммуникации; 2) в реализации на вышеуказанной информационно-технологической основе методов обработки больших объемов разнородных данных; 3) в неограниченных возможностях использования указанных средств для совершения преступлений, включая экономические и финансовые (с. 67). Очевидно, что без оснащения правоохранительных органов соответствующими средствами, организационно и технически интегрированными в ИИС, не будет должного контроля над такой новой средой.

В этой части книги авторы обоснованно обращают внимание на то, что в настоящее время в общественной коммуникации и даже в официальных государственных документах получили широкое распространение замена и подмена понятий из сферы информатики и автоматизации человеческой деятельности с использованием ИИС на образные выражения, которые не всегда полно и корректно отображают сущность и содержание описываемых феноменов. К числу таких образных выражений относятся слова: «цифровизация», «цифровая экономика», «цифровые деньги» и т.п. (с. 70–73).

Интерес представляют рассуждения авторов о направлениях использования ИИС в целях противодействия криминальным угрозам финансовой безопасности России. Среди таких направлений выделяются: мониторинг экономического, прежде всего финансового, состояния предприятия и криминологический анализ оперативной обстановки на соответствующей территории; традиционный экономико-правовой анализ финансово-хозяйственной деятельности как самих предприятий, так и их контрагентов; криминологический анализ оперативной обстановки в регионах и на предприятиях, выявление условий и предпосылок для совершения экономических и финансовых преступлений в целях нейтрализации различных источников угроз финансовой безопасности России (с. 79).

Для получения полного и четкого представления о роли, структуре и задачах ИИС в противодействии криминальным угрозам финансовой безопасности России в деятельности правоохранительных органов авторы прежде всего уточняют содержание основных понятий, как то: «финансы», «криминальные финансы», «финансовые расследования», «органы финансового расследования» и др. Так, «органы финансовых расследований» как категория, синонимичная понятию «органы расследования финансовых преступлений» – это органы государственной власти, уполномоченные, согласно законодательству, осуществлять финансовые расследования (с. 93).

Далее приводятся и обосновываются основные понятия, имеющие отношение к ИИС как средству автоматизации правоохранительной деятельности по противодействию криминальным угрозам безопасности России. Исходными для множества терминов являются синонимичные понятия «информационная система» (ИС) и «автоматизированная система» (АС), описывающие класс систем, к которому относятся ИИС и ИИ.

К основным компонентам ИС авторы относят: общесистемную программно-аппаратную платформу; информационные ресурсы; прикладные программные средства (технологии) формирования, обработки и распределения информационных ресурсов; конечных пользователей и обслуживающий персонал и др. (с. 94). Важно то, что эти компоненты ИС не только перечисляются, но каждому из них посвящена отдельная глава монографии. Для специалистов такой подход даст новые знания использования инструментов ИИС для противодействия криминальным угрозам финансовой безопасности. Основная цель функционирования ИИС финансового расследования (ФР), исходя из ее назначения, – создание условий эффективного осуществления оперативно-служебной деятельности органов ФР (ОФР), в том числе путем автоматизации процессов сбора, обработки и распределения тематических информационных ресурсов в соответствии с профилем деятельности ОФР, оснащенных этими системами (с. 109).

Любопытен подход авторов к изучению механизма противодействия криминально-коррупционным отношениям в финансовой сфере, в том числе в системе ОФР и органов финансовой безопасности. Анализируя негативные социальные явления финансово-экономической направленности, т.е. криминальные угрозы, они делают следующие обобщения: 1) масштабная автоматизация всех сфер жизнедеятельности общества на основе многофункциональ-

ных ИИС многократно усиливает способности людей и предоставляет новые возможности в реализации тех или иных видов деятельности; 2) преступность криминально-коррупционной финансово-экономической направленности имеет возможности широкого использования достижений научно-технического прогресса с явными конкурентными преимуществами перед законопослушными гражданами и органами государственного управления, обусловленными игнорированием всяких правовых ограничений, норм и запретов; 3) эффективная организация, обеспечение и реализация противодействия криминально-коррупционным угрозам финансовой безопасности России невозможны без создания многофункциональных ИИС (с. 176).

Основными составляющими обеспечения функционирования ИИС ФР учеными признаются:

– нормативное правовое обеспечение работы ИИС ФР;

– обеспечение функционирования деятельности персонала и сотрудников органов финансовых расследований – пользователей ИИС ФР;

– обеспечение развития ИИС ФР;

– кадровое обеспечение ИИС ФР.

К числу наиболее важных мероприятий по нормативному правовому обеспечению функционирования ИИС ФР, которые имеют внутриведомственное значение, авторы относят: унификацию и типизацию документов первичного учета, возникающих в процессе оперативно-служебной деятельности ОФР; взаимную увязку должностных инструкций по линиям оперативно-розыскной деятельности, оперативному документированию с технологией учетно-регистрационной работы и формирования интегрированных баз данных ИИС ФР; организационную оптимизацию системы статистических показателей о результатах работы подразделений ОФР; регламентирование порядка доступа к информационным ресурсам ИИС ФР; формирование нормативно-распорядительных документов, определяющих порядок эксплуатации и обслуживания оборудования, программного обеспечения и средств телекоммуникаций (с. 288–289).

При этом достаточно сложными с правовой точки зрения они признают регулирование отношений по вопросам: использования и управления сетями, базами данных; организационно-технического обеспечения развития и устойчивого функционирования единого информационного пространства; подготовки персонала; технического обслуживания и др. Важное значение здесь имеют

правовое регулирование комплекса отношений, связанных с информацией, ее производством, движением, применением, в том числе вопросы соблюдения авторского права и права собственности на документированную информацию и информационные ресурсы; ответственности субъектов информационного пространства за нарушения, допущенные при формировании информационных ресурсов и их использовании; обеспечения информационной безопасности (с. 290–291).

Следует обратить внимание на то, что, формулируя задачи создания и использования в оперативно-служебной деятельности ОФР интегрированных информационных ресурсов ИИС ФР, равно как и их регламентное предоставление внешним организациям, авторы указывают, что это потребует реализации комплекса дополнительных мероприятий, предусматривающих: создание в перспективе системы обязательной сертификации и лицензирования единого информационного пространства для обеспечения контроля полноты, достоверности, надежности соответствующих технических и программных устройств; определения порядка и правил формирования и использования информационных ресурсов, обязательных для всех субъектов информационных отношений в рамках единого информационного пространства; определение порядка и правил разрешения конфликтных ситуаций, возникающих в процессе формирования и использования информационных ресурсов (с. 292).

Данная монография ценна тем, что она восполняет проблемы информированности сотрудников ОФР по одному из сложнейших вопросов автоматизации информационно-аналитической работы правоохранительных органов в сфере экономики и финансов. Успехом авторов книги – В.Н Анищенко, А.Н. Выборного и А.Г. Хабибулина – следует признать разностороннее исследование вопросов информационного обеспечения финансовых расследований и программно-технических основ обработки информации, включая определенные организационные, технико-технологические, научные, правовые и другие аспекты. Важно то, что авторы провели систематизацию понятийного аппарата и основных проблемных вопросов применения АИАС в деятельности органов финансовых расследований, представили свой взгляд в будущее развития перспективных искусственных интеллектуальных систем.

УДК 349 DOI: 10.31249/iajpravo/2025.03.17

КРЫСАНОВА Н.В.[1] РЕЦЕНЗИЯ НА КНИГУ: АВТОНОМНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА И ГРАЖДАНСКАЯ ОТВЕТСТВЕННОСТЬ В ГЛОБАЛЬНОЙ ПЕРСПЕКТИВЕ: ИССЛЕДОВАНИЕ ЗАКОНОДАТЕЛЬСТВА ОБ ОТВЕТСТВЕННОСТИ ПО ВСЕМУ МИРУ В СООТВЕТСТВИИ СО СТАНДАРТОМ SAE J3016 ДЛЯ АВТОМАТИЗАЦИИ ВОЖДЕНИЯ / под ред. Х. Штеге, И.А. Каджано, М.К. Гаэты, Б. фон Бодунгена.

KRYSANOVA N.V. Book Review: Autonomous Vehicles and Civil Liability in a Global Perspective: An Examination of Liability Laws around the World in Accordance with the SAE J3016 Driving Automation Standard / ed. H. Steege, I.A. Caggiano, M.C. Gaeta, B. von Bodungen. – 2024. – Cham: Springer, 2024. – 548.

Ключевые слова: искусственный интеллект; деликтная ответственность; беспилотные транспортные средства; страхование гражданской ответственности; ответственность производителя.

Keywords: artificial intelligence; tort liability; unmanned vehicles; civil liability insurance; product liability.

Для цитирования: Крысанова Н.А. [Рецензия] // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. Государство и право. – 2025. – № 3. – С. 209–217. – Рец. на кн.: Autonomous Vehicles and Civil Liability in a Global Perspective: An Examination of Liability Laws around the World in Accordance with the SAE J3016 Driving Automation Standard / ed. H. Steege, I.A. Caggiano, M.C. Gaeta, B. von Bodungen. – 2024. – 548 p. – Автономные транспортные средства и гражданская ответственность в глобальной перспективе: исследование законодательства об ответственности по всему миру в соответствии со стандартом SAE J3016 для автоматизации вождения / под ред. Х. Штеге,

[1] *Крысанова Нина Владимировна*, старший научный сотрудник отдела правоведения ИНИОН РАН, кандидат юридических наук.

И.А. Каджано, М.К. Гаэты, Б. фон Бодунгена. – 2024. – 548 с. – DOI: 10.31249/iajpravo/2025.03.17

Данное исследование представлено в серии книг издательства Шпрингер «Наука о данных, машинный интеллект и право», и создано авторами двух исследовательских институтов – Исследовательского центра европейского частного права Неаполитанского университета Суор Орсола Бенинкаса (University Suor Orsola Benincasa, Naples, Italy) и Междисциплинарного института автоматизированных систем (Ганновер, Германия (Interdisziplinäres Institut für Automatisierte Systeme e.V. – RifaS–Hannover, Germany)), изучающих проблемы правового регулирования автоматизации в междисциплинарном контексте.

В монографии рассматриваются сложные вопросы законодательного регулирования использования автономных транспортных средств и гражданско-правовой ответственности в случаях причинения вреда, в том числе при дорожно-транспортных происшествиях (ДТП). Авторы пытаются найти ответ на главный вопрос: кто является виновным в аварии с участием автоматизированного или автономного транспортного средства?

Гражданско-правовая ответственность – один из важнейших инструментов в регулировании современной автоматизации, распространения инноваций в целях защиты жизни человека и установления общих правил для всех участников правовых отношений в данной сфере.

Важно то, что в монографии дан анализ основных моделей гражданской ответственности за ущерб, причиненный автоматизированным и автономным вождением, на примерах разных стран, и не только для того чтобы охватить наиболее актуальные рынки автомобильной промышленности, но и с учетом того, что такие транспортные средства, по всей вероятности, будут пересекать границы государств, и возможны ДТП на территории другой «юрисдикции». В связи с этим рассматриваются проблемы распределения рисков между сторонами, а также действие страхового законодательства в случае ДТП с «автономным» транспортом (p. VI). С этой точки зрения монография представляет большой интерес для отечественного читателя, особенно для специалистов, как работающих в сфере автоматизации вождения и внедрения автоматизированных и автоматических транспортных средств в России, так и юристов различного профиля.

Содержание книги разделено на шесть частей, различных по объему, поскольку в отдельных регионах еще незначительно развито использование ИИ при вождении автономных транспортных средств. В части I исследуется режим гражданско-правовой ответственности в Южной Африке. В части II – особенности гражданско-правовой ответственности в случае ДТП в Соединенных Штатах и Колумбии. В часть III – правила автономного вождения в Китае, Японии, Сингапуре и Корее. Действующее законодательство в рассматриваемой области и проекты нормативных правовых актов по его дополнению, точки зрения ученых на развитие этого законодательства в Австралии исследуются в части IV книги. С нашей точки зрения, для читателей будет интересен материал, представленный в части V, посвященной опыту правового регулирования и гражданско-правовой ответственности в сфере автоматизированных автономных транспортных средств в таких странах, как Бельгия, Германия, Франция, Испания, Италия, Нидерланды, Австрия, Румыния и Швеция. В заключительной IV части раскрываются особенности юридической ответственности в сфере автоматизированных транспортных средств в Великобритании.

Положительным моментом можно считать рассмотрение технических характеристик транспортных средств с использованием ИИ. В соответствии с классификацией в SAE J3016 выделяются пять уровней автоматизированного вождения. По мере роста автоматизированности водитель-человек поэтапно заменяется транспортным средством. В частности, согласно стандарту SAE J 3016, автоматизированные системы управления автотранспортными средствами выполняют часть или все задачи в области вождения на постоянной основе. Эта система управления включают трех основных участников: человека, систему автоматизации вождения, а также другие системы и компоненты транспортного средства.

Стандарт SAE J 3016 содержит различные *уровни автоматизации вождения*: 0 (отсутствие автоматизации вождения); 1 (помощь водителю); 2 (частичная автоматизация вождения); 3 (условная автоматизация вождения); 4 (высокая автоматизация вождения); 5 (полная автоматизация вождения).

Уровень 0 – это, по сути, обычные автомобили, не содержащие никаких систем автоматизации. При этом некоторые транспортные системы, охватываемые уровнями 1 или 2, уже представлены на рынке продолжительное время. Это касается авто с системами ABS, круиз-контроля и т.п. В конечном итоге, как считают авторы книги, водитель-человек будет полностью устранен

от управления, и в будущем автомобиль сможет перевозить пассажиров автономно, без сопровождения водителя. Именно из-за растущей степени автоматизации возникают многочисленные вопросы юридической ответственности. Основным правовым вопросом, связанным с эксплуатацией автономных транспортных средств с ИИ, является вопрос юридической ответственности за действия, совершаемые с участием автономного транспортного средства. Данный вопрос, с точки зрения авторов, требует как минимум гражданско-правового регулирования (p. VI).

Для отечественного читателя, полагаем, особенно интересно будет ознакомиться с полезным опытом США, КНР и ФРГ по регулированию отношений, возникающих в области управления автономным транспортом, и вопросам гражданско-правовой ответственности.

Соединенные Штаты Америки

По состоянию на 1 июня 2020 г. в 35 штатах и округе Колумбия были приняты законы, прямо касающиеся автономных транспортных средств. Это нормативное правовое регулирование в основном касается условий эксплуатации автономных транспортных средств, включая правила, регулирующие работу операторов и технические характеристики автоматизированных систем вождения. Лишь в нескольких штатах созданы независимые механизмы определения ответственности в случае аварии. Как отмечают авторы, федеральное законодательство, регулирующее автономные транспортные средства, пока не вступило в силу в полном объеме, однако развитие событий в сфере автоматизированного и автономного транспорта таково, что есть все основания считать, что федеральные нормативные правовые акты будут в скором времени приняты, и это в конечном счете определит базовые стандарты безопасности, предъявляемые к автономным транспортным средствам, и др. (p. 9).

В США федеральный закон имеет верховенство над законодательством штата, и поэтому с принятием федерального законодательства в сфере автономного вождения одновременно будут устранены любые противоречивые положения из законодательства штатов, а кроме того, автономное транспортное средство, соответствующее требованиям и стандартам, установленным федеральным законодательством, будет освобождено от деликтной ответственности (tort liability). Если же транспортное средство не будет

соответствовать применимым федеральным стандартам, и в результате произойдет авария, – сторона, которая будет признана виновной, будет нести гражданско-правовую ответственность за причиненный вред (p. 95).

На сегодняшний день, в отсутствие федерального законодательства, ответственность за аварию автономного транспортного средства определяется деликтным правом штатов. В подавляющем большинстве штатов производители несут строгую юридическую ответственность за любые дефекты продукции, которые приводят к поломке или аварии транспортных средств, в том числе изготовленных и применяющих технологии ИИ, автоматизированных или автономных.

В целом, в США деликтное право является наиболее распространенным источником гражданской ответственности за ДТП. Большинство деликтных дел, рассматриваемых в судах штатов, связанных с ДТП, подразумевает неосторожность водителя (driver's negligence): согласно данным, собранным в судах 17 штатов, количество дел по деликтам, например, в 2015 г. варьировалось от 32% от общего числа дел о гражданских правонарушениях (Миссури) до 75% (Техас), причем дела по деликтам в связи с транспортными средствами превысило 50% общего числа слушавшихся деликтных дел в большинстве штатов США. Деликты, возникающие в результате автомобильных аварий, обычно связаны с причинением вреда здоровью, материального ущерба или смерти по неосторожности в результате небрежного управления транспортным средством. С устранением фактора водителя-человека, по мере автоматизации транспорта, а также в ситуациях с автономными транспортными средствами, будут устранены основания для исков о возмещении вреда и деликтной ответственности водителей. Вместо этого юридическую ответственность за ходовые качества и «вождение» автономного транспортного средства будет нести производитель, потенциально подпадая под деликтную ответственность за аварию в соответствии с правилами строгой ответственности за качество продукции (p. 92).

Китайская Народная Республика

С 2009 г. Китай является крупнейшим автомобильным рынком в мире. В 2021 г. на производство автомобилей в Китае приходилась почти треть мирового производства, что превысило аналогичный показатель в США, Японии и ФРГ, вместе взятых.

Китайское правительство считает, что новые электромобили необходимы для превращения Китая из автомобильного гиганта в автомобильную державу. В Плане развития индустрии новых энергетических транспортных средств (2021–2035) (New Energy Vehicle Industry Development Plan (2021–2035), утвержденном Государственным советом 20 октября 2020 г., в отношении самоуправляемых автомобилей (self-driving cars) намечено использовать автомобили с высокой степенью автономности (уровня 4 классификаций SAE) в коммерческом применении в ограниченных районах и по конкретным программам – к 2025 г., и обеспечить их масштабное использование – к 2035 г. Считается, что достижение этой цели должно способствовать сокращению выбросов и повышению социальной эффективности. Кроме того, согласно этому Плану развития, Китай также намерен усовершенствовать правовую базу в области дорожного движения, ответственности за ДТП и использования данных, чтобы соответствовать требованиям в связи с разработкой «интеллектуально подключенных транспортных средств» (intelligent connected vehicles) (p. 125–126).

В вопросах правового развития в сфере автоматизированного вождения и автономного транспорта План развития предусматривает решение вопросов, касающихся юридического статуса автоматизированных или автономных транспортных средств (status of legal subjects of the AVs), распределения юридической ответственности, кибербезопасности и управления данными, разработки законов, регулирующих проведение тестирования, авторизацию, использование и надзор за автоматизированными и автономными транспортными средствами, а также совершенствования действующих законов, включая Закон о безопасности дорожного движения КНР (Law on Road Traffic Safety).

Стимулируемое быстрым ростом промышленности, китайское правительство опубликовало несколько стратегий / программ для решения предстоящих проблем. Эти стратегии и программы подразделяются на центральные и местные (central and local), и в совокупности с действующим законодательством, в том числе Законом о безопасности дорожного движения (Law of the People's Republic of China on Road Traffic Safety [2003]) и Законом о качестве продукции (Product Quality Law of the People's Republic of China (amendment) [2000]), составляют правовую базу для решения вопроса о распределении ответственности, связанной с автономным вождением, автоматизированными и автономными транспортными средствами в Китае (p. 127).

Федеративная Республика Германия

В 2017 г. в Федеральный закон о дорожном движении (Federal Road Traffic Act) Германии были добавлены положения, касающиеся условной автоматизации транспортных средств. В 2021 г. был осуществлен еще один качественный скачок в законодательстве в отношении регулирования юридического статуса высокоавтоматизированных автомобилей. Намерение правительства Германии в тот период, как отмечают авторы, состояло в том, чтобы продемонстрировать лидерство страны в разработке самоуправляемых транспортных средств и окружающей экосистемы (p. 281–284).

Правовые последствия применения автоматизированных транспортных средств в Германии предусмотрены в части законодательства о юридической ответственности. Основное внимание в нем уделяется транспорту SAE уровней 0–2, где этот стандарт тщательно разграничивает статус водителя, владельца транспортного средства и производителя как потенциальных ответственных лиц, а также определяются условия наступления такой ответственности. Прогресс в области автоматизации транспортных средств внес на повестку дня общественности и законодателя новые вопросы ответственности, возникающие при эксплуатации автотранспортных средств на уровнях SAE 3 и 4. Особенности этих уровней автоматизации уже были предусмотрены поправками к Закону ФРГ о дорожном движении 2017 и 2021 гг. Тем не менее в Германии, наряду с достоинствами предложенных подходов, имеются и «подводные камни» этих нововведений. В связи с этим особенную остроту приобретает сегодня обсуждение сложного распределения ответственности в контексте новых тенденций в автомобильном секторе, таких как ИИ и обновление программного обеспечения. Авторы отмечают, что до сих пор в Германии нет специальных правовых норм, регулирующих эксплуатацию полностью автоматизированных транспортных средств – SAE уровня 5. Ответственность за вождение по этому стандарту – актуальная проблема для ФРГ, и в настоящее время в стране обсуждается адаптируемость существующей системы гражданской ответственности к роботизированным транспортным средствам (p. 279).

Триада внедоговорной ответственности в отношении ДТП в законодательстве ФРГ составляет: прежде всего раздел 7 Федерального закона о дорожном движении (Federal Road Traffic Act – Staßenverkehrsgesetz (StVG)), что предусматривает ответствен-

ность владельца транспортного средства за ущерб, возникший в результате смерти или увечья лица или материальный ущерб и причиненный во время эксплуатации транспортного средства; раздел 18 StVG, который регулирует ответственность водителя в случае доказательства его вины в ДТП. Кроме того, водитель может нести ответственность в соответствии с общими нормами деликтного права – раздела 823 Гражданского кодекса Германии, где также предполагается наличие вины со стороны водителя.

Наконец, производитель бракованного изделия несет ответственность за ущерб, вызванный недостатком его продукта. Немецкое законодательство не предусматривает специального правового режима ответственности за качество продукции в контексте дорожного движения. Законодательство об ответственности за качество продукции основывается на двух принципах: первый – существует Директива Совета 85/374/EEC от 25 июля 1985 г. о сближении законов, нормативных актов и административных положений государств-членов, касающихся ответственности за дефектную продукцию, O.J. L 210/29 (1985)) (Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, O.J. L 210/29 (1985)), которая была введена в действие в Германии Законом об ответственности за качество продукции (Product Liability Act – Produkthaftungsgesetz – (ProdHaftG)). Второй – производители могут подлежать ответственности в соответствии с общими нормами деликтного права, предусмотренными в разделе 823 ГК Германии, с последующими изменениями. Сегодня деликтная ответственность производителей основывается преимущественно на прецедентах и известных случаях (делах), разрешавшихся в судах, которые в основном связаны с нарушением производителем конкретных обязательств по заботливости и осмотрительности (duties of care), а также организационных требованиях на различных этапах производства (например при конструировании, производстве, инструктаже пользователя и мониторинге продукции в полевых условиях). Эту деликтную ответственность часто называют «ответственностью производителя» (“producer” liability), в отличие от «ответственности за продукт» (“product” liability), вытекающей из Закона об ответственности за качество продукции (Product Liability Act) (p. 281–282).

Исследование рассмотренных в монографии многих других национальных режимов юридической ответственности позволяет

авторам сделать обобщения и в целом правильный вывод о том, что в настоящее время сложилось два подхода к определению национального режима юридической ответственности, *когда*: 1) государства полагаются на общие концепции юридической ответственности (которые варьируются от полуобъективной до объективной (строгой) ответственности) и правила дорожного движения (в том числе когда и если существуют специальные нормы законодательства, касающиеся автономных транспортных средств). В таком подходе отсутствует возможность полностью определить виновного для всех потенциальных случаев с участием автоматизированного транспортного средства, а в нормативном плане не существует сформировавшегося правового института или полноценного массива законодательства, позволяющего гарантировать должный уровень правовой защиты в обстоятельствах применения автономных транспортных средств; 2) государства принимают специальное законодательство, вносящее изменения в традиционную схему юридической ответственности на основе принципа строгой ответственности, в соответствии с которым владелец или оператор транспортного средства и производитель будут нести ответственность за причинение вреда (p. VI).

Следует согласиться с авторами исследования в том, что сегодня существует большое количество проблем, которые необходимо решить, чтобы масштабно выпускать на рынок коммерческие автономные транспортные средства, что будут надежными, безопасными и принятыми пользователями и другими участниками дорожного движения. Высокая неопределенность, свойственная дорожному движению вообще, обусловливает требование, чтобы алгоритмы, в том числе ИИ, для передвижения автономных транспортных средств были максимально устойчивы к неопределенности, что диктует необходимость большего понимания природы этой неопределенности, включая работу с большими данными, и того, как следует измерять возникающие риски. Хотя техническая разработка методов оценки и проверки безопасности идет достаточно активно, специалисты верно подчеркивают, что в этом вопросе требуется законодательное регулирование – новые нормативные правовые акты, устанавливающие стандарты безопасности беспилотного транспорта (p. 38).

В целом данное исследование следует признать актуальным и полезным как для специалистов, работающих в сфере автоматизации транспорта, так и юристов-практиков и правоведов.

Социальные и гуманитарные науки
Отечественная и зарубежная литература
Информационно-аналитический журнал
Серия 4

**ГОСУДАРСТВО
И
ПРАВО**

2025 – № 3

Техническое редактирование
и компьютерная верстка В.Б. Сумерова
Корректор Д.Г. Валикова

Подписано к печати 07.09.2025

Формат 60×84/16	Бум. офсетная № 1
Печать офсетная	Цена свободная
Усл. печ. л. 13,75	Уч.-изд. л. 11,5
Тираж 800 экз.	Заказ №

**Институт научной информации по общественным наукам
Российской академии наук**
Нахимовский проспект, д. 51/21,
Москва, 117418
http://inion.ru

Отдел печати и распространения изданий
Тел. : (925) 517-36-91
e-mail: inion-print@mail.ru

Отпечатано в типографии
АО «Т8 Издательские Технологии»
109316, Москва, Волгоградский проспект, д. 42, корп. 5, к. 6