ПРАВО

Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2022. Т. 22, вып. 4. С. 413–423
Izvestiya of Saratov University. Economics. Management. Law, 2022, vol. 22, iss. 4, pp. 413–423
https://eup.sgu.ru https://doi.org/10.18500/1994-2540-2022-22-4-413-423
EDN: IIUKSC

Научная статья
УДК 349

Концептуальный подход к классификации и сертификации роботов и сложных автоматизированных информационных систем

Р. В. Амелин[1] ✉, Л. В. Бессонов[1], Г. Н. Комкова[1], С. Е. Чаннов[1,2]

[1]Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского, Россия, 410012, г. Саратов, ул. Астраханская, д. 83

[2] Поволжский институт управления имени П. А. Столыпина – филиал РАНХиГС при Президенте РФ, Россия, 410012, г. Саратов, ул. Московская, д. 164

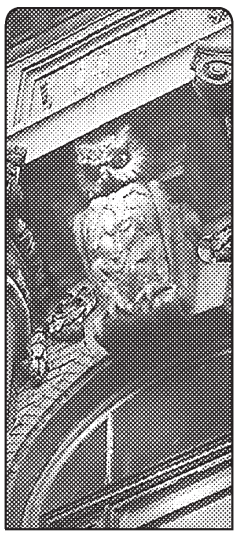
Амелин Роман Владимирович, кандидат юридических наук, доцент кафедры конституционного и муниципального права, ame-roman@yandex.ru, https://orcid.org/0000-0002-7054-5757

Бессонов Леонид Валентинович, кандидат физико-математических наук, начальник управления цифровых и информационных технологий, lexx.besson@gmail.com, https://orcid.org/0000-0002-5636-1644

Комкова Галина Николаевна, доктор юридических наук, профессор, декан юридического факультета, komkova_galina@mail.ru, https://orcid.org/0000-0002-2572-2443

Чаннов Сергей Евгеньевич, доктор юридических наук, [1]профессор кафедры таможенного, административного и финансового права, [2]заведующий кафедрой служебного и трудового права, sergeychannov@yandex.ru, https://orcid.org/0000-0002-3342-7487

Аннотация. ***Введение.*** С развитием и распространением роботов, систем искусственного интеллекта и сложных автоматизированных информационных систем связана проблема причинения вреда их решениями и действиями, а также проблема юридической ответственности за этот вред. ***Теоретический анализ.*** Одной из основных функций юридической ответственности является общая и частная превенция. В применении к роботам она требует их перепрограммирования, переобучения или ликвидации. Таким образом, с проблемой юридической ответственности автономных и временами непредсказуемых программно-технических механизмов напрямую связан экзистенциальный вопрос о возможности, формах и условиях их существования. Системная правовая конструкция, направленная на обеспечение безопасности и предсказуемости при создании и эксплуатации роботов может быть построена на основе классифицирующего стандарта, причем с каждым классом будут связаны определенные формы и модели ответственности. ***Эмпирический анализ.*** Основой правовой классификации роботов и сложных автоматизированных информационных систем будут являться угрозы, связанные с причинением вреда в результате их самопроизвольных действий и решений, соотнесенные с формами юридической ответственности. Могут быть выделены угрозы: причинения смерти человека; неправомерного изменения правового статуса субъекта; причинения материального вреда; нарушения личных неимущественных прав лица; информации или иному имуществу владельца (пользователя), не связанная с причинением вреда третьим лицам; угроза противоправного поведения роботов. ***Результаты.*** Предложена



НАУЧНЫЙ ОТДЕЛ

классификация роботов и сложных автоматизированных систем, а также подходы к юридической ответственности и обеспечению безопасности для каждого класса, указаны направления перспективной разработки правовых и технических стандартов, необходимых для обеспечения данной классификации и сертификации.

Ключевые слова: роботы, автоматизированные информационные системы, самопроизвольное поведение, юридическая ответственность, угроза причинения вреда, стандарты, классификация

Благодарности: Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект № 20-011-00355 «Эволюция права под воздействием современных цифровых технологий»).

Для цитирования: *Амелин Р. В., Бессонов Л. В., Комкова Г. Н., Чаннов С. Е.* Концептуальный подход к классификации и сертификации роботов и сложных автоматизированных информационных систем // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2022. Т. 22, вып. 4. С. 413–423. https://doi.org/10.18500/1994-2540-2022-22-4-413-423, EDN: IIUKSC

Article

Conceptual approach to the classification and certification of robots and complex automated information systems

R. V. Amelin[1] ✉, L. V. Bessonov[1], G. N. Komkova[1], S. E. Channov[1,2]

[1]Saratov State University, 83 Astrakhanskaya St., Saratov 410012, Russia

[2]Stolypin Volga Region Institute of Administration of the Russian Presidential Academy of National Economy and Public Administration, 164 Moskovskaya St., Saratov 410012, Russia

Roman V. Amelin, ame-roman@yandex.ru, https://orcid.org/0000-0002-7054-5757

Leonid V. Bessonov, lexx.besson@gmail.com, https://orcid.org/0000-0002-5636-1644

Galina N. Komkova, komkova_galina@mail.ru, https://orcid.org/0000-0002-2572-2443

Sergey E. Channov, sergeychannov@yandex.ru, https://orcid.org/0000-0002-3342-7487

Abstract. ***Introduction.*** The development and spread of robots, artificial intelligence systems and complex automated information systems are associated with the problem of causing harm by their decisions and actions, as well as the problem of legal liability for this harm. ***Theoretical analysis.*** One of the main functions of legal liability is general and private prevention. When applied to robots, it requires them to be reprogrammed, retrained, or eliminated. Thus, the issue of the possibility, forms and conditions of their existence is directly related to the problem of legal responsibility of autonomous and sometimes unpredictable software and hardware mechanisms. A systemic legal structure aimed at ensuring safety and predictability in the creation and operation of robots can be built on the basis of a classifying standard, and each class will be associated with certain forms and models of responsibility. ***Empirical analysis.*** The basis of the legal classification of robots and complex automated information systems will be the threats associated with causing harm as a result of their spontaneous actions and decisions, correlated with the forms of legal liability. The following threats can be identified: causing the death of a person; unlawful change in the legal status of the subject; causing material harm; violation of the personal non-property rights of a person; information or other property of the owner (user), not related to causing harm to third parties; the threat of illegal behavior of robots. ***Results.*** The authors propose a classification of robots and complex automated systems, as well as approaches to legal liability and security for each class, and indicate directions for promising development of legal and technical standards necessary to ensure this classification and certification.

Keywords: robots, automated information systems, spontaneous behavior, legal liability, threat of harm, standards, classification

Acknowledgements: This work was supported by the Russian Foundation for Basic Research (project No. 20-011-00355 "Evolution of law under the influence of modern digital technologies").

For citation: Amelin R. V., Bessonov L. V., Komkova G. N., Channov S. E. Conceptual approach to the classification and certification of robots and complex automated information systems. *Izvestiya of Saratov University. Economics. Management. Law*, 2022, vol. 22, iss. 4, pp. 413–423 (in Russian). https://doi.org/10.18500/1994-2540-2022-22-4-413-423, EDN: IIUKSC

Введение

Наиболее актуальная проблема, связанная с развитием систем искусственного интеллекта и распространением роботов, – проблема юридической ответственности за вред, причиненный их действиями [1–3]. Ее генезис обусловлен тремя важнейшими признаками роботов, которые, по мнению исследователей, принципиально выделяют их из класса иных программно-технических систем. Во-первых, *автономность* – робот предназначен (или способен) функционировать без участия человека, в том числе самостоятельно определять цели, принимать решения и выполнять действия, направленные на их реализацию. Во-вторых, *самообучаемость* – решения и действия робота определяются не столько заложенными в него алгоритмами, сколько внутренним состоянием, которое формируется под воздействием огромного количества обработанных данных, в том числе уже в процессе автономного функционирования робота [4]. Таким образом, разработчик,

оператор, владелец робота, а также иные субъекты в ряде ситуаций не способны предсказать решения и действия робота и каким-то образом повлиять на них. Самообучаемость очень тесно коррелирует с *необъяснимостью* – современные алгоритмы искусственного интеллекта, которые показывают наиболее эффективные результаты работы, с точки зрения человека (даже своего разработчика) представляют собой «черный ящик», не позволяющий понять, почему робот принял определенное решение или совершил определенное действие, и каким-либо образом трассировать цепочку причинно-следственных связей, приведших к этому действию и/или решению [5]. Наконец, робот обычно рассматривается как киберфизическая система, действующая в реальном мире, т. е. способная *осуществлять физическое воздействие на людей и предметы*, следовательно, причинять вред имуществу, здоровью и даже жизни людей – и прецеденты уже начинают накапливаться [6].

Однако крайне важно отметить, что проблема характерна не только для роботов. Сложные автоматизированные информационные системы (включая системы искусственного интеллекта, но не ограничиваясь ими) могут обладать теми же свойствами, порождающими те же последствия. Прежде всего, *непредсказуемостью* (невозможностью заранее предвидеть результат работы в каждом случае), но если для роботов и систем искусственного интеллекта она обусловлена объективными свойствами алгоритма (так, механика работы глубокой нейронной сети не имеет никакой объяснимой взаимосвязи с категориями реального мира, для которых она находит предсказания и взаимосвязи), то для «обычных» детерминированных систем и алгоритмов – субъективной сложностью всестороннего анализа и восприятия человеческим мозгом. Это является причиной возникновения аномалий в ситуациях, которые не были предусмотрены на этапе разработки таких систем [7, с. 28–32]. Кроме того, информационные системы *могут причинять существенный вред третьим лицам*, необязательно путем физического воздействия, а путем нарушения их субъективных прав. Руководствуясь данными, полученными от почтовой информационной системы, были несправедливо уволены, оштрафованы или привлечены к уголовной ответственности за воровство тысячи сотрудников английской почты [8]. «Предвзятое» отношение экзаменационной информационной системы способствовало несправедливому отчислению ряда студентов [9]. Некорректно работающее приложение «Социальный мониторинг» выписало множество административных штрафов без всяких на то оснований [10], не говоря уже о бесчисленном множестве нарушений субъективных информационных прав из-за сбоев и некорректного поведения самых разных информационных систем. В большинстве случаев вред, причиненный нарушением прав, достаточно сложно возместить из-за отсутствия надлежащего субъекта по тем же причинам, которые справедливы и для роботов. Поэтому важно отметить универсальный характер проблемы, притом что в сфере создания и эксплуатации автоматизированных информационных систем уже накоплено достаточное количество опыта, который может быть учтен.

Далее в этой работе мы будем для краткости использовать термины «робот» и «информационная система» в зависимости от контекста, не теряя общности и подразумевая, что посылки и выводы относятся к обеим категориям.

Теоретический анализ

На современном этапе происходит формирование и развитие теоретико-правовых подходов к проблеме юридической ответственности за решения и действия роботов. Он характеризуется множественностью таких подходов, которые существенно различаются в следующих аспектах.

Субъектный состав деликтов, связанных с роботами. В частности, при каких условиях и в каком качестве в круг субъектов может быть включен сам робот. Некоторые подходы принципиально отрицают целесообразность наделения робота правосубъектностью (позиция Европейской комиссии) [11], некоторые исследователи отрицают такую возможность по причине отсутствия у робота «человеческих» качеств, неотъемлемо связанных в существующей правовой доктрине с концепцией юридической ответственности – воли, мотивов, эмоций, самосознания и др. [12, с. 35; 13, с. 176; 14, с. 13]. Существуют подходы, связанные с наделением робота квазисубъектностью (в виде ограниченной способности нести юридическую ответственность и исполнять обязанности по возмещению вреда, равно как и в виде наделения робота только ограниченным набором прав [15]) или даже признание его полноценным субъектом права [16, с. 108].

Органы, уполномоченные рассматривать инциденты с участием роботов, устанавливать правила регулирования данной сферы: законодательные органы, суды, органы исполнительной власти, специализированные технические комиссии и т.д. [5]

Виды и формы ответственности: строгая ответственность, основанием которой является сам факт причинения вреда; деликтная ответственность, подлежащая доказыванию и распределению (солидарная или субсидиарная) [17], каскадная ответственность (ответственность без вины) [18, 19]. Пользуются популярностью подходы, основанные на модели страхования: формирование страховых фондов за счет производителей и/или владельцев роботов и квалификация причинения вреда роботом как страховых случаев (в том числе рассматриваемых как обстоятельства непреодолимой силы) [20].

Основания ответственности. Можно выделить модели, основанные на вине (что предполагает возможность и необходимость доказывания умысла или неосторожности лиц, участвующих в создании и эксплуатации робота, приведших к причинению вреда), и модели, основанные на риске, предполагающие установление общей обязанности проявлять разумную осмотрительность для предотвращения предсказуемого риска причинения вреда. Как правило, такая обязанность сводится к строгому следованию стандартам безопасности продукции и связанных с ней процессов, принятых в индустрии. Основная проблема на данном этапе заключается в том, что стандарты в сфере робототехники только формируются.

Проблема юридической ответственности не ограничивается вопросами восстановления справедливости (статус-кво) и возмещения вреда пострадавшим от действий робота. Одной из основных функций юридической ответственности является *общая и частная превенция* [21, с. 274]. Если в отношении поведения человека превенция осуществляется путем воздействия на его психическое состояние (формируя волевые импульсы, направленные на воздержание от совершения общественно вредных и опасных деяний под страхом наказания), то изменение поведения роботов требует их перепрограммирования, переобучения или ликвидации [22, с. 67]. Другими словами, с проблемой юридической ответственности автономных и временами непредсказуемых программно-технических механизмов напрямую связан экзистенциальный вопрос о возможности, формах и условиях их существования.

Решение этого вопроса может быть связано с установлением различных требований как программно-технической, так и интеллектуально-поведенческой природы. В перспективе наделения роботов правосубъектностью эти требования могут быть сформулированы в виде обращенных непосредственно к ним правовых норм, однако на текущем этапе речь может идти лишь о требованиях в отношении роботов, обращенных к лицам, ответственным за их создание и эксплуатацию. Наиболее естественно подобные требования формализуются в технических регламентах и *стандартах*.

Исторически инициатива в техническом регулировании исходит как от регулирующих органов, так и от сообщества производителей. С одной стороны, производители новых технологий и продукции заинтересованы в максимальной гибкости при разработке и вхождении на рынок (что подразумевает минимум регулирования), с другой стороны, они же заинтересованы в минимизации рисков, в том числе связанных с безопасностью использования таких технологий и продукции. Стандартизация позволяет учесть и закрепить «лучшие практики», а также внести правовую определенность в деятельность производителя, ограничивая его обязанности по обеспечению безопасности продукции соблюдением требования стандарта, если этот стандарт получает нормативное закрепление [23]. В частности, в Российской Федерации обязательные требования к продукции и связанным с ней процессам устанавливаются техническими регламентами, при этом техническому регламенту ставится в соответствие набор стандартов, добровольное соответствие которым влечет автоматическое соблюдение требований регламента [24, ч. 1 ст. 16.1].

В случае если инициатива формирования стандартов в сфере новых технологий и продукции идет от производителей, обычно имеет место период конкуренции альтернативных стандартов, их обобщение и принятие единых стандартов всеми участниками рынка, после чего такие стандарты находят отражение в нормативных правовых актах.

Представляется, что технические регламенты и стандарты, формализующие требования к роботам (в первую очередь – стандарты, поскольку для современного этапа развития данной сферы характерна множественность и конкуренция подходов к установлению требований), способны заполнить вакуум правовой определенности и лечь в основу системной правовой конструкции, направленной на обеспечение безопасности и предсказуемости при создании и эксплуатации роботов.

В частности, исходя из вышесказанного, ключевым элементом такой системы может стать

система классификации (классифицирующий стандарт), которая определит классы (категории) роботов в зависимости от их характеристик и предъявляемых к ним требований. Поскольку именно превентивная функция ответственности влияет на экзистенциальные аспекты использования роботов, то с каждым классом могут быть связаны определенные формы и модели ответственности. Этот подход как нельзя лучше, на наш взгляд, позволит систематизировать и теоретико-правовые модели ответственности за действия/решения роботов, поскольку уже сейчас представляется достаточно очевидным, что различные модели наиболее эффективны для разных типов роботов.

При этом в определении классифицирующего признака важную роль будет играть экзистенциальный *императив оценки безопасности робота*: худший сценарий его поведения является приемлемым с точки зрения риска, который включает вероятность реализации данного сценария (с учетом всех принятых мер, в том числе программно-технических ограничителей, предусмотренных у робота) и последствия его реализации (включая как причиненный ущерб, так и реальную возможность его компенсации, восстановления статус-кво).

Эмпирический анализ

Прежде чем перейти к рассмотрению концепции предлагаемого стандарта (системы классификации), выделим с позиции юридической ответственности две наиболее распространенные категории программно-технических систем, правовое регулирование которых не требует особенных новаций, но, тем не менее, имеет важные нюансы, не всегда учитываемые при создании и использовании таких систем.

1. *Контролируемые роботы и информационные системы.* Отнесем к ним программно-технические системы или их компоненты, действия которых выполняются по инициативе и под контролем человека – оператора. Оператор полностью несет ответственность за последствия таких действий, если эти системы обладают двумя важными свойствами:

– *причинность и предсказуемость*: передавая на выполнение команду, оператор должен знать ее назначение и быть способен предвидеть результаты ее выполнения. Как минимум соответствующие разъяснения и инструкции должны содержаться в пользовательской документации. Если же поведение системы отличается от того, что ожидал и должен был ожидать оператор, ответственность за последствия будет нести разработчик;

– *апеллируемость:* оператор, отдавший системе команду на выполнение определенных действий, не может отрицать своей роли и объяснять действия программной ошибкой, самопроизвольной реакцией системы, результатами обучения робота и т.д. [25, с. 29]. Другими словами, во всех случаях, когда инициатором действия является человек, система должна позволять безошибочно это удостоверить.

2. *Предсказуемые роботы и информационные системы.* Эта категория включает первую и расширяет ее в отношении автономных подсистем, которые выполняют действия не только в ответ на команды оператора, но и в автоматическом режиме (включая реакцию на данные с приборов и датчиков, результаты обработки первичных данных, иные действия, вызванные изменением внутреннего состояния системы). Действия предсказуемых систем являются результатами причинно-следственных связей, предусмотренных и умышленно заложенных разработчиками (другими словами, система делает именно то, что от нее и хотели), которые изначально несут ответственность за последствия (при этом она может быть делегирована владельцу, пользователю или бенефициару системы, например, на основе соглашения).

В парадигме предшествующего периода все программно-технические системы предполагались по умолчанию контролируемыми и предсказуемыми, при этом наличие в них ошибок (зачастую многочисленных) эту парадигму не колебало, ошибки в основном рассматривались как неумышленная форма вины (небрежность) со стороны разработчиков, при этом подход, установившийся в качестве фактического стандарта индустрии, предусматривал отказ от претензий на основании пользовательского соглашения [26]. Хотя эта парадигма возникла в период однопользовательских систем, выгоду от использования которых нес их владелец и он же брал на себя все риски, она принципиально не изменилась при повсеместном распространении многопользовательских информационных систем – прежде всего социальных сетей и сервисов, а также государственных и муниципальных информационных сетей, ошибки которых влияли уже на пользователей, лишь косвенно заинтересованных в их функционировании. Однако перспективы распространения роботов и систем, способных причинить существенный вред третьим лицам, требуют смены парадигмы. Оставляя за пределами данного исследования вопросы допустимости делегирования ответственности за действия контролируемых и предсказуемых систем, отметим, что в новой парадигме

наиболее важно предусмотреть последствия *самопроизвольного*[1] поведения роботов, которое не ожидалось и не планировалось человеком, а обусловлено внутренним состоянием системы, сформировавшимся под воздействием машинного обучения, непредсказуемых внешних факторов, программных ошибок или комбинации перечисленного.

Таким образом, в основу правовой классификации роботов и сложных автоматизированных информационных систем предлагается положить основные угрозы, связанные с причинением вреда в результате их самопроизвольных действий и решений, соотнесенные с формами юридической ответственности. Отметим, что общие контуры такого подхода уже обсуждались в литературе. В частности, И. Р. Бегишев приходил к выводу, что деликтная ответственность за вред, причиненный роботом, должна наступать в зависимости от класса его опасности и степени автономности робота [27]. Мы, однако, видим перспективы применения не только деликтной, но и иных форм ответственности в зависимости от класса опасности робота. Кроме того, ключевым моментом данной концепции является акцент на отсутствие умысла субъекта-человека в сценариях вероятных угроз. Роботы, иные программно-технические системы, запрограммированные на причинение вреда или причиняющие такой вред в результате соответствующих команд оператора, относятся к традиционным описанным выше категориям, не требующим специальных моделей юридической ответственности.

Выделим в качестве концептуальных следующие классы угроз.

Класс А. Угроза смерти человека (людей) в результате решений и действий робота. Следует специально подчеркнуть еще раз, что к данному классу относятся системы, способные причинить смертельный вред «неумышленно», вследствие самообучения или возникновения нестандартной ситуации, которую было невозможно или крайне сложно предвидеть на этапе проектирования и разработки. Тем не менее, исходя из физических характеристик, сферы использования и особенностей алгоритмов робота можно определить возможность и вероятность такого развития событий. Очевидно, что домашний пылесос и беспилотный автомобиль принципиально различаются в этом отношении [1, p. 20] точно так же, как полностью управляемый военный беспилотник и автономный робот-разведчик. Но если в первом случае различие в уровне угрозы относится к физическим характеристикам, то во втором – к возможности совершения непредсказуемых и неконтролируемых действий.

Для отнесения определенной модели роботов к данному классу потребуются стандарт и связанная с ним система сертификации, определяющие актуальность угрозы причинения смерти. Даже робот-пылесос при определенных обстоятельствах может привести к фатальной ситуации (например, неожиданно наехать на человека с больным сердцем или стоящего на краю балкона со снятыми ограждениями), но подобное развитие событий крайне маловероятно, поэтому угроза причинения смерти действиями робота-пылесоса должна быть классифицирована стандартом как неактуальная, а сам робот не должен относиться к рассматриваемому классу.

Угроза причинения смерти людей в результате неуправляемых и непредсказуемых решений и действий робота, очевидно, является неприемлемой, поэтому производитель обязан предусмотреть механизмы для ее предотвращения, такие как возможность вмешательства оператора в действия робота, автоматическое отключение или переход на управление оператором в случае возникновения непредвиденной или опасной для человека ситуации, возможность деактивации всей партии роботов после инцидента и т.д. Потребуется ряд стандартов, определяющих требования к наличию этих механизмов и их характеристикам.

Предполагаем, что для роботов класса А должна вводиться *превентивная ответственность*, связанная с установлением запрета на производство и эксплуатацию таких роботов без соответствующих механизмов предотвращения (минимизации) угрозы. Лицо, производящее или использующее таких роботов, должно подлежать административной и/или уголовной ответственности с формальным составом, независимо от факта причинения вреда. Аналогичная ответственность должна наступать за использование несертифицированного робота, который при расследовании инцидента будет отнесен к классу А.

Отметим также, что любой инцидент со смертельным исходом, так или иначе связанный с действиями и/или решениями робота (сложной автоматизированной информационной системы),

[1] Мы используем термин «самопроизвольное» («спонтанное») для обозначения такого поведения с некоторой долей условности за неимением лучшего термина (варианты: «непредусмотренное», «собственное» поведение). Условность заключается в том, что самопроизвольность (спонтанность) подразумевает обычно поведение под влиянием исключительно внутренних факторов, на поведение робота оказывают влияние и внешние факторы (хотя, безусловно, перед этим они трансформируются в изменения внутреннего состояния). В нашем понимании делается акцент на трактовке спонтанности (самопроизвольности) как независимости от человеческого воздействия (и зачастую необъяснимости человеческой логикой).

должен расследоваться специальной комиссией, а результаты такого расследования – учитываться органами и организациями по сертификации, а также служить основанием для пересмотра класса соответствующей категории роботов.

Класс B. Угроза неправомерного изменения правового статуса субъекта. Связана с непредсказуемыми действиями автоматизированной информационной системы, способной устанавливать и квалифицировать юридические факты и принимать решения, влияющие на правовой статус людей (а также юридических лиц и иных субъектов). В первую очередь, это касается государственных и муниципальных информационных систем, обеспечивающих формирование и ведение реестров, предназначенных для регистрации и/или удостоверения таких прав. Ошибочные действия подобных систем в нестандартных ситуациях могут повлиять не просто на отдельные права, но и на правовой статус лица в целом. Вполне логично прогнозировать и появление роботизированных систем, действующих от лица государства (робот-полицейский, предотвращающий правонарушения или применяющий меры воздействия к нарушителю).

Для систем класса B предлагается установление строгой ответственности их владельца – государства или государственного органа. Таким образом, мы согласны с утверждением, что ответственность за нарушение прав человека должна вытекать из самого факта (в отличие от ответственности за нанесение материального вреда, которая доказывается и распределяется) [1]. Правовой режим такой системы должен включать процедуры обжалования решений и действий системы, выявления ошибочных действий. Пострадавший субъект подлежит восстановлению в правовом статусе с компенсацией, а система, принимающая некорректные решения, должна быть выведена из обращения до устранения причин. Процедура должна быть эквивалентна процедуре отмены незаконного правового акта с приданием обратной силы иным незаконным решениям, которые были вынесены вследствие аналогичных причин.

Класс C. Угроза материального вреда (имуществу, здоровью и т.д.). Исходя из общих начал частного права, неумышленно причиненный материальный вред подлежит возмещению. Основные дискуссии, связанные с правовым положением роботов, касаются распределения материальной ответственности между владельцем, производителем, оператором робота, специальным страховым фондом и даже самим роботом (в перспективе наделения его правосубъектностью). Некоторые обобщения этой дискуссии с учетом принципов справедливости и реализуемости позволяют предварительно выделить несколько подклассов:

– *C1. Робот, обладающий индивидуальным страховым фондом*. К этому классу целесообразно отнести прежде всего роботов, приносящих прибыль в процессе своей эксплуатации: беспилотное такси, нейронная сеть, рисующая художественные произведения, и т.д. В процессе деятельности такого робота может формироваться индивидуальный фонд, достаточный для покрытия потенциального вреда от использования данного робота. Начальное формирование фонда может происходить за счет средств бенефициара робота, а функционирование робота может быть поставлено в зависимость от его обеспечения (приостанавливается, если объем фонда становится меньше необходимой величины). Методики формирования и расчета минимального объема фонда могут устанавливаться соответствующими стандартами в зависимости от сферы деятельности робота;

– *C2. Робот, обеспеченный коллективным страховым фондом*. Наиболее перспективный подход к обеспечению ответственности за решения и действия робота в текущей правовой парадигме и в то же время требующий наиболее сложного технического регулирования как в части принципов формирования и расходования страхового фонда, так и правил отнесения роботов к обеспечиваемой группе (поскольку с учетом фундаментальных различий в рисках, связанных с их использованием, разные виды и модели роботов будут давать принципиально разную нагрузку на общий фонд);

– *C3. «Необеспеченный» робот*. В отсутствие страхового фонда или иных фондов, обеспечивающих материальную компенсацию пострадавшим от действий роботов и сложных автоматизированных систем, ответственность (солидарная или субсидиарная) должна быть возложена на субъектов, организующих создание и/или использование робота.

Важно отметить, что уменьшить риск причинения вреда самопроизвольными действиями подобного робота путем минимизации ущерба достаточно сложно (в отличие от подклассов C1 и C2, для которых действенной мерой является формирование страхового фонда), поэтому основные усилия должны быть сосредоточены на минимизации вероятности возникновения таких событий. Помимо технических требований к обеспечению безопасности их деятельности необходима серия стандартов для различных сфер деятельности и типов роботов, устанавливающих необходимые механизмы управления и контро-

ля, позволяющие предотвращать или иным образом влиять на инциденты. Соответствующие стандарты позволят обеспечить возможность определения лица, ответственного за инцидент (производитель, владелец, оператор, иное лицо) и несущего основную ответственность. Если же робот не обладает подобным механизмом и не имеет соответствующего сертификата, полную материальную ответственность за результаты его действий несет владелец робота.

Таким образом, для данного подкласса наиболее органично подходит, на наш взгляд, модель, предложенная М. Шерером, который предложил создать агентство по делам роботов, которое занималось бы разработкой требований (политик) в сфере искусственного интеллекта, а также их сертификацией. В соответствии с моделью ответственности М. Шерера производители и продавцы программ искусственного интеллекта, сертифицированных агентством, будут подлежать ограниченной деликтной ответственности, в то время как вред, причиненный в результате коммерческой продажи и использования несертифицированных программ, предполагает полную солидарную ответственность [5, p. 394].

Класс D. Угроза нарушения личных неимущественных прав лица, в частности, нарушение права на свободу информации (системой автоматической фильтрации), нарушение авторского права (нейронной сетью, создающей вторичные произведения), причинение морального вреда и т.д. Представляется, что общий подход к юридической ответственности за действия таких роботов может быть схожим с описанным для класса С.

Класс E. Угроза информации или иному имуществу владельца (пользователя) робота или автоматизированной информационной системы, не связанная с причинением вреда третьим лицам. Ответственность может быть определена соглашением владельца с производителем данного робота или системы.

Класс F. Угроза противоправного поведения роботов, не связанного с причинением вреда конкретным субъектам, но создающего опасность причинения такого вреда в будущем, либо иные общественно опасные последствия (например, робот, «обучившийся» производить наркотические вещества или создавать других роботов, не соответствующих требованиям безопасности). Представляется, что общий подход должен быть аналогичен классу А: робот, который по своим программно-техническим характеристикам относится к классу F, должен иметь сертификат, подтверждающий наличие механизмов, нивелирующих угрозу самопроизвольного противоправного поведения. Однако стоит отметить, что поскольку понятие противоправного поведения постоянно эволюционирует вместе с законодательством, а требовать от любого робота (или автоматизированной информационной системы) самостоятельно следить за новыми нормативными правовыми актами бессмысленно, то при разработке соответствующих стандартов понадобятся некоторый универсализированный подход, подтверждающий гарантии законопослушного поведения робота по ряду направлений (которые могут быть связаны со сферами деятельности либо с возможными объектами правонарушений), а также регулярная повторная сертификация, учитывающая изменения требований по соответствующему направлению.

В зависимости от возможностей и характеристик робота он может быть отнесен к смежным классам (например, «АС»), что потребует соблюдения требований стандартов, относящихся к каждому из составляющих классов, и гибридной модели ответственности – в зависимости от конкретных последствий самопроизвольных действий и решений робота. Очевидно также, что одна и та же система/робот может быть способна на запрограммированные (предсказуемые), контролируемые и самопроизвольные действия – в каждом из этих случаев будут применяться соответствующие виды ответственности.

Результаты

Подход к классификации программно-технических систем, в которой ключевые критерии носят юридический характер, является достаточно устоявшимся в российском праве, в частности, можно привести пример классов объектов критической информационной инфраструктуры, систем, обрабатывающих персональные данные, и т.д.

Системная правовая конструкция в сфере создания и использования роботов на современном этапе развития технологий искусственного интеллекта, сложных автоматизированных информационных систем и кибернетических механизмов может быть построена на базе системы стандартов, основным из которых будет выступать нормативно закрепленный классифицирующий стандарт, концепция которого представлена выше. В дополнение к нему потребуется ряд обеспечивающих стандартов, часть из которых будет носить технико-юридический, а часть – технический характер, в том числе:

– общие стандарты, устанавливающие этические и другие экзистенциальные ограничения при создании и использовании роботов;

– идентифицирующие стандарты, позволяющие отнести робота к определенному классу или классам в соответствии с предложенной концепцией (например, стандарт для расчета риска непредусмотренного причинения смерти человека при использовании робота);

– стандарты, устанавливающие требования к безопасности робота (в зависимости от его класса, сферы действия, типов используемых алгоритмов и т.д.), включая требования к системам управления и контроля;

– технические стандарты, регламентирующие различные аспекты безопасности, совместимости, эффективности отдельных компонентов, алгоритмов, технических средств, а также методов создания и использования роботов.

Множество таких стандартов уже сейчас разрабатывается и используется различными производителями. Их системная интеграция и частичная имплементация в правовых нормах позволит, в частности, подойти к решению проблемы юридической ответственности за действия и решения роботов, а в общем – обеспечить безопасное и устойчивое развитие современных цифровых технологий.

Список литературы

1. *Yeung K.* Responsibility and AI, Council of Europe Study DGI, 2019. URL: https://rm.coe.int/responsability-and-ai-en/168097d9c5 (дата обращения: 15.08.2022).
2. *Незнамов А. В., Наумов В. Б.* Стратегия регулирования робототехники и киберфизических систем // Закон. 2018. № 2. С. 69–89.
3. *Михалева Е. С., Шубина Е. А.* Проблемы и перспективы правового регулирования робототехники // Актуальные проблемы российского права. 2019. № 12. С. 26–35. https://doi.org/10.17803/1994-1471.2019.109.12.026-035
4. *Russell S. J., Norvig P.* Artificial Intelligence: A Modern Approach. Malaysia : Pearson Education Limited, 2016. 1152 p.
5. *Scherer M. U.* Regulating Artificial Intelligence Systems: Risks Challenges Competencies and Strategies // Harvard Journal of Law & Technology. 2016. Vol. 29, № 2. P. 354–400. http://dx.doi.org/10.2139/ssrn.2609777
6. *Бегишев И. Р.* Пределы уголовно-правового регулирования робототехники // Вестник Санкт-Петербургского университета. Право. 2021. № 3. С. 529–530. https://doi.org/10.21638/spbu14.2021.303
7. *Шубинский И. Б.* Функциональная надежность информационных систем. Методы анализа. М. : Журнал «Надежность», 2012. 296 с.
8. Mitchell C. Bad software sent postal workers to jail, because no one wanted to admit it could be wrong // The Verge, 2021. URL: https://www.theverge.com/2021/4/23/22399721/uk-post-office-software-bug-criminal-convictions-overturned (дата обращения: 15.08.2022).
9. *Алиева Ф.* Студентов СПбГУ отчислили за «отвод глаз от монитора» во время онлайл-экзамена. «Списывание» зафиксировала программа // Сноб, 2021. URL: https://snob.ru/news/studentov-spbgu-otchislili-za-otvod-glaz-ot-monitora-vo-vremya-onlajl-ekzamena-spisyvanie-zafiksirovala-programma/ (дата обращения: 15.08.2022).
10. Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций : в 2 т. / под ред. Н. Н. Ковалёвой. Т. 2. Саратов : Изд-во Саратовской гос. юрид. акад., 2020. 202 с.
11. European Commission, Directorate-General for Justice and Consumers, Liability for artificial intelligence and other emerging digital technologies, Publications Office, 2019. https://data.europa.eu/doi/10.2838/573689
12. *Чиркин В. Е.* Юридическое лицо публичного права. М. : Норма, 2007. 352 с.
13. *Грачева Ю. В., Арямов А. А.* Роботизация и искусственный интеллект: уголовно-правовые риски в сфере общественной безопасности // Актуальные проблемы российского права. 2020. Т. 15, № 6. С. 169–178. https://doi.org/10.17803/1994-1471.2020.115.6.169-178
14. *Карлаш Д. С.* Право роботов: метафизические и социально-экономические аспекты // Предпринимательское право. Приложение «Право и Бизнес». 2018. № 4. С. 9–15.
15. *Пономарева Е. В.* Субъекты и квазисубъекты права: теоретико-правовые проблемы разграничения : дис. … канд. юрид. наук. Екатеринбург, 2019. 208 с.
16. Регулирование робототехники: введение в «робоправо». Правовые аспекты развития робототехники и технологий искусственного интеллекта / под ред. А. В. Незнамова. М. : Инфотропик Медиа, 2018. 232 с.
17. *Головизнин А. В.* Деликтная ответственность в случаях применения роботов // Вестник Уральского юридического института МВД России. 2022. № 2. С. 82–88.
18. *Луценко* С. Имплементация института искусственного интеллекта в российское законодательство // Цифровая экономика, 2002. URL: http://digital-economy.ru/images/easyblog_articles/802/impl24324.pdf (дата обращения: 15.08.2022).
19. *Дэгерг М.* Ответственность без вины и социализация рисков во французском праве // Lex Russica. 2016. № 1. С. 51–58.
20. P8_TA(2017)0051 Civil Law Rules on Robotics, European Parliament (2014–2019). URL: https://www.eu-roparl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf (дата обращения: 15.08.2022).
21. *Алексеев С. С.* Проблемы теории права: курс лекций : в 2 т. Т. 1. М. : Юридическая литература, 1982. 359 с.
22. *Васильев А. А., Васильева О. В., Ибрагимов Ж. И.* «Закон Гришина» и право ЕС о робототехнике и искусственном интеллекте: сравнительный анализ // Проблемы правовой и технической защиты информации. 2019. № 7. С. 64–70.
23. *Авдашева С. В., Крючкова П. В.* Система технического регулирования в Российской Федерации:

формирование, возможное и ожидаемое воздействие на конкуренцию и конкурентоспособность. М. : Гос. ун-т «ВШЭ», 2009. 68 с. (Препринт / НИУ ВШЭ WP1/2009/04) (Серия WP1. Институциональные проблемы российской экономики).

24. О техническом регулировании : федер. закон от 27.12.2002 № 184-ФЗ (ред. от 02.07.2021) // Собр. законодательства Рос. Федерации. 2002. № 52 (ч. 1), ст. 5140.
25. *Сухостат В. В., Васильева И. Н.* Основы информационной безопасности : учеб. пособие. СПб. : Изд-во СПбГЭУ, 2019. 104 с.
26. M.A. Mortenson Company, Inc. (Petitioner), v. Timberline software corporation and Softworks Data Systems, Inc., Respondents // FindLaw. URL: https://caselaw.findlaw.com/wa-supreme-court/1409490.html (дата обращения: 15.08.2022).
27. *Бегишев И. Р.* Размышления о проекте Федерального закона «Об обороте роботов, их составных частей (модулей)» // Право и цифровая экономика. 2021. № 2. С. 379–390.

References

1. Yeung K. *Responsibility and AI, Council of Europe Study DGI*, 2019. Available at: https://rm.coe.int/responsability-and-ai-en/168097d9c5 (accessed 15 August 2022).
2. Neznamov A. V., Naumov V. B. Regulation strategy for robotics and cyberphysical systems. *Zakon* [Law], 2018, no. 2, pp. 69–89 (in Russian).
3. Mikhaleva E. S., Shubina E. A. Challenges and prospects of the legal regulation of robotics. *Aktual'nye problemy rossiiskogo prava* [Actual Problems of Russian Law], 2019, no. 12, pp. 26–35 (in Russian). https://doi.org/10.17803/1994-1471.2019.109.12.026-035
4. Russell S. J., Norvig P. *Artificial Intelligence: A Modern Approach*. Malaysia, Pearson Education Limited, 2016. 1152 p.
5. Scherer M. U. Regulating Artificial Intelligence Systems: Risks Challenges Competencies and Strategies. *Harvard Journal of Law & Technology*, 2016, vol. 29, no. 2, pp. 354–400. http://dx.doi.org/10.2139/ssrn.2609777
6. Begishev I. R. Limits of criminal law regulation of robotics. *Vestnik of Saint Petersburg University. Law*, 2021, no. 3, pp. 529–530 (in Russian). https://doi.org/10.21638/spbu14.2021.303
7. Shubinskij I.B. *Funktsional'naya nadezhnost' informatsionnykh sistem. Metody analiza* [Functional Reliability of Information Systems. Analysis Methods]. Moscow, Zhurnal "Nadezhnost'", 2012. 296 p. (in Russian).
8. Mitchell C. Bad software sent postal workers to jail, because no one wanted to admit it could be wrong. *The Verge*, 2021. Available at: https://www.theverge.com/2021/4/23/22399721/uk-post-office-software-bug-criminal-convictions-overturned (accessed 15 August 2022).
9. Alieva F. St Petersburg University students were expelled for "taking their eyes off the monitor" during an online exam. "Write-off" was fixed by the program. *Snob*, 2021. Available at: https://snob.ru/news/studentov-spbgu-otchislili-za-otvod-glaz-ot-monitora-vo-vremya-onlajl-ekzamena-spisyvanie-zafiksirovala-programma/ (accessed 15 August 2022) (in Russian).
10. Kovaleva N. N. (ed.) *Problemy i vyzovy tscifrovogo obshchestva: tendentsii razvitiya pravovogo regulirovaniya tsifrovykh transformatsiy* [Problems and Challenges of the Digital Society: Trends in the Development of Legal Regulation of Digital Transformations]. Vol 2. Saratov, Saratov State Law Academy Publ., 2020. 202 p. (in Russian).
11. European Commission, Directorate-General for Justice and Consumers, Liability for artificial intelligence and other emerging digital technologies, Publications Office, 2019. https://data.europa.eu/doi/10.2838/573689
12. Chirkin V. E. *Juridicheskoe litso publichnogo prava* [Legal Entity of Public Law]. Moscow, Norma Publ., 2007. 352 p. (in Russian).
13. Gracheva Ju. V., Aryamov A. A. Robotization and artificial intelligence: Criminal legal risks in the field of public security. *Aktual'nye problemy rossiiskogo prava* [Actual Problems of Russian Law], 2020, vol. 15, no. 6, pp. 169–178 (in Russian). https://doi.org/10.17803/1994-1471.2020.115.6.169-178
14. Karlash D. S. The right of robots: Metaphysical and socioeconomic aspects. *Predprinimatel'skoe pravo. Prilozhenie "Pravo i Biznes"* [Entrepreneurial Law. Application "Law and Business"], 2018, no. 4, pp. 9–15 (in Russian).
15. Ponomareva E. V. *Subjects and Quasi-Subjects of Law: Theoretical and Legal Problems of Differentiation*. Diss. Cand. Sci. (Jur.). Yekaterinburg, 2019. 208 p. (in Russian).
16. Neznamov A. V. (ed.) *Regulirovanie robototekhniki: vvedenie v "robopravo". Pravovye aspekty razvitiya robototekhniki i tekhnologiy iskusstvennogo intellekta* [Regulation of Robotics: An Introduction to "Robolaw". Legal Aspects of the Development of Robotics and Artificial Intelligence Technologies]. Moscow, Infotropik Media, 2018. 232 p. (in Russian).
17. Goloviznin A. V. Delict responsibility in cases of the use of robots. *Bulletin of the Ural Law Institute of the Ministry of the Interior of Russia*, 2022, no. 2, pp. 82–88 (in Russian).
18. Lucenko S. Implementation of the Institute of Artificial Intelligence in Russian Legislation. *Digital Economy*, 2002. Available at: http://digital-economy.ru/images/easyblog_articles/802/impl24324.pdf (accessed 15 August 2022) (in Russian).
19. Deguergue M. Liability Without Fault and Socialization of Risks in French Law. *Lex Russica*, 2016, no. 1, pp. 51–58 (in Russian).
20. P8_TA(2017)0051 Civil Law Rules on Robotics, European Parliament (2014–2019). Available at: https://

www.eu-roparl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf (accessed 15 August 2022).

21. Alekseev S. S. *Problemy teorii prava* [Problems of the Theory of Law]. Vol. 1. Moscow, Juridicheskaya literatura Publ., 1982. 359 p. (in Russian).
22. Vasiliev A. A., Vasilieva O. V., Ibragimov Zh. I. "Grishin's Law" and EU law on robotics and artificial intelligence: a comparative analysis. *Problemy pravovoi i tekhnicheskoi zashchity informatsii* [Problems of Legal and Technical Protection of Information], 2019, no. 7, pp. 64–70 (in Russian).
23. Avdasheva S. V., Krjuchkova P. V. *Sistema tekhnicheskogo regulirovaniya v Rossiiskoi Federatsii: formirovanie, vozmozhnoe i ozhidaemoe vozdeistvie na konkurentsiyu i konkurentosposobnost'* [The System of Technical Regulation in the Russian Federation: Formation, Possible and Expected Impact on Competition and Competitiveness]. Moscow, NIU VShE, 2009. 68 p. (Preprint NIU VShE WP1/2009/04) (Series Institutional problems of the Russian economy) (in Russian).
24. On Technical Regulation. Federal Law 184-FZ of December 27, 2002 (an edition of July 2, 2021). *Sobranie zakonodatel'stva RF* [Collection of Laws of the Russian Federation], 2002, no. 52 (pt. 1), art. 5140 (in Russian).
25. Sukhostat V. V., Vasil'eva I. N. *Osnovy informatsionnoy bezopasnosti* [Fundamentals of Information Security]. St. Petersburg, St. Petersburg State University of Economics Publ., 2019. 104 p. (in Russian).
26. M.A. Mortenson Company, Inc. (Petitioner), v. Timberline software corporation and Softworks Data Systems, Inc., Respondents. *FindLaw*. Available at: https://caselaw.findlaw.com/wa-supreme-court/1409490.html (accessed 15 August 2022).
27. Begishev I. R. Reflections on the draft federal law "On the turnover of robots, their components (modules)". *Law and Digital Economy*, 2021, no. 2, pp. 379–390 (in Russian).

Поступила в редакцию 29.08.2022; одобрена после рецензирования 10.09.2022; принята к публикации 16.09.2022
The article was submitted 29.08.2022; approved after reviewing 10.09.2022; accepted for publication 16.09.2022