

Дата поступления рукописи в редакцию: 12.09.2026 г.

DOI: 10.24412/2076-1503-2026-10-970-975

Дата принятия рукописи в печать: 29.10.2026 г.

КОВАЛЬКОВА Елена Юрьевна,
кандидат юридических наук, доцент,
Казанский филиал ФГБОУ ВО «Российский государственный
университет правосудия им. В.М. Лебедева»,
Казань, Россия,
тел.: +7-917-273-22-87,
e-mail: ekovalkova@yandex.ru

АЛЕМПЕЕВ Георгий Сергеевич,
Казанский филиал ФГБОУ ВО «Российский государственный
университет правосудия им. В.М. Лебедева»,
Казань, Россия,
тел.: +7-987-187-90-97,
e-mail: georgyalempееv@yandex.ru

ГРАЖДАНСКО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЛАЧНЫХ ЭКОСИСТЕМАХ ОРГАНИЗАЦИЙ

Аннотация. В статье рассматриваются актуальные вопросы гражданско-правового регулирования применения систем искусственного интеллекта (ИИ) в облачных экосистемах. Авторы анализируют структуру облачных сервисов (IaaS, PaaS, APM, Cloud Security, Big Data и ИИ), определяют место ИИ в цепочке договорных связей между предпринимателем, облачным провайдером и провайдером СУБД. Особое внимание уделяется проблеме определения субъекта гражданско-правовой ответственности за вред, причинённый автономными системами ИИ. Исследуется зарубежный опыт и положения Европейского закона об ИИ (AI Act). Обосновывается необходимость применения риск-ориентированного подхода к регулированию ИИ, а также предлагается признать ИИ, задействованный в облачных экосистемах, источником повышенной опасности с внесением соответствующих дополнений в п. 1 ст. 1079 ГК РФ.

Ключевые слова: искусственный интеллект, облачные экосистемы, облачный провайдер, СУБД, гражданско-правовая ответственность, источник повышенной опасности, риск-ориентированный подход, AI Act.

Для цитирования: Ковалькова Е. Ю., Алемпеев Г. С. Гражданско-правовое регулирование использования искусственного интеллекта в облачных экосистемах организаций // Образование и право. 2026. № 10. С. 970–975.

KOVALKOVA Elena Yuryevna,
Candidate of Legal Sciences, Associate Professor,
Kazan branch of the Federal State Budget-Funded
Educational Institution of Higher Education
"Russian State University of Justice named after V.M. Lebedev"
(the city of Kazan), Kazan, Russia

ALEMPREEV Georgy Sergeyevich,
Kazan branch of the Federal State Budget-Funded
Educational Institution of Higher Education
"Russian State University of Justice named after V.M. Lebedev"
(the city of Kazan), Kazan, Russia

CIVIL LAW REGULATION OF THE USE OF ARTIFICIAL INTELLIGENCE IN CLOUD ECOSYSTEMS

Annotation. *The article deals with the current issues of civil law regulation of the use of artificial intelligence (AI) systems in cloud ecosystems. The author analyzes the structure of cloud services (IaaS, PaaS, APM, Cloud Security, Big Data and AI) and determines the place of AI in the chain of contractual relations between an entrepreneur, a cloud provider and a DBMS provider. Particular attention is paid to the problem of determining the subject of civil liability for harm caused by autonomous AI systems. The foreign experience is studied, in particular, the case Ruby Lowe v. Cerner Corporation and the provisions of the European AI Act. The necessity of applying a risk-based approach to AI regulation is substantiated, and it is proposed to recognize AI used in cloud ecosystems as a source of increased danger with corresponding amendments to paragraph 1 of Article 1079 of the Civil Code of the Russian Federation.*

Key words: *artificial intelligence, cloud ecosystems, cloud provider, DBMS, civil liability, source of increased danger, risk-based approach, AI Act.*

For citation: *Kovalkova E. Yu., Alempiev G. S. Civil law regulation of the use of artificial intelligence in cloud ecosystems. Education and law. 2026;(10):970–975. (In Russ.).*

Введение

В настоящее время стремительными темпами развивается цифровизация, а особенно системы на базе искусственного интеллекта (далее – ИИ). Национальный стандарт РФ ГОСТ Р 71476-2024 даёт следующее определение: «система ИИ: техническая система, использующая одну или несколько моделей ИИ, которая порождает такие конечные результаты, как контент, прогнозы, рекомендации или решения для заданного набора определённых человеком целей».

Вступивший в силу с 1 сентября 2026 г. Федеральный закон от 26.07.2026 № 243-ФЗ «О поддержке развития технологий искусственного интеллекта в Российской Федерации» [8] (далее – 243-ФЗ) даёт уже более развернутое и современное определение: ИИ – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая способность самостоятельно совершенствовать свои функции, повышать точность решений за счет анализа новых данных и выполнять 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 такое, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений.

Оцифровка документов, развитие электронных коммуникационных сетей, стремление к сокращению производственных издержек приводят к появлению так называемых облачных экосистем.

Облачные экосистемы представляют собой набор сервисов, документов, корпоративных порталов, мессенджеров, хранилищ и т.п., а также сторонних независимых разработчиков ПО, взаимосвязанных между собой с целью упрощения создания и интеграции бизнес-решений. Ключевы-

ми элементами подобных баз данных являются: 1) IaaS – инфраструктура и вычислительные ресурсы, непосредственно облачное хранилище, а также сетевые инфраструктуры (VPC, CDN); 2) PaaS – реляционные и нереляционные базы данных, очереди сообщений, бессерверные вычисления; 3) APM – комплекс инструментов, использующихся для отслеживания и дальнейшего анализа производительности систем, CD и CI платформы; 4) Cloud Security – контроль прав пользователей, сервисов, средства шифрования и т.д.; 5) Big Data и ИИ.

Степень научной разработанности темы. Вопросы правового регулирования ИИ и облачных технологий рассматривались в работах Т. В. Батуры, Ф. А. Мурзина, Д. Ф. Семич [1], а также в аналитических отчётах Gartner [2] и практических руководствах [3]. Однако комплексный анализ гражданско-правовой ответственности за деятельность ИИ именно в облачных экосистемах остаётся недостаточно изученным, что обуславливает актуальность настоящего исследования.

Цель и задачи исследования

Целью работы является выявление особенностей гражданско-правового регулирования использования ИИ в облачных экосистемах и определение оптимальной модели ответственности за причинение вреда такими системами.

Для достижения указанной цели поставлены следующие задачи: проанализировать структуру облачных экосистем и роль ИИ в них; исследовать договорные связи между участниками облачных отношений; изучить существующие концепции ответственности за вред, причинённый ИИ; обосновать применение риск-ориентированного подхода и необходимость признания ИИ источником повышенной опасности.

Методы исследования

В работе использованы общенаучные и частнонаучные методы: анализ, синтез, формально-юридический метод, сравнительно-правовой ме-

тод (при сопоставлении российского и европейского законодательства), а также метод кейс-стади (при рассмотрении судебного дела *Ruby Lowe v. Cerner Corporation*).

Результаты исследования

Важно отметить, что в облачных сценариях ИИ представляет собой не просто чат-бот, который организации внедряют в цифровую структуру, а элемент аналитической системы. Интеграция ИИ непосредственно с CRM открывает доступ к данным с информацией о клиентах, перепискам, историям заказов, что позволяет ему самостоятельно сформировать предложение и отправить его клиенту. Более того, ИИ способен не только анализировать уже имеющиеся данные, но и прогнозировать новые. Имея доступ к базе данных, хранилищу, ИИ приступает к созданию аналитической сводки, на основании которой создаёт документ, отправляемый в мессенджер. В таком сценарии использования представляется резонным наделять его статусом «электронного агента». Перечень задач, выполняемых ИИ в облачных экосистемах, обширен, вследствие чего некорректно разделять его на генеративный, аналитический и рекомендательный. Так, генеративный может быть полезен в составлении SQL-запросов, аналитический, в свою очередь, способен анализировать продажи, находить аномалии, а генеративный предлагает экономически и юридически оптимальное дальнейшее действие.

Помимо клиентов и контрагентов, предприниматель заключает договор с облачным провайдером, предоставляющим вычислительные ресурсы, программное обеспечение, хранение данных, доступ к ИИ и т.д. Облачный провайдер – это не одно конкретное физическое лицо, а целая организация, предоставляющая системы хранения данных, вычислительные ресурсы, средства информационной безопасности. Понятие облачного вычисления Gartner определяет следующим образом: «Это стиль вычислений, при котором масштабируемые и эластичные ИТ-возможности предоставляются как услуга внешним клиентам с использованием интернет-технологий» [2].

Представляется важным отметить, какое место занимает провайдер в облачной экосистеме. Выделяются три основных направления: 1) предоставление инфраструктуры, т.е. различные сети, дисковое пространство, виртуальные серверы; 2) предоставление платформы как услуги, т.е. уже готовая среда для вычислений; 3) программное обеспечение, т.е. клиент приобретает уже готовую программу.

Обобщая, работу облачного провайдера можно представить следующим образом: организация обращается к нему как к некоторой замене

недостающих ресурсов (серверы, дата-центры, соответствующие специалисты для их обслуживания), весь перечень недостающих ресурсов и услуг осуществляет провайдер и размещает готовые данные в облаке.

Казалось бы, предприниматель заключает с облачным провайдером договор возмездного оказания услуг (ст. 779 ГК РФ), а в случае ненадлежащего выполнения услуг по договору заказчик в соответствии с нормами ГК РФ и Закона РФ от 07.02.1992 № 2300-1 «О защите прав потребителей» имеет право требовать: безвозмездного устранения, соразмерного уменьшения стоимости услуг, повторного выполнения, возмещения своих расходов, отказа от договора. Однако в начале нашего исследования не просто так был затронут вопрос о роли ИИ в облачных экосистемах.

Современные тенденции таковы, что в облачные экосистемы активно внедряются системы управления базой данных (далее – СУБД), с которыми именно ИИ взаимодействует через API [3]. СУБД представляют собой комплексную систему, позволяющую анализировать, создавать, хранить информацию, находящуюся в базе данных. Три года назад Gartner опубликовал аналитический отчёт «2023 Magic Quadrant for Cloud DBMS (CDBMS)» [2], в котором был изучен рынок аналитических и транзакционных баз данных, функционирующих в облаках. Уже тогда прослеживалась тенденция расширения перечня функций СУБД (управление данными, история данных, безопасность данных) и пролеживался потенциал взаимодействия с уже имеющимися системами.

В настоящее время СУБД обретают новый виток развития, теперь они не просто подразделяются на модели, работающие с аналитикой и транзакцией отдельно, сегодня разрабатываются модели, совмещающие в себе эти функции одновременно. Системы обладают встроенным механизмом ИИ, способным оптимизировать сложные структурированные запросы, самостоятельно прогнозировать сбои [4].

Таким образом, получая доступ к базам данных, ИИ в процессе своей деятельности начинает апеллировать корпоративными данными организации, куда входит личная информация о сотрудниках, агентах, контрагентах. В такой ситуации возникают вопросы, связанные с передачей нематериальных благ, в частности информации о частной жизни, в пользование ИИ, а также гражданско-правовой ответственности в случае правонарушений. Сложность ситуации заключается в том, что информация, предоставляемая гражданином, попадает в структуру деятельности ИИ не напрямую, а через предпринимателя, облачного провайдера, систему управления базой данных.

Необходимо разобрать, какие гражданско-правовые отношения возникают между компанией и провайдерами ИИ. Основопологающим договором в данной ситуации выступает договор на облачное оказание услуг, который по своей природе является смешанным договором возмездного оказания услуг с элементами аренды или лицензионного соглашения. Он может включать в себя точную информацию о модели сервиса, соглашение об уровне сервиса и, что не менее важно, условия обработки персональных данных и метрики потребителя. В системе B2B (business-to-business – «бизнес для бизнеса») данный договор заключается между юридическим лицом или ИП с организацией, предоставляющей услуги облачного провайдера. Важно отметить, что на этом «цепочка договоров» не заканчивается. В конечном итоге получается следующая цепочка договоров: предприниматель – облачный провайдер – провайдер СУБД – разработчик ИИ.

Возникает вопрос об определении гражданско-правовой ответственности. В первую очередь стоит упомянуть концепцию, согласно которой ответственность за системные сбои и ошибки в работе системы должны нести сотрудники, круг которых определяется корпоративным договором организации. Вследствие чего необходимо обратиться ко второй концепции, согласно которой гражданско-правовую ответственность за правонарушения, совершённые системой на базе ИИ, несёт лицо, на тот момент курировавшее её деятельность. В пример можно привести дело *Ruby Lowe v. Cerner Corporation*, No. 20-2270 (4th Cir. 2022) [5]. Организацией Cerner было разработано программное обеспечение для медицинского оборудования. Врачом было внесено назначение на непрерывный контроль уровня кислорода в крови пациента, однако программа дала сбой, в результате чего пациент получил повреждение мозга. Истец предъявил требования разработчику программного обеспечения, аргументируя это тем, что система имела недочёты в проектировании. В конечном итоге апелляционный суд пришёл к выводу о множественности причин, заключив, что истец должен учитывать возможную ответственность врача или больницы. При этом немаловажен тот факт, что система обладает долей автономности, что усложнит процесс определения виновного лица. Стоит обратиться к европейскому опыту, а именно к Закону Европейского союза об ИИ (Artificial Intelligence Act, далее – AI Act) [6], где отмечается, что правовая ответственность за деятельность ИИ может быть наложена не на первоначального поставщика системы, а на дистрибьюторов или импортёров.

Для решения вопроса о гражданско-право-

вой ответственности следует учитывать квалификацию систем на базе ИИ, состоящую из 4 категорий:

1. Системы неприемлемого риска, которые представляют серьёзную угрозу безопасности и правам граждан. К ним относятся системы биометрической идентификации, манипулятивные системы, системы социального рейтинга.

2. Системы высокого риска, то есть программы, управляющие движением транспортных средств, использующиеся в прогностической деятельности в медицине. Они требуют строгого надзора и находятся под наибольшим контролем.

3. Системы ограниченного риска, к которым относятся чат-боты, приложения, использующие ИИ, виртуальные помощники и т.д. При их использовании тщательный надзор не требуется, однако разработчики должны убедиться, как ИИ взаимодействует с пользователями.

4. Системы минимального риска. Ими выступают программы, использующиеся для развлечения, как правило, в компьютерах для увеличения производительности в играх. Контроля они не требуют и не попадают под большинство нормативных требований, выдвигаемых Законом об ИИ.

Определение системы позволяет решать вопрос правового регулирования деятельности ИИ в облачных экосистемах. Как уже отмечалось ранее, система насчитывает множество сотрудников, так или иначе взаимодействующих с ИИ, поэтому определить конкретное лицо, виновное в правонарушении программы, вряд ли представляется возможным. Наиболее целесообразным видится наделить ИИ, использующийся в облачных экосистемах и СУБД, новым статусом программы повышенной опасности, что потребует её специальной регистрации. Таким образом, регистрируя программу, организация подтверждает, что осознаёт опасность и рискованность применения подобной системы, следовательно, по нашему мнению, в случае правового нарушения ответственность будут нести провайдеры, непосредственно работающие с ИИ, то есть провайдер облачной экосистемы и провайдер СУБД.

Необходимо дополнить п. 1 ст. 1079 ГК РФ, признав ИИ, задействованный в облачных экосистемах, источником повышенной опасности, так как его ошибки и неисправность могут привести к утечке большого количества личных данных. По нашему мнению, это необходимая мера в условиях стремительного развития и внедрения облачных сервисов в отечественные платформы [7], например, такие системы, как Yandex Cloud, VK Cloud, Cloud.ru, существуют уже более 7 лет. Системы управления базами данных, созданные Яндексом – YDB и ClickHouse, уже включают в

себя ИИ-ассистентов и MCP [4], из чего можно сделать вывод, что современные технологии ушли далеко вперёд.

Подводя итоги, считаем, что наиболее применимой моделью для правового регулирования деятельности ИИ в облачных экосистемах является риск-ориентированный подход. Суть его в том, что правила и строгость регулирования зависят от уровня риска, который несёт конкретная ИИ-система (минимальный риск, ограниченный, высокий, недопустимый), и для каждой устанавливается свой набор требований. Там, где риск минимален, правила мягче (акцент на прозрачности), а для систем высокого риска (например, в здравоохранении, управлении критической инфраструктурой, правосудии) вводятся более жёсткие нормы: обязательная оценка рисков, детальная документация, мониторинг, отчётность об инцидентах. В частности, Европейский AI Act – яркий пример риск-ориентированного подхода. Он как раз закладывает основу для регулирования ИИ, в том числе в облачных сценариях: требования к логированию, объяснимости решений, управлению рисками встраиваются в архитектуру облачных решений. Российский 243-ФЗ тоже движется в этом направлении: закон сфокусирован на больших фундаментальных моделях (от 1 млрд параметров) и сочетает стимулирующие меры с точечными требованиями безопасности и суверенитета.

Заключение

Проведённое исследование позволяет сделать следующие выводы. Во-первых, использование ИИ в облачных экосистемах порождает сложную цепочку договорных связей, в которой определение виновного лица затруднено ввиду автономности систем и множественности участников (облачный провайдер, провайдер СУБД, разработчик ИИ). Во-вторых, существующие концепции ответственности (ответственность сотрудников, ответственность курирующего лица) не в полной мере учитывают специфику облачных ИИ-систем. В-третьих, наиболее эффективным представляется риск-ориентированный подход, реализованный в AI Act и частично в российском 243-ФЗ. В-четвёртых, обоснована необходимость признания ИИ, задействованного в облачных экосистемах, источником повышенной опасности с внесением дополнений в п. 1 ст. 1079 ГК РФ, что позволит возложить ответственность на провайдеров, непосредственно работающих с ИИ.

Список литературы:

[1] Батура Т. В., Мурзин Ф. А., Семич Д. Ф. Облачные технологии: основные модели, приложения, концепции и тенденции развития // Программные продукты и системы. 2014. № 3

(107). С. 64–66.

[2] Gartner. 2023 Magic Quadrant for Cloud Database Management Systems. // Gartner. URL: <https://www.gartner.com> (дата обращения: 01.10.2026).

[3] Ловцов В. API от Ф до Я (теория и практика). // Хабр. URL: <https://habr.com/ru/articles/768752/> (дата обращения: 01.10.2026).

[4] Skillbox Media. SQL-запросы: основные команды для управления базами данных. // Skillbox Media. URL: <https://skillbox.ru/media/code/sqlzaprosy-osnovnye-komandy-dlya-upravleniya-bazami-dannykh/> (дата обращения: 01.10.2026).

[5] U.S. Court of Appeals for the Fourth Circuit. Ruby Lowe v. Cerner Corporation, No. 20-2270 (4th Cir. 2022). // United States Law :: U.S. Law :: Justia. URL: <https://law.justia.com/cases/federal/appellate-courts/ca4/20-2270/20-2270-2022-11-29.html> (дата обращения: 02.10.2026).

[6] SentinelOne. The EU AI Act, Demystified. // SentinelOne. URL: <https://www.sentinelone.com/lp/eu-ai-act-guide/> (дата обращения: 01.10.2026).

[7] Бондаренко П. ТОП-5 лучших облачных провайдеров России в 2026 году // Server Space. URL: <https://serverspace.ru/about/blog/top5-cloudproviders-2026/> (дата обращения: 01.10.2026).

[8] Федеральный закон N 243-ФЗ "О поддержке развития технологий искусственного интеллекта в Российской Федерации" // Собрание законодательства РФ. - 2026. - № 30. – Ст. 4089.

References:

[1] Batura T. V., Murzin F. A., Semich D. F. Cloud Technologies: Basic Models, Applications, Concepts, and Development Trends // Software Products and Systems. 2014. No. 3 (107). pp. 64–66.

[2] Gartner. 2023 Magic Quadrant for Cloud Database Management Systems. // Gartner. URL: <https://www.gartner.com> (accessed: 01.10.2026).

[3] Lovtsov V. APIs from A to Z (Theory and Practice). // Habr. URL: <https://habr.com/ru/articles/768752/> (accessed: 01.10.2026).

[4] Skillbox Media. SQL Queries: Basic Commands for Database Management. // Skillbox Media. URL: <https://skillbox.ru/media/code/sqlzaprosy-osnovnye-komandy-dlya-upravleniya-bazami-dannykh/> (accessed: 01.10.2026).

[5] U.S. Court of Appeals for the Fourth Circuit. Ruby Lowe v. Cerner Corporation, No. 20-2270 (4th Cir. 2022). // United States Law :: U.S. Law :: Justia. URL: <https://law.justia.com/cases/federal/appellate-courts/ca4/20-2270/20-2270-2022-11-29.html> (accessed: 02.10.2026).

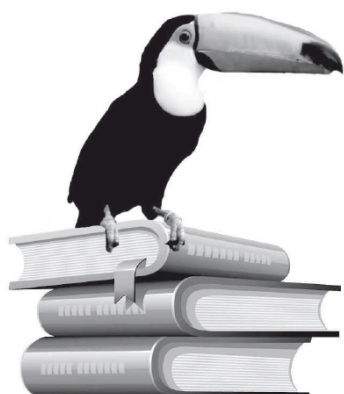
[6] SentinelOne. The EU AI Act, Demystified. //

SentinelOne. URL: <https://www.sentinelone.com/lp/eu-ai-act-guide/> (accessed: 01.10.2026).

[7] Bondarenko P. Top 5 Best Cloud Providers in Russia in 2026 // Server Space. URL: <https://serverspace.ru/about/blog/top5-cloudprovide>

rs-2026/ (accessed: 01.10.2026).

[8] Federal Law No. 243-FZ "On Supporting the Development of Artificial Intelligence Technologies in the Russian Federation" // Collected Legislation of the Russian Federation. – 2026. – No. 30. – Art. 4089.



ЮРКОМПАНИ

www.law-books.ru

Юридическое издательство
«ЮРКОМПАНИ»

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

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.