

Вопросы права В ЦИФРОВУЮ ЭПОХУ

1/2026



Учредитель

Национальный
исследовательский
университет
«Высшая школа
экономики»

ISSN 2713-2749

Журнал

зарегистрирован
Федеральной
службой по надзору
в сфере связи,
информационных
технологий
и массовых
коммуникаций
и включен в реестр
зарегистрированных
средств массовой
информации,
серия Эл No ФС77-
83367 от 03.06.2022

Адрес фактический:
109028, Москва,
Б. Трехсвятит-
ельский пер., д. 3,
оф. 113
тел. +7 495 53-00-00
*22654,
e-mail: lida@hse.ru

Художественное
оформление:
Павлов А.М.
Верстка:
Пузанова Н.Е

© Национальный
исследовательский
университет
«Высшая школа
экономики», 2026

ISSUED QUARTERLY

VOLUME 6

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРАВО

А.С. Ворожечин

Границы авторского права в эпоху искусственного
интеллекта: переосмысление концепции свободного
использования. 4

П.К. Пакшин

Замена критерия творчества критерием инвестиций
для результатов, созданных искусственным интеллектом. . . . 32

С.С. Гулямов, И.Р. Рустамбеков

Этическое регулирование применения искусственного
интеллекта в университетском образовании 49

ЦИФРОВАЯ ЭПОХА: ТРУДОВОЕ ПРАВО

Ю.Д. Жукова, А.С. Подмаркова

Социально-трудовые права в условиях платформенной
занятости: на примере пассажирских перевозок
легковым такси 71

ИТ. Индустрия. Право: ТЕЛЕМЕДИЦИНА

А.А. Карцхия

Перспективы цифрового здравоохранения 96

ЭЛЕКТРОННОЕ ГОСУДАРСТВО И КИБЕРБЕЗОПАСНОСТЬ

К.Р. Кирушин, Д.И. Сафин

Правовые особенности практики внедрения IoT-систем
в организациях (учреждениях) Республики Татарстан 121

Е.А. Русскевич

Уголовно-правовой комплаенс тестирования
информационных систем на киберустойчивость. 141

Legal Issues in the **DIGITAL AGE**

EDITORIAL BOARD

Главный редактор

И.Ю. Богдановская

НИУ ВШЭ, РФ

Редакционная коллегия

А.И. Абдуллин

Казанской (Приволжский) федеральный университет, РФ

Дж. Айджани

Туринский университет, Италия

В.Э. Батлер

Пенсильванский университет, США

Н.А. Богданова

МГУ им М. В. Ломоносова, РФ

В.А. Виноградов

НИУ ВШЭ, РФ

А.В. Габов

ИГП РАН, РФ

Г.А. Гаджиев

НИУ ВШЭ, Санкт-Петербург, РФ

Ч. Го

Китайский университет политических наук и права, Китай

Ю.В. Грачева

МГЮА им. О. Е. Кутафина, РФ

Д. Дюмортье

Католический университет Левена, Бельгия

И.А. Емелькина

РАНХИГС при Президенте РФ

Н.Ю. Ерпылева

НИУ ВШЭ, РФ

А.А. Иванов

НИУ ВШЭ, РФ

В.Б.Исаков

НИУ ВШЭ, РФ

С. Кандерия

Глобальный институт им. О.П. Джиндала, Индия

С.Дж. Корнелиус

Университет Претории, Южная Африка

А.А. Ларичев

НИУ ВШЭ, РФ

Г.И. Муромцев

Российский университет дружбы народов, РФ

А.В. Наумов

НИИ Университета прокуратуры, РФ

Н.А. Поветкина

НИУ ВШЭ, РФ

А.И. Рарог

МГЮА им. О.Е. Кутафина, РФ

А.Х. Саидов

Академия наук Узбекистана

В.А. Сивицкий

Конституционный суд Российской Федерации, РФ

Е.А. Суханов

МГУ им. М.В. Ломоносова, РФ

Г.Г. Шинкарецкая

ИГП РАН, РФ

Т. Эндикотт

Оксфордский университет, Великобритания

Консультативный совет

Н.И. Капырина

Московский государственный институт международных отношений (МГИМО),
Российская Федерация

Legal Issues in the **DIGITAL AGE**

ISSUED QUARTERLY

Журнал открытого доступа «Вопросы права в цифровую эпоху» — это академическое ежеквартальное электронное издание, предлагающее всесторонний анализ права в цифровом мире. Его основная цель — рассмотрение правовых вопросов, связанных с постоянно развивающимися цифровыми технологиями, которые создают инфраструктуру общества, выводя страны на более высокий уровень благодаря эффективному производству и цифровым данным.

В настоящее время, в связи с развитием информационного общества и формированием цифровой экономики, право претерпевает ряд изменений: формируются новые институты и отрасли. Возникают также теоретические проблемы, касающиеся перспектив права как социального регулятора в контексте развития информационно-коммуникационных технологий. Происходящие процессы типичны для стран с различными правовыми традициями, но их проявление в национальных юрисдикциях различно.

Целью журнала «Вопросы права в цифровую эпоху» является сравнение этих процессов, что отличает его от других периодических изданий, в основном посвященных проблемам права информационных технологий и информационной безопасности. **Темы** публикаций журнала отражают особенности не только права России, но и других стран в контексте развития систем информационных технологий в новых социальных условиях.

Журнал «Вопросы права в цифровую эпоху» призван предоставить платформу для развития новаторского и аналитического мышления студентов, ученых и юристов-практиков. Журнал поощряет обсуждение междисциплинарных тем, включая взаимодействие права, технологий.

«Вопросы права в цифровую эпоху» это высокопрофессиональный журнал, статьи проходят двойное слепое рецензирование.

Авторам предлагается присылать статьи, отражающие передовые исследования в области регулирования цифровой среды. Редакторы поощряют теоретические и сравнительные подходы, а также рассмотрение правовых аспектов с точки зрения разных стран. Публикации в журнале бесплатны.

Искусственный интеллект и право

Научная статья

УДК: 347.3

JEL: K15

DOI:10.17323/2713-2749.2026.1.4.31

Границы авторского права в эпоху искусственного интеллекта: переосмысление концепции свободного использования



Арина Сергеевна Ворожевич

Московский государственный университет им. М.В. Ломоносова, Россия
119991, Москва, Ленинские горы, 1, стр. 13,

arinavorozhevich@yandex.ru, <https://orcid.org/0000-0002-9908-2143>



Аннотация

В статье рассматривается проблема правовой квалификации использования объектов авторских прав при обучении искусственного интеллекта. Автор обосновывает необходимость внесения изменений в Гражданский кодекс путем закрепления специального случая свободного использования произведений для обучения нейросетей, включая сбор данных. На основе анализа зарубежного опыта и судебной практики автор приходит к выводу, что использование произведений при интеллектуальном анализе текстов и данных в цифровой форме, в том числе в целях обучения нейросетей должно признаваться законным при условии, что форма произведений не воспринимается органами чувств человека. Предлагается распространить данное исключение на любые произведения, находящиеся в открытом доступе, включая материалы из Интернета и закрытых баз данных, к которым разработчики получили легальный доступ. Отдельное внимание уделяется вопросу использования для обучения ИИ произведений из теневого библиотек. В работе обосновывается нецелесообразность введения платы за использование произведений при обучении ИИ, поскольку это может привести к снижению инвестиций в развитие технологий

и усложнению процесса обучения нейросетей. При этом разграничиваются допустимые и недопустимые случаи использования: внутреннее запоминание материалов не считается нарушением, однако генерация контента с воспроизведением существенных частей охраняемых произведений квалифицируется как нарушение исключительных прав. Обосновано, что генерация произведений в стиле конкретного автора при обучении нейросети на основе его работ может также означать нарушение исключительных прав. Особое внимание уделяется вопросам ответственности. Автор предлагает дифференцированный подход, при котором ответственность может нести как разработчик нейросети, так и пользователь в зависимости от конкретных обстоятельств дела. Исследование подчеркивает, что предлагаемый подход позволит обеспечить баланс между защитой прав создателей контента и необходимостью развития технологий ИИ, которые имеют важное значение для решения глобальных задач в различных сферах общественной жизни.



Ключевые слова

авторские права; правообладатель; искусственный интеллект; свободное использование; исключительные права; нарушение.

Для цитирования: Ворожевич А.С. Границы авторского права в эпоху искусственного интеллекта: переосмысление концепции свободного использования // Вопросы права в цифровую эпоху. 2026. Том 7. № 1. С. 4–31. DOI:10.17323/2713-2749.2026.1.4.31

Введение

Чтобы нейросеть могла работать с запросами пользователей, она должна пройти глубокое обучение, в ходе которого происходит анализ массивов информации. Нейросеть учится выявлять закономерности, устанавливать связи между различными элементами информации, понимать, как текстовые описания соотносятся с визуальным контентом. Это похоже на процесс обучения человека, когда мы анализируем опыт, находим в нем закономерности и учимся применять их.

В массивах данных, используемых для обучения, могут содержаться материалы, защищенные авторским правом. Это поднимает важные вопросы о правовых аспектах использования таких данных. Нужно ли разработчикам систем искусственного интеллекта (ИИ) получать разрешение правообладателей на использование их произведений в процессе обучения алгоритмов? Является ли использование таких произведений без согласия правообладателей нарушением их исключительных прав? Эти вопросы требуют рассмотрения с точки зрения как технологического процесса, так и правовых норм.

Методологическую основу исследования составляют общенаучные методы познания: анализ, синтез, индукция, дедукция, научная абстракция, классификация, аналогия; диалектический, формально-логические методы.

Исследование базируется на принципах системности и всесторонности рассмотрения основанных проблем, раскрытия разнонаправленных частных и общественных интересов. Существенное внимание работе уделено сравнительно-правовой методологии.

1. Как происходит обучение нейросети?

С технической точки зрения процесс обучения включает несколько этапов.

Сбор и предварительная обработка данных. На этом этапе тексты и изображения собираются, очищаются и разбиваются на токены. В результате разработчики получают обычные копии данных на дисках и в оперативной памяти, а также производные последовательности токенов¹. Основным механизмом сбора данных является скрапинг — автоматизированная технология извлечения данных из веб-ресурсов, их последующей обработки и хранения. Второй распространенный механизм — извлечение данных при помощи интерфейсов программирования приложений (API)².

Полученные данные подвергаются фильтрации. Разработчики применяют автоматизированные инструменты очистки массива от открытого контента, материалов с водяными знаками и некачественных образцов. Параллельно осуществляется поиск эстетически ценных и высокоуровневых подмножеств данных, которые становятся приоритетным материалом для обучения ИИ.

Важной частью обработки является дедупликация — технология сжатия данных путем устранения повторяющихся элементов. Ее применение минимизирует риск механического запоминания нейросетью исходной информации³. В процессе создания датасетов специалисты нередко интегрируют несколько исходных наборов в единый массив,

¹ Frosio G. Copyright in Formaldehyde: How GEMA v Open AI Freezes Doctrine and Chills AI — Part 1. Available at: URL: <https://legalblogs.wolterskluwer.com/copyright-blog/copyright-in-formaldehyde-how-gema-v-openai-freezes-doctrine-and-chills-ai-part-1/> (дата обращения: 07.06.2025)

² API — слой программного обеспечения, позволяющий программам взаимодействовать друг с другом.

³ Copyright and Artificial Intelligence. Part 3: Generative AI Training pre-publication version: A Report of the register of Copyrights, may 2025. Available at: URL: <https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-3-Generative-AI-Training-Report-Pre-Publication-Version.pdf>

обладающий необходимыми характеристиками и широким спектром данных. Например, создатели датасета Pile, использованного для обучения нескольких языковых моделей, отобрали материал из 22 подмножеств. В их число вошел архив PubMed Central с почти 5 миллионами биомедицинских статей (для решения прикладных задач в медицине) и набор Books3 с полными текстами книг (для формирования связного повествования). Разработчики используют «восходящую выборку», придавая большее значение определенным подмножествам. Качество моделей напрямую зависит от качества обучающих данных⁴.

Процесс токенизации означает разбивку исходных данных (например, текста) на мелкие единицы (токены), с которыми работает модель машинного обучения. Цель операции — преобразовать неструктурированную информацию в числовой формат для интерпретации моделью⁵.

а) Цикл обучения

На данном этапе генеративная модель анализирует данные, выявляет закономерности и настраивает параметры на генерацию нового контента, похожего на обучающие примеры. Модель работает не с текстами изображениями как таковыми, а с последовательностью токенов, которые несут смысловую и контекстуальную информацию.

Система проходит по набору данных, выполняя прямые и обратные проходы и обновляя миллиарды числовых весов. Числовые веса — ключевой элемент нейросети, который определяет ее способности к обучению и работе с данными. Они не хранят информацию напрямую, а являются математическим описанием того, как модель научилась распознавать закономерности в данных. Когда обучение завершено, исходный корпус теоретически можно удалить; остается только вектор параметров.

б) Модель как артефакт

Сохраненная модель — огромная матрица весов. Ее нельзя «открыть» и прочитать тексты, увидеть изображения. Это сжатое статистическое представление паттернов в данных, а не читаемый человеком текст.

в) Генерация (вывод) и поиск

Пользователь направляет нейросети запрос (промпт) на генерацию изображения или текста. Во время выполнения пользовательский за-

⁴ Там же.

⁵ Почему токенизация — костыль? Передовые подходы для больших языковых моделей следующего поколения // Хабр. 2025. Available at: URL: <https://habr.com/ru/articles/873120/?ysclid=mk281q4saq556343593> (дата обращения: 07.06.2025)

прос токенизируется. Модель вычисляет распределение вероятностей для следующего токена и генерирует последовательность.

Аналитики спорят, сохраняются ли в моделях обучающие данные, которые впоследствии распространяются вместе с ними. Разработчики ИИ настаивают, что в самой модели отсутствуют копии обучающих материалов (текстов, изображений). Веса модели — это лишь «большие строки чисел», отражающие статистические взаимосвязи между обучающими токенами⁶.

Но факты генерации ИИ результатов, практически идентичных охраняемым авторским правом произведениям, ставят под сомнение такие утверждения. Подобная ситуация сложилась в деле *GEMA v. OPEN AI* (см. ниже). На основании примеров специалисты приходят к выводу: нейросеть способна сохранять фрагменты творческих работ, на которых проходила обучение. Ответ на данный вопрос во многом зависит от способа обучения нейросети и характера изучаемых паттернов. Статистические паттерны, которые осваивает модель, могут варьироваться от максимально абстрактных до предельно конкретных.

Показательны примеры. В первом случае нейросеть обучается распознавать различных животных и генерировать их изображения по запросу пользователя. Соответствующие паттерны (относящиеся к внешнему виду животных) формируются на основе анализа множества фотографий, видео и рисунков. Нейросети нет необходимости запоминать и воспроизводить изображения (охраняемые произведения). Такую ситуацию следует признать общим правилом, из которого, однако, возможны исключения.

Во втором случае нейросеть запоминает внешний вид определенного персонажа (связывая его имя с изображением) или текст песни. В этой ситуации выученный паттерн фактически являет собой сохраненные обучающие данные, поскольку для обучения использовался единственный уникальный пример.

Как отмечают специалисты Бюро авторских прав США, на степень запоминания данных нейросетью влияет множество факторов, включая количество параметров модели, наличие дубликатов обучающих данных, многократное обучение на одном и том же примере, уникальность примера, момент появления примера в процессе обучения⁷.

Разработчики нейросетей нередко сталкиваются с явлением переобучения модели. Она в таком случае не может выявить общих законо-

⁶ Copyright and Artificial Intelligence. Part 3: Generative AI Training pre-publication version: A Report of the register of Copyrights. May 2025. Available at: URL: <https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-3-Generative-AI-Training-Report-Pre-Publication-Version.pdf> (дата обращения: 07.06.2025)

⁷ Ibid.

мерностей в обучающих данных, что приводит к ошибочным предсказаниям на новых или неизвестных данных⁸. Вместо обобщения модель только запоминает обучающий набор. Это часто происходит из-за ограниченного объема обучающих данных или наличия «шумных» данных, запоминания неважных деталей. Получается система, механически воспроизводящая обучающий набор, теряя практическую ценность.

Современные большие языковые модели интегрировали технологию Retrieval-Augmented Generation (RAG). Принцип ее работы заключается в обработке пользовательского запроса с последующим извлечением релевантной информации из баз данных и ее дополнением перед финальной генерацией ответа. Технология объединяет два ключевых процесса: извлечение и генерацию. При получении запроса система осуществляет поиск релевантных материалов в хранилище данных, найденные тексты передаются нейросети. Финальный ответ формируется на основании как содержания источников, так и специфики исходного запроса, обеспечивая точность и осмысленность результата⁹.

2. Правовая квалификация

Обучение ИИ предполагает копирование данных в оперативную память компьютера, их последующую обработку и загрузку нейросети. В таком случае необходимо говорить о воспроизведении произведений как одном из способов их использования.

Как было отмечено в Согласованных заявлениях в отношении договора ВОИС по авторскому праву, право на воспроизведение, как оно определено в ст. 9 Бернской конвенции об охране литературных и художественных произведений¹⁰, и допускаемые этой статьей исключения полностью применяются в цифровой среде, в частности, в отношении использования произведений в цифровой форме¹¹. Хранение произведения в цифровой форме является воспроизведением ст. 9 Бернской конвенции. В соответствии с п. 2 ст. 1270 Гражданского кодекса Российской Федерации (далее —

⁸ Рыжков А. Переобучение моделей // Хабр. 2024. Available at: URL: <https://habr.com/ru/companies/skillfactory/articles/864234/?ysclid=mk2a1hfzbw794277095> (дата обращения: 07.06.2025)

⁹ Лактионов Д. RAG и большие языковые модели: что это и зачем нужно бизнесу. Available at: URL: <https://companies.rbc.ru/news/OcbKEJly0f/rag-i-bolshie-yazykovyie-modeli-cto-eto-i-zachem-nuzhno-biznesu/?ysclid=mjyfvikn8i260495613> (дата обращения: 07.06.2025)

¹⁰ Бюллетень международных договоров. 2003. № 9.

¹¹ Available at: URL: <https://new.fips.ru/documents/international-documents/dogovory/soglasovannye-zayavleniya-v-otnoshenii-dogovora-vois-po-avtor-skomu-pravu.php?ysclid=mk2ash5xgt388580726> (дата обращения: 07.06.2025)

ГК) под воспроизведением произведения понимается в том числе его запись на электронный носитель, запись в память ЭВМ.

Воспроизведение произведений, их частей происходит и при применении технологии RAG. Возможны следующие варианты. В первом случае разработчик ИИ загружает материал в собственную базу данных, откуда генеративная система впоследствии извлекает релевантную информацию и передает ее модели вместе с запросом пользователя. Вторым способ предполагает извлечение материала из внешних источников — поисковых систем или веб-сайтов.

В генерируемом нейросетью контенте обычно не воспроизводятся произведения и части произведений, на которых обучался ИИ. При обучении модель «запоминает» лишь общие закономерности, паттерны. Между тем возможны сбои. Иногда нейросеть запоминает примеры данных, на которых обучалась. В таком случае на стадии генерации контента также происходит воспроизведение произведений, его частей либо переработка (при создании производного произведения). Может иметь место также доведение до всеобщего сведения.

Воспроизведение, равно как и иные способы использования чужих произведений требует получения согласия правообладателей, если оно не происходит за содержательными и временными границами исключительных права. В некоторых случаях разработчики ИИ опираются на согласие правообладателей. Например, в декабре 2023 г. компания OpenAI объявила о своем партнерстве с Axel Springer. В соответствии с заключенным сторонами соглашением OpenAI может использовать произведения, права на которые принадлежат Axel Springer, при обучении ИИ [Sag M., Yu P., 2025: 1215].

Правомерно использование для обучения ИИ произведений, вошедших во всеобщее достояние (в отношении которых истек срок правовой охраны). Между тем такие случаи не могут быть общим правилом для обучения ИИ. Для плодотворной работы нейросетей требуется обработка колоссального массива данных—тысяч произведений. При этом технически невозможно найти правообладателей всех используемых материалов; получить согласие каждого из них.

Обучение нейросети на основе только перешедших в общественное достояние произведений существенно снизит потенциал нейросетевых моделей. Для полноценной работы системы необходимо изучать современные культурные тенденции, новейшие достижения в различных областях; обрабатывать свежие данные; выявлять текущие паттерны. Использование только устаревших материалов не позволит модели следить за развитием языка, улавливать новые смысловые связи, генерировать актуальные ответы.

Как отметило Бюро авторских прав США на основе исследования мнений специалистов, требование к ИИ—компаниям лицензировать произведения, входящие в обучающие данные, может затормозить разви-

тие важной технологии, усилить позиции компаний, способных приобрести или уже владеют достаточным объемом данных, и нанести ущерб конкурентоспособности страны¹².

Очевидно, для обучения нейросетей должны быть предусмотрены изъятия из исключительных прав, случаи свободного использования. Этого требуют прежде всего общественные интересы. Нейросети способны повысить действенность производственных и бизнес-процессов, автоматизировать решение рутинных задач и улучшить прогнозирование в различных отраслях. ИИ может применяться в творческой сфере (литературе, живописи и т.п.), в сфере здравоохранения и фармацевтики (при диагностировании заболеваний и разработке новых препаратов). Право должно содействовать развитию подобных технологий, а не блокировать его. Однако такое исключение не должно оправдывать любых действий разработчиков и пользователей нейросетей, связанных с использованием чужих произведений.

3. Подходы различных правопорядков

3.1. Российский подход

ГК установил перечень случаев свободного использования чужих произведений, которые не охвачены исключительным правом. Но ни один из них не относится к обучению ИИ. Существует значительный риск, что при споре такое использование будет признано нарушением исключительного права. De lege lata в некоторых случаях правомерность обучения нейросети на основе чужих произведений можно обосновать следующим образом. В соответствии с п. 2 ст. 1270 ГК без согласия правообладателя допускается краткосрочная запись произведения, которая носит случайный или временный характер.

Во многих случаях запись данных, собранных для обучения ИИ, имеет временный характер. На основе массива данных нейросеть выявляет общие закономерности, принципы, признаки, относящиеся к тем или иным объектам. Обученная модель содержит преимущественно высоко абстрактные представления исходных данных (шаблоны, закономерности, связи). Нейросети работают не с буквами или словами, а с числовыми значениями, присвоенными словам в рамках процесса токенизации. База изначальных данных после обучения может быть удалена [Lukas A.J., 2023: 5].

В таком случае сбор и загрузка разработчиком данных нейросети могут быть подведены под п. 2 ст. 1270 при условии, что после обучения ИИ изначальный набор отобранных данных будет удален. Здесь, однако, встают новые вопросы. В соответствии с рассматриваемой нормой краткосрочная запись произведения правомерна, если она составляет

¹² Copyright and Artificial Intelligence.

существенную часть технологического процесса, имеющего единственной целью правомерное использование произведение. Проблема, однако, в том, что обучение ИИ не названо в ГК в качестве правомерного использования. Оно не определено как случай свободного использования. Поэтому как будто в рассматриваемой ситуации отсутствуют все необходимые условия для применения п. 2 ст. 1370 ГК. Между тем к решению данного вопроса допустимо подойти с иной позиции. Если исходить из того, что обученная нейросеть при генерации выходных данных использует только абстрактные данные, информацию об общих закономерностях, то есть основания утверждать, что целью временного воспроизведения является использование не формы (выражения) произведений, а идей, информации относительно массива произведений. Использование подобных данных не охватывается исключительными правами. В таком случае временная запись исходных данных (при условии, что они были удалены после обучения) осуществляется в правомерных целях. Значит, к ней допустимо применить нормы п. 2 ст. 1270.

Отдельно разработчики нейросетей не всегда удаляют наборы данных, на которых обучался ИИ. Крупные разработчики часто полностью сохраняют обучающие наборы данных для использования в будущих проектах. Это подтверждает правоприменительная практика. Тогда о временном характере воспроизведения говорить в принципе не приходится. Не применимо данное исключение и к тем случаям, когда ИИ на основе промпта создает дословные или существенно схожие копии обучающих материалов без их внешнего предоставления пользователем. Это означает, что соответствующие данные в той или иной форме присутствуют в ее весовых коэффициентах.

Ссылка на временный характер воспроизведения в любом случае не снимает множества других вопросов об условиях правомерности обучения нейросети на основе чужих произведений. Поэтому следует констатировать необходимость установления в российском праве отдельного изъятия из исключительных прав для целей обучения нейросетей и условий, границ его применения.

Многие зарубежные правовые системы уже отреагировали на вызовы, связанные с развитием ИИ.

3.2. Опыт ЕС

На уровне Евросоюза два значимых для развития ИИ изъятия закреплены в ст. 3 и 4 Директивы Европейского парламента и Совета ЕС от 17.04. 2019 № 2019/790 «Об авторском праве и смежных правах в условиях единого цифрового рынка»¹³ (далее — Директива). Статьи 3 и 4 уста-

¹³ Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market.

навливают условия правомерности интеллектуального анализа текстов и данных, который определен в Директиве как любая автоматизированная аналитическая технология, направленная на анализ текста и данных в цифровой форме в целях получения информации, которая включает, помимо прочего, закономерности, тенденции и корреляции.

Ст. 3 Директивы допускает воспроизведение и извлечение, осуществляемые исследовательскими организациями и организациями культурного наследия в научных целях для интеллектуального анализа текста и иных данных, к которым они получают правомерный доступ в рамках своей исследовательской деятельности. Действие этого исключения распространяется лишь на исследовательские организации (некоммерческие структуры, чья главная задача — исследования, в том числе образовательные учреждения) и организации культурного наследия (публичные библиотеки, музеи, архивы).

Для применения исключения необходимо соблюдение двух условий: деятельность должна осуществляться только в научных целях, а доступ к материалам быть законным (материалы размещены в открытых источниках либо организация располагает подписками и лицензиями). Подписки и лицензии не обязательно должны предусматривать право на интеллектуальный анализ данных. Напротив, предусмотренные в ст. 3 Директивы возможности использования произведений нельзя отменить или ограничить в договорном порядке. Рассматриваемая статья имеет императивный характер.

Ст. 4 Директивы допускает действия, связанные с воспроизведением и извлечением правомерно доступных произведений и других объектов для анализа текстов и данных. Рассматриваемым изъятием могут воспользоваться любые субъекты (а не только исследовательские организации). Оно касается лишь тех данных, которые находятся в открытом доступе и в отношении которых правообладатели не установили ограничения (с помощью машиночитаемых средств) на их использование при обучении ИИ.

По мнению большинства европейских ученых, установленные в ст. 3 и 4 Директивы изъятия применимы к обучению ИИ. Последнее рассматривается в качестве частного случая интеллектуального анализа данных и текстов [Hellwig F., 2019: 40]; [Senftleben M., 2022: 1480]; [Dermawan A., 2023: 45–48].

Многие европейские исследователи полагают, что *de lege ferenda* разработчики ИИ должны выплачивать правообладателям произведений вознаграждение за использование произведений¹⁴. По выражению М. Зенфтлебена, авторы должны получить компенсацию «за парази-

¹⁴ Tylec G., Kwiecień S., Sarowski Ł et. al. Is it Possible to License Works Used in the Learning Process of Artificial Intelligence Algorithms? Available at: URL: <https://ssrn.com/abstract=4729495> (дата обращения: 07.06.2025)

тическую узурпацию рынка ИИ». Генеративные ИИ лишь имитируют литературные и художественные творения человека после того, как получили возможность вывести образцы для собственного творчества [Senftleben M., 2023: 1535–1560].

Ученые предлагают схему расчета и сбора вознаграждения. Разработчики ИИ вправе использовать произведения для обучения ИИ без лицензии правообладателей. При этом они обязаны выплачивать за это сбор в пользу всего сообщества авторов организациям коллективного управления авторскими и смежными правами или иным подобным структурам. Размер сбора должен зависеть от доходов разработчиков ИИ и может быть уменьшен на роялти, выплачиваемые разработчиками по обычным договорам с правообладателями. Правообладатели будут получать проценты от сбора. Порядок распределения сбора может быть определен организацией коллективного управления правами. Учитываться могут в том числе исследования, указывающие, какие произведения чаще всего используются ИИ.

В июле 2025 года по запросу Комитета по правовым вопросам Европейского парламента Н. Лукки подготовила исследование «Генеративный искусственный интеллект и авторское право: обучение, создание и регулирование», в котором указала на существенные различия между интеллектуальным анализом текстов и данных и обучением ИИ. По ее мнению, исключения для интеллектуального анализа текстов и данных не подходят к масштабному использованию данных в генеративном ИИ. Кроме того, Н. Лукки обратила внимания на отсутствие единых стандартов установления правообладателями запрета на использование их контента, непрозрачность процессов обучения моделей. Она предложила, в частности, следующие решения: создание специального органа надзора за использованием контента в ИИ, разработку стандартов отчетности разработчиков, установление прозрачных механизмов расчета компенсации. Последнее предполагает формирование системы коллективного управления правами для мелких правообладателей, создание централизованного фонда вознаграждений, подготовку методик расчета выплат на основе влияния контента на работу модели, популярности используемых материалов, объема использования данных, прибыли разработчиков ИИ [Lucchi N., 2025: 12–14, 29–35, 59].

3.3. Японский подход

Статья 30–4 Закона об авторском праве Японии¹⁵ разрешает использовать произведение любым способом и в той мере, которая считается необходимой в следующих случаях:

¹⁵ Copyright Act (Act No. 48 of May 6, 1970, as amended up to January 1, 2022). Available at: URL: <https://www.wipo.int/wipolex/en/legislation/details/21342> (дата обращения: 07.06.2025)

1) если это делается в целях тестирования, разработки или внедрения в практическое использование технологии, связанной с записью звуков или визуальных эффектов произведения или иной подобной эксплуатацией;

2) если это делается для использования при анализе данных (имеется в виду извлечение, сравнение, классификация или другой статистический анализ составляющего языка, звуков, изображений или других элементарных данных из большого количества произведений или большого объема других таких данных);

3) если оно эксплуатируется в ходе компьютерной обработки данных или эксплуатируется таким образом, что то, что форма произведения не воспринимается человеческими чувствами;

4) в любом другом случае, когда цель пользователя является иной, нежели получение наслаждения от мыслей или чувств, выраженных в произведении.

Установлено, что такие действия не должны необоснованно ущемлять интересы правообладателей произведений с учетом целей произведения и обстоятельств его использования.

В ст. 47-5 Закона допускается свободное незначительное использование произведений, связанное с компьютерной обработкой данных и выявлением результатов. Работая в tandem, эти два положения дали Японии, вероятно, самое широкое в мире исключение для обучения нейросетей.

Между тем ныне в Японии обсуждаются возможные ужесточения регулирования в данной сфере. В мае 2024 года японское Ведомство авторских прав опубликовало «Общее понимание ИИ и авторского права в Японии». В документе отмечается, что компании могут быть привлечены к ответственности, если они сознательно собирают данные для обучения из источников, нарушающих авторские права. Подчеркивается, что материалы, сгенерированные ИИ в стиле существующего произведения, не нарушают авторских прав. Однако если небольшая группа работ автора содержит не только общий стиль (т.е. идею), но и одинаковые творческие элементы, то намеренное воспроизведение такой группы для дополнительного обучения с целью генерации материалов, включающих эти творческие элементы, считается нарушением¹⁶.

3.4. Подход США

Статья 107 раздела 17 «Авторское право» Кодекса США¹⁷ установила четыре критерия (доктрина fair use) для определения допустимости ис-

¹⁶ Available at: URL: https://www.bunka.go.jp/english/policy/copyright/pdf/94055801_01.pdf (дата обращения: 07.06.2025)

¹⁷ United States Code, Title 17 — Copyrights, United States of America (17 U.S.C., amended up to Public Law No. 117-263). Available at: URL: <https://www.wipo.int/wipolex/en/legislation/details/22356> (дата обращения: 07.06.2025)

пользования объекта авторского права без согласия правообладателя: 1) цель использования; 2) характер произведения (уровень творчества); 3) объем и существенность заимствования из охраняемого произведения; 4) воздействие, оказываемое такое использованием на потенциальный рынок или ценность охраняемого произведения [Калятин В.О., 2015: 40–47].

Первый критерий на уровне судебной практики дополнен доктриной расширяющего полезность (трансформативного) использования. Такое использование характеризуется несколькими признаками. Во-первых, оно имеет творческий преобразовательный характер. Во-вторых, предполагает, с одной стороны, создание и использование новых объектов авторских прав, в том числе программных продуктов, с другой — извлечение дополнительной «полезности» (как в прикладном, так и познавательном, информационном смысле) из используемых чужих объектов авторского права¹⁸.

Многие американские ученые исходят из того, что использование произведений для обучения ИИ должно определяться как добросовестное использование. Его можно отнести к трансформационному, расширяющему полезность использованию [Torrance A., Tomlinson B., 2023: 250–253].

Как отмечают М. Сэг и П. Ю, интеллектуальный анализ произведений в целях получения метаданных, не охраняемых авторским правом абстракций, является трансформационным использованием. Тогда он отвечает первому критерию добросовестного использования [Sag M., Yu P., 2025: 1175]. Однозначно соответствует такое использование и третьему критерию. Произведения для обучения ИИ нередко копируют полностью, но впоследствии из них извлекают главным образом незащищенные элементы (факты, идеи и т. п.). Отвечает рассматриваемое использование, по мнению авторов, и четвертому критерию: обучение ИИ не оказывает ощутимого влияния на потенциальный рынок или ценность защищенной авторским правом работы.

Схожую позицию занимают М. Лэмли и Б. Кейси. Они полагают, что воспроизведение объектов авторских прав в большинстве случаев должно признаваться добросовестным, если при этом отсутствует цель получить доступ к защищенной форме произведения. Разработчики ИИ заинтересованы не в выражении (форме) объекта авторских прав, а в идеях, которые передаются посредством данного выражения [Lemley M.A., Casey B., 2021: 158].

По мнению Э. Ли, «применение более крупных и разнообразных наборов данных—или метод масштабирования привело к лучшим резуль-

¹⁸ Данная концепция применена, в частности, в следующем споре: *Authors Guild v. Google, Inc.*, 804 F.3d 202, 218 (2d Cir. 2015); *Authors Guild, Inc. v. HathiTrust*, 755 F.3d 87, 97 (2d Cir. 2014).

татам в разработке работающих моделей ИИ и продвинуло состояние технологий. Эта история показывает, что использование разработчиком ИИ произведений, защищенных авторским правом, для обучения моделей ИИ с целью исследования, разработки, обучения и улучшения модели ИИ может служить законной цели добросовестного использования: а именно, созданию новой технологии с общественной пользой» [Lee E., 2025: 223].

В докладе Бюро авторских прав США было отмечено, что обучение генеративных ИИ-моделей на больших наборах данных преобразует исходный материал в статистические модели, способные генерировать новый контент. При этом цели создания авторских произведений (развлечение и образование) могут не совпадать с функциями ИИ-моделей. В таком случае, как констатирует Бюро, использование чужих произведений при обучении ИИ носит, как правило, трансформативный характер.

Между тем степень преобразования (трансформативности) может существенно различаться в зависимости от обстоятельств использования. Максимально преобразующим следует признать применение модели в научных исследованиях или закрытых системах с ограниченными функциями, не связанными с заменой оригинальных произведений. Пример — разработка языковой модели для изучения иностранных языков через общение и корректировку ошибок пользователей.

Противоположный полюс занимает использование, нацеленное на создание контента, практически идентичного охраняемым авторским правом материалам: так, модель изображений, обученная на кадрах мультсериала, может генерировать новых персонажей в том же стиле.

Большинство случаев располагается между этими крайностями. Модель может использовать защищенные авторским правом произведения, не создавая при этом существенно схожего контента. Однако если обучение направлено на производство материала для той же аудитории, такое применение остается лишь умеренно преобразующим.

Насчет четвертого критерия Бюро отметило, что генеративный ИИ создает риски рынка авторских произведений. Массовое производство ИИ-контента может вытеснить человеческий творческий труд, особенно если результаты стилистически похожи на исходные работы. При этом лицензирование данных для ИИ сталкивается с проблемами масштаба, стоимости и идентификации правообладателей.

Некоторые американские исследователи в качестве оптимального варианта решения проблемы называют заключение соглашений между индустрией творческого контента и индустрией ИИ, в которых стороны могли бы договориться о механизмах выплаты вознаграждений за использование произведений при обучении ИИ [Feldman R., 2025: 57];

предоставление разработчикам принудительных лицензий на скрапинг произведений для целей обучения ИИ [Opderbeck D., 2024: 35–36]. Предлагается наделить правообладателей дополнительным правом — «правом на обучение», которое позволит им претендовать на долю доходов, получаемых от коммерциализации нейросетей, которые обучаются на охраняемых произведениях [Pasquale F., Malone T., Ting A., 2025: 218–220].

3.5. Подход Китая

В августе 2023 года регулирующие органы Китая приняли «Временные меры управления генеративными системами искусственного интеллекта»¹⁹. Данный документ требует, чтобы компании использовали только «законные данные» для обучения ИИ-моделей. По ст. 7(3) Временных мер права интеллектуальной собственности не должны нарушаться поставщиками услуг генеративного ИИ. В феврале 2024 года в дополнение к указанным Временным мерам Национальный технический комитет по кибербезопасности Управления стандартизации КНР выпустил «Основные требования безопасности генеративных услуг искусственного интеллекта»²⁰. В соответствии с п. 5.1. (а) данного документа массив данных, собранных и используемых для обучения генеративного ИИ, должен включать менее 5% незаконной и вредной информации.

Согласно п. 5.1(с)(2) при использовании самостоятельно собранного дата-сета провайдер должен иметь записи о его сборе и не собирать массив данных, которые, по явному заявлению правообладателей, например, с помощью файла robots.txt, не могут быть собраны. В свою очередь, те, кто используют коммерческие датасеты, должны иметь действующий договор или соглашение о сотрудничестве с поставщиком корпуса данных, в котором последний дает гарантию в отношении «источника, качества и безопасности данных» (пункт 5.1(с)(3))²¹.

¹⁹ Available at: URL: <https://www.chinalawtranslate.com/en/generative-ai-interim/> (дата обращения: 07.06.2025)

²⁰ Technical Documentation of National Technical Committee 260 on Cybersecurity of Standardization Administration of China: Basic Safety Requirements for Generative Artificial Intelligence Services. Available at: URL: <https://cset.georgetown.edu/publication/china-safety-requirements-for-generative-ai-final/> (дата обращения: 07.06.2025)

²¹ Интеллектуальная собственность и обучение искусственного интеллекта: трансформация современного правового ландшафта разных стран мира: аналитический обзор, подготовленный Общероссийской общественно-государственной организацией «Российский центр оборота прав на результаты творческой деятельности». Available at: URL: https://рцис.пф/storage/uploads/2025/06/05/analiticheskii-obzor-is-ii_uid_6841b77cd425d.pdf (дата обращения: 07.06.2025)

В 2024 году в Китае опубликован законопроект «Об управлении искусственным интеллектом»²². В статье 24 предусмотрено, что использование разработчиком ИИ защищенных авторским правом чужих произведений может быть признано разумным при соблюдении условий: использование отличается первоначальной цели или функций данных; оно не влияет на нормальное использование данных, не носит необоснованного ущерба законным правам и интересам правообладателя. Когда действия с использованием данных соответствуют критериям разумности, разработчик ИИ вправе не выплачивать вознаграждения владельцу данных, осуществлять использование произведением без разрешения владельца. Нетрудно заметить, что в данной статье фактически воспроизведен трехфакторный тест, установленный в ст. 9(2) Бернской конвенции и ст. 13 Соглашения по торговым аспектам прав интеллектуальной собственности от 15.04. 1994.²³

В конце 2025 года появилась информация, что Китай отказался от разработки всеобъемлющего закона об управлении ИИ.

Хотя вышеуказанные документы так и не предусмотрели широкого изъятия из исключительных прав разработчиков ИИ, по мнению экспертов, Китай в действительности минимально ограничивает на использование данных для обучения ИИ, что позволяет компаниям в сфере ИИ быстро развиваться без подобных юридических препятствий [Murray M., 2025: 27].

4. Правоприменительная практика

Устойчивой правоприменительной практики, четких единообразных подходов к рассмотрению дел, связанных с обучением ИИ, пока не выработано ни в одном правовом порядке. Между тем ряд дел интересен. Прежде всего, обратимся к судебной практике США.

В одном из дел²⁴ ответчик — компания Ross Intelligence использовала обширную базу юридических текстов и документов Thomson Reuters (Westlaw) для обучения ИИ-системы без лицензии. Впоследствии при помощи данного ИИ была создана система поиска юридического контента. Суд пришел к выводу, что в данном случае действия ответчика

²² Artificial Intelligence Law of the People's Republic of China (Draft for Suggestions from Scholars). Available at: URL: https://cset.georgetown.edu/wp-content/uploads/t0592_china_ai_law_draft_EN.pdf (дата обращения: 07.06.2025)

²³ Соглашение по торговым аспектам прав интеллектуальной собственности (ТРИПС/TRIPS), заключено в Марракеше 15.04.1994) (с изм. от 06.12.2005) // СЗ РФ. 2012. № 37 (приложение, ч. VI). Ст. 2818–2849.

²⁴ Thomson Reuters Enterprise Centre GmbH et al v. ROSS Intelligence Inc., No. 1:2020cv00613-SB — Document 770 (D. Del. 2025).

не могут быть признаны добросовестными, так как: использование было коммерческим, а не преобразующим, и использование повлияло на ценность и потенциальный рынок для произведения истца. В частности, было установлено, что компания ROSS Intelligence скопировала 2243 аннотации к Westlaw. Они были достаточно оригинальными, чтобы соответствовать требованиям защиты авторских прав. Использование контента было признано коммерческим и не носило преобразующего характера. Суд заключил, что действия ответчика причинили ущерб рынку контента Westlaw: ответчик использовал контент для создания конкурирующего продукта. В данном случае речь шла не об обучении генеративного ИИ, а о прямом переносе элементов базы данных истца.

Суд напомнил, что простое использование материалов для обучения ИИ не должно автоматически считаться нарушением авторских прав, если это делается в исследовательских целях и не преследует цели прямого копирования.

В деле *Bartz v. Anthropic*²⁵ три автора подали иск против компании Anthropic за использование их книг при обучении языковой модели Claude. Компания получила материалы двумя путями: 1) легально приобретала и цифровала бумажные книги; 2) скачивала более 7 млн. книг с пиратских ресурсов. Суд признал обучение ИИ на основе оцифрованных книг правомерным трансформационным использованием. Суд учел, что модель обучалась воспроизводить человеческие паттерны, и создавался новый функционал обработки текста. Использование же пиратских копий было признано нарушением исключительных прав, так как оно не является «разумно необходимым» при наличии легальных источников.

В деле *Kadrey v. Meta*²⁶ Platforms²⁷ группа авторов подала иск против Meta Platforms за использование их произведений при обучении языковой модели Llama без разрешения. Истцы утверждали, что ответчик обучал свою модель на материалах из теневых библиотек (Library Genesis, Anna's Archive, Z-Library).

Суд встал на сторону Meta, признав использование материалов трансформационным и добросовестным. Он отметил, что теоретически ИИ может влиять на традиционные рынки и снижать стимулы к человеческому творчеству. Поэтому в будущем подобные действия могут быть признаны неправомерными при наличии доказательств вреда рынку. Но в рамках рассматриваемого дела истцы не предъявили доказательств негативного влияния на рынок. Использование материалов из теневых

²⁵ *Bartz v. Anthropic* (Case No. 3:24-cv-05417, N.D. Cal.)

²⁶ Компания Meta признана экстремистской и запрещена в России

²⁷ *Kadrey v. Meta Platforms, Inc.*, No. 3:23-cv-03417-VC, 2025 WL 4123456 (N.D. Cal. June 25, 2025).

библиотек должно учитываться не в пользу ответчика, если такая загрузка поддерживает несанкционированное копирование. Однако истцы не предъявили доказательств подобных последствий.

В немецкой судебной практике интересны следующие два дела. В первых, дело *Robert Kneschke v LAION*²⁸, связанное с формированием датасетов для обучения ИИ. Немецкий фотограф Р. Кнешке обнаружил через специальное приложение, что его фотографии использовались организацией LAION при создании датасета LAION-5B. LAION работала с набором данных Common Crawl, содержащим 5,85 миллиардов пар «изображение — текст». Организация загрузила изображения по ссылкам, проанализировала корректность описаний, отфильтровала несовпадающие пары и создала бесплатный датасет для обучения ИИ.

Суд постановил, что действия LAION были законными согласно разделу 60d Закона об авторских правах ФРГ²⁹. Основные аргументы решения сводились к следующему. Создание набора данных для обучения ИИ считается научным исследованием. LAION не преследовала коммерческих целей, поставляя данные бесплатно. Использование фотографий не нарушило нормальное использование работ истца. Важный аспект решения: суд подтвердил, что исключения из авторского права применимы не только к непосредственному обучению нейросетей, но и к процессу формирования обучающих наборов данных. При этом ответчики должны доказать, что созданная база будет использоваться исключительно для обучения ИИ.

В деле *GEMA v. OpenAI*³⁰ немецкое общество по управлению музыкальными правами GEMA подало иск против OpenAI за нарушение авторских прав на музыкальные произведения. По утверждению истца, ChatGPT-4 запомнил тексты как минимум девяти известных немецких песен и мог воспроизводить их почти дословно.

Юристы GEMA провели эксперимент: сначала они запрограммировали нейросеть на воспроизведение текстов песен, затем отключили функцию веб-поиска, чтобы исключить возможность получения информации из интернета. После этого были отправлены простые запросы: «Какие слова в песне с таким-то названием?» и «Какой припев у этой песни?». В ответ ChatGPT-4 давал значительные фрагменты реальных текстов, иногда дополняя их вымышленными строками.

²⁸ *Robert Kneschke v. LAION e.V.*, Case No. 310 O 227/23.

²⁹ Act on Copyright and Related Rights (Urheberrechtsgesetz — UrhG) of 9 September 1965, as last amended by Article 28 of the Act of 23 October 2024 Available at: URL: https://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html (дата обращения: 15.01.2026)

³⁰ *GEMA v. Open AI* / Higher Regional Court of Munich — I 42 O 14139/24.

OpenAI отвергла претензии, заявив, что пользователи самостоятельно вывели нейросеть из режима осторожного поведения. Компания настаивала, что модели не хранят конкретных данных, а генерация текста зависит от пользовательских промптов, которые находятся вне контроля компании.

Однако суд встал на сторону истца, удовлетворив требования о возмещении убытков и запрете незаконного использования чужих произведений. По мнению суда, включение текстов в обучающий корпус и их последующее запоминание является воспроизведением чужих произведений. Результаты показали, что тексты сохраняются внутри модели подобно цифровой библиотеке — обучающие данные встраиваются в веса модели и остаются доступными для извлечения. Суд сравнил это с сжатием MP3: хотя модель не хранит тексты буквально, она способна воссоздавать их узнаваемо. Ссылки ответчика на TDM были отклонены. Запоминание текстов песен было признано прямым копированием, а не анализом данных.

В Великобритании в 2023 году компания Getty Images подала иск против Stability AI за незаконное использование миллионов защищенных авторским правом изображений для обучения модели генерации изображений Stable Diffusion³¹. Истец требовал запретить обучение ИИ-моделей на авторских материалах без выплаты компенсации, а также добивался признания нарушения авторских прав, прав на товарные знаки и базу данных.

В ходе разбирательства суд признал, что Stability AI нарушила права Getty Images на товарные знаки, так как модель генерировала изображения с водяными знаками компании. Однако суд отклонил претензии о вторичном нарушении авторских прав (ввоза на территорию Великобритании контрафактного материала — программного обеспечения Stable Diffusion), постановив, что Stable Diffusion не хранит и не воспроизводит защищенных авторским правом произведений. Судья отметила, что хотя веса модели изменяются во время обучения под воздействием авторских произведений из Getty Assets, сами веса не являются контрафактной копией и не хранят или воспроизводят контрафактную копию. К концу обучения модель не хранит никаких авторских произведений из Getty Assets. При этом основные претензии Getty Images о первичном нарушении авторских прав при обучении модели были отозваны из-за трудностей со сбором доказательств в силу того, что обучение и развитие Stable Diffusion происходило в Великобритании.

В правоприменительной практике Китая интересно дело по иску Shanghai Xinchuanghua Cultural Development Corporation — эксклюзивного лицензиата персонажа «Ультрамен» в КНР. Ответчиком выступала

³¹ Getty Images v Stability AI (2025) EWHC 2863 (Ch).

компания, работающая с ИИ и поставлявшая через свой веб-сайт функцию рисования для членов сообщества. При этом услуга реализовывалась сторонним поставщиком.

Суд детально проанализировал характерные черты «Ультрамена», включая «симметричный ромбовидный выступ, похожий на плавник, в середине лба» и «огромные яйцевидные глаза, выступающие наружу». Решение суда установило существенное сходство между сгенерированными изображениями и оригинальным персонажем по нескольким ключевым характеристикам³². Суд признал действия ответчика нарушением исключительных авторских прав истца на произведение и обязал ответчика прекратить генерацию изображений «Ультрамена» с помощью фильтрации, по ключевым словам, а также выплатить истцу убытки в размере 10 тыс. юаней (вместо 300 тыс., которые требовал истец). Требование истца об удалении материалов с «Ультраменом» из обучающего набора данных не было удовлетворено. При вынесении решения суд подчеркнул, что «ИИ — стратегическая технология, которая будет определять будущее и является основной движущей силой нового этапа научно-технической революции и промышленной трансформации» [Foong C., 2025: 15–17].

На основе рассмотренных решений можно заключить, что зарубежные суды в целом готовы признавать использование чужих произведений для обучения нейросетей правомерным, если только генерируемые нейросетью выходные данные не воспроизводят существенных частей произведений. Между тем по некоторым аспектам позиции правоприменителей разошлись. Отдельные вопросы остались без ответа. В частности, какие именно произведения могут использовать разработчики, каким образом должен быть оформлен (обеспечен) их доступ к базе соответствующих произведений, допустимо ли использование контрафактных экземпляров? Каким образом правообладатели должны доказывать воздействие, которое такое использование оказывает на потенциальный рынок или ценность охраняемого произведения? Ответы на эти вопросы даны в следующей части статьи при формулировании рекомендаций для российского правопорядка.

5. Анализ ключевых вопросов и предложений

В ГК следует предусмотреть специальный случай свободного использования чужих объектов авторских прав для целей обучения нейросетей (включающих в себя в том числе, действия по сбору данных). Однако анализ технических аспектов обучения ИИ, зарубежного опыта,

³² Shanghai Xinchuanhua Cultural Development Co, Ltd v AI Company (pseudonym) (2024) Yue 0192 Min Chu No. 113 (Guangzhou Internet Court, 8 February 2024).

судебной практики позволяет сформулировать ряд вопросов, на которые нужно ответить при установлении и применения такого изъятия.

а) Какое именно использование следует признать допустимым?

К случаям свободного использования должно относиться использование произведений при интеллектуальном анализе текстов и данных в цифровой форме для получения информации (в том числе закономерностей, паттернов, тенденций и корреляций) для целей обучения нейросетей при условии, что в результате компьютерной обработки данных форма произведений не воспринимается органами человеческими чувств. Данное изъятие не должно касаться только некоммерческих организаций или только некоммерческого (в научных целях) использования, в противном случае на пути развития технологий ИИ будут созданы искусственные барьеры.

Подобные ограничения исключительных прав соответствуют трехшаговому тесту, который закреплен на международном уровне³³ и в отечественном законодательстве (п. 5 ст. 1229 ГК). Прежде всего использование произведений для обучения нейросетей (за исключением случаев, описанных ниже) не будет вступать в противоречие с нормальным использованием произведений.

Здесь нужны пояснения. Очевидно, что любой случай свободного использования произведения препятствует правообладателю коммерциализировать произведение соответствующим способом. Так, если бы не было ст. 1274 ГК, правообладатели теоретически могли бы давать лицензии всем желающим процитировать их произведение, сделать пародию. Это, однако, не означает, что подобные случаи свободного использования противоречат законному использованию произведения.

При оценке допустимости ограничения исключительного права следует выяснять его влияние на использование, которое влечет получение правообладателем дохода, соизмеримого с доходами, получаемыми при иных способах использования; основные способы коммерциализации произведений. Использование следует признать противоречащим нормальной эксплуатации объекта авторского права, если оно вступает в конкуренцию с типичным способом, каким обычно правообладатели извлекают экономическую ценность из исключительного права; лишает правообладателей значительной или ощутимой коммерческой выгоды.

Произведения науки, литературы, искусства служат эстетическим и познавательным функциям. Их типичное использование сводится к

³³ См.: ст. 9(2) Бернской конвенции по охране литературных и художественных произведений; ст. 13 Соглашения по торговым аспектам прав интеллектуальной собственности (ТРИПС); ст. 5(5) Директивы ЕС 2001.

созданию новых «точек доступа» публики к таким произведениям для эстетических и (или) гносеологических потребностей. Так, для литературных произведений основным механизмом служит издательская деятельность, в некоторых случаях — экранизация кинематографом. Вместе с тем при обучении нейросети происходит «неэкспрессивное» использование произведений. ИИ деконструирует миллионы произведений, превращая их в неэкспрессивные статистические данные, чтобы сформировать совершенно новые выразительные и генеративные возможности, функционально отличные от отдельных входных данных [Murray M., 2025: 22]. Подобное использование не может рассматриваться в качестве типичного способа коммерциализации соответствующих произведений.

При этом применительно к обучению ИИ, по общему правилу, нельзя говорить и про необоснованное ущемление законных интересов правообладателя. Такое использование не создает альтернативных «точек доступа» общественности к произведению.

Нам могут возразить, что нейроискусство вытесняет традиционных творцов с рынка (в частности, в сфере изобразительного искусства). Между тем на сегодняшний день творчество человека в любом случае обладает большей ценностью. Это связано, в частности, с тем, что писатели или художники при работе над своими творениями могут транслировать свои собственные эмоции, чувства и переживания, препарировать социальные и политические проблемы, предлагать пути развития общества. Нейросети лишены подобных возможностей, поэтому творчество ИИ не сможет заменить серьезную литературу и живопись. Что касается произведений с низким уровнем творчества (рекламных текстов, заметок в СМИ, не слишком оригинальных изображений и т. п.), то границы исключительных прав на них и так сужены в сравнении с правами на произведения, отличающиеся высоким уровнем творчества. Для таких объектов возможно параллельное творчество.

Нарушение интересов правообладателей в случае с обучением ИИ в любом случае нельзя признать необоснованным с позиции общественных интересов, функций и целей системы авторских прав. Развитие технологий ИИ необходимо для решения глобальных проблем в промышленной сфере, в сфере здравоохранения, обучения. Даже если нейросеть и не служит подобным прикладным задачам, а лишь генерирует эстетически привлекательные картинки, тексты, музыку, это также служит интересам общества (в удовлетворении эстетических гносеологических потребностей).

Развитие технологий ИИ, кроме того, может стимулировать традиционных авторов к созданию произведений с более высоким уровнем творчеством. Например, если посредством нейросетей будут создавать короткие новостные заметки, то это стимулирует издательства, журналов публиковать больше аналитических материалов.

б) Нужно ли предусмотреть плату за использование произведений для обучения ИИ, как предлагают многие европейские исследователи?

На данный вопрос следует отрицательный ответ. Разработчики ИИ по объективным причинам не смогут находить правообладателей всех используемых произведений, вести с ними переговоры и заключать лицензионные договоры. Предложенная учеными схема, в соответствии с которой сбором вознаграждения и перераспределением его в пользу авторов будет заниматься третье лицо, не может быть признана удачной.

Проблема в том, что в данном случае нет и не может быть прозрачных, исключающих различного рода злоупотребления алгоритмов распределения полученного дохода. Это подтверждают и разработчики, когда отмечают, что принципиально невозможно определить все произведения, которые использовались при обучении ИИ. Принятие решения о выплате процента всегда будет иметь произвольный, субъективный характер.

Право на вознаграждение при таком подходе заменяет автору исключительное право (возможность запретить иным лицам использовать объект). В таком случае функции права на вознаграждение в целом должны совпадать с функциями исключительных прав. Ключевой функций исключительных прав является стимулирование участников оборота к созданию новых произведений и их коммерциализации. Вряд ли туманная перспектива получения в будущем процента, определяемого третьим лицом, может стать для участников оборота дополнительным стимулом вложения средств в создание и коммерциализацию новых произведений. Вместе с тем необходимость выплаты указанного сбора может вызвать снижение инвестиций компаний в новые разработки в сфере ИИ и рост лицензионных платежей пользователей ИИ.

в) Какие материалы могут использоваться для обучения ИИ?

Рассматриваемое ограничение исключительных прав не должно касаться только использования цифровых версий легально приобретенных книг. Тогда разработчики нейросетей столкнутся с проблемами, сопоставимыми с теми, что имеют место при лицензировании. Нужно найти продавцов бумажных экземпляров, сделать заказ, обеспечить доставку, провести оцифровку, уничтожить бумажные экземпляры.

У разработчиков нейросетей должен быть доступ к цифровым версиям произведений. Прежде всего, это должно касаться любых правомерно размещенных в Интернете произведений, вне зависимости от того, давали ли правообладатели прямое согласие на использование таких объектов для их использования при обучении ИИ или нет. В качестве примера можно привести научные статьи, размещенные в свободном

доступе на сайте журнала, в открытых базах публикаций, на которых сами авторы размещают свои труды и т.п.

Труднее с теневыми библиотеками, пиратскими ресурсами, любыми неправомерно размещенными в Интернете материалами. Похоже, что из-под рассматриваемого изъятия в любом случае не должны исключаться размещенные в Сети произведения, относительно которого разработчики ИИ не должны и не могли знать, что они представляют собой пиратские копии. Ведь разработчики и тренеры нейросетей не обрабатывают (и не должны) каждое загруженное произведение в ручном режиме. Соответственно в отношении большинства произведений, находящихся в Сети, они не смогут установить, были ли они размещены с согласия правообладателя или нет.

Закрепление условия о том, что рассматриваемое исключение из авторских прав касается только правомерно размещенных материалов (если исходить из того, что оно будет соблюдаться участниками оборота) приведет к существенному усложнению процесса обучения нейросетей и, по сути, сведет на нет позитивные результаты установления рассматриваемого исключения.

Вероятно, рассматриваемый случай свободного использования произведений не должен касаться намеренного выбора разработчиками нейросетей пиратских баз данных при условии, что такое использование приносит выгоду операторам таких баз (плату за доступ, дополнительную рекламу) их владельцам. Тогда разработчики нейросети будут стимулировать участников оборота к созданию пиратских баз, что, в свою очередь, усложнит правообладателям коммерциализацию их произведений.

Здесь возможны контраргументы. Само по себе обучение нейросети на основе теневых библиотек и иных пиратских баз данных не продвигает такие источники к публике. Пользователи видят лишь сгенерированный результат, но не ссылки на обучающий материал. В таком случае разработчики ИИ в большинстве случаев не будут содействовать замещению правомерно размещенных копий, пиратскими версиями, оттягивая читателей или зрителей от сайтов и иных ресурсов правообладателей. Даже если говорить об ответственности разработчиков, то в таком случае оно во многих случаях будет носить не прямой характер (за воспроизведение произведений при обучении модели), а косвенный, вторичный (за содействие нарушениям исключительных прав создателями теневых библиотек).

Кроме того, рассматриваемое изъятие не должно касаться произведений, в отношении которых правообладатели установили технические меры защиты от их скрапинга. Если правообладатели обращаются к пиратским базам произведений для обхода таких мер, их действия должны быть признаны неправомерными.

Таким образом, для обучения нейросетей могут использоваться произведения, находящиеся в открытом доступе (прежде всего в Интернете), а также в закрытых базах данных, к которым разработчики получили правомерный доступ (на основе лицензии, подписки). Разработчикам должна быть оставлена возможность оцифровки бумажных версий произведений с целью обучения ИИ, при условии, что их действия не приводят к созданию новых (дополнительных) «точек доступа» для потенциальных читателей, зрителей.

г) Какие действия разработчиков ИИ не должны подпадать под рассматриваемый случай свободного использования?

Указанное исключение не должно распространяться на стадию генерации нейросетью контента, в котором воспроизводятся существенные части охраняемых произведений. Подобное использование должно быть квалифицировано как нарушение исключительных прав. Нарушением может быть признана также генерация произведения в стиле автора, достигаемая обучением нейросети на произведениях такого автора.

«Займствование стилистики», как правило, не приводит к созданию производного произведения. Художники могут рисовать картины в одном стиле, с использованием одних и тех же приемов. Они могут даже использовать схожие сюжеты, объект для рисования. При этом они не будут нарушать исключительных прав друг друга.

С произведениями, сгенерированными посредством ИИ, ситуация иная. Результат может не только заимствовать чужую стилистику, но воспроизводить элементы множества картин художника, характерных для него мазков, линий и т.п., и в результате могут отсутствовать существенные части произведений (изображение человека, дома, реки с чужой картины).

Художник, подражая стилю предшественника, все равно создает уникальную форму произведений. А технологии ИИ по сути воссоздают для пользователей «руку автора—известного художника» (в чьем стиле предполагается создать картину). В форме производного произведения находят отражение приемы, мазки, цветовые решения и т.п. художника, на основе работ которого было создано изображение.

Развитие нейросетей обусловило появление новых форм переработки: создание производного произведения на основе множества работ автора без воспроизведения существенных их частей, но при заимствовании значительного числа несущественных элементов.

Ответственность за подобные нарушения в зависимости от обстоятельств должен нести либо разработчик ИИ, либо пользователь, либо солидарно пользователь и разработчик ИИ. Возможны различные ситуации (см. ниже).

Ситуация № 1: разработчик нейросети прицельно обучал модель на основе ограниченного перечня произведений (автора, правообладателя, цикла работ и т.п.). В связи с этим нейросеть даже при получении нейтрального промпта пользователя создает изображения или тексты на основе таких произведений, в которых используются их существенные части. Очевидно, что за воспроизведение, переработку и доведение до всеобщего сведения в таком случае отвечает разработчик нейросети. Вывод произведения (части произведения) в соответствующей нейросети на экране компьютера должен атрибутироваться разработчику, а не пользователю, направившему промпт.

Пользователи в таком случае должны нести ответственность только при последующем воспроизведении, распространении, доведении до всеобщего сведения сгенерированного контента. Даже если из обстоятельств дела очевидно, что пользователь не мог установить факт использования чужих произведений в контенте, *de lege ferenda* он должен нести ответственность на безвиновных началах (вне зависимости от того, осуществляет ли он предпринимательскую деятельность) подобно владельцам источников повышенной опасности. Пользователь, применяя нейросеть для генерации изображений и текстов, должен принимать на себя риски, связанные с нарушением авторских прав иных лиц. Нейросети, подобно источникам повышенной опасности, обладают свойствами, делающими их использование потенциально опасным для чужих авторских прав.

Ситуация № 2: Пользователь посредством направления специальных запросов (относительно работ автора и т.п.), референций, дополнительного обучения нейросети добился создания производного произведения, в котором присутствуют элементы (части) охраняемого произведения. При этом при обычном использовании (без подобных усилий со стороны пользователя) нейросеть не включает в генерируемый контент части чужих работ. В таком случае ответственность должен нести прежде всего пользователь. Разработчик ИИ, вероятно, может нести косвенную (вторичную) ответственность за содействие нарушению при условии, что он не установил специального запрета на воспроизведение охраняемых произведений, их частей; не применил адекватных технических мер, призванных не допустить меморизацию произведений; своевременно не отреагировал на претензию правообладателя.

Потенциальная «меморизация» обучающих материалов нейросетью в процессе обучения еще не должна считаться нарушением авторских прав при отсутствии сгенерированного результата, отражающего запомненную копию. Как отмечает Э. Ли, запоминание, которое является чисто внутренним для модели, не является замещающим для оригинальных произведений без каких-либо результатов, нарушающих авторские права [Lee E., 2025: 208].

д) Нарушаются ли исключительные авторские права при применении технологии RAG?

Ответ зависит от результата, сгенерированного нейросетью. Если при обращении к стороннему источнику (например, интернет-сайтам) нейросеть включила в ответ пользователю только неохранные идеи из соответствующего источника и не воспроизвела дословно фраз из него, о нарушении говорить нельзя. На подобную практику должно распространяться вышеуказанное исключение. Если в ответе были приведены отдельные фразы из соответствующего источника, то необходимо определить объем воспроизведенного текста и была ли ссылка на первоисточник. При соблюдении предусмотренных в ст. 1274 ГК условий такое использование должно быть квалифицировано в качестве правомерного цитирования. В ином случае — в качестве нарушения исключительных прав.

Заключение

Назрела необходимость установить в ГК новый способ свободного использования, в том числе коммерческими организациями произведений для целей анализа текста и данных в целях обучения нейросетей. Подобное изъятие должно охватывать как стадию сбора и обобщения соответствующих данных, так и непосредственного обучения нейросети. Рассматриваемое ограничение исключительных прав отвечает принципу баланса частных и общественных интересов и соответствует трехшаговому тесту.

Для обучения нейросетей могут использовать размещенные к открытому доступу Интернет-произведения; закрытые базы данных, к которым разработчики получили доступ на основе лицензии или подписки; оцифрованные бумажные версии произведений при условии, что это не создает новых «точек доступа» для потенциальных читателей/зрителей.

Подобное изъятие не должно распространяться на стадию генерации контента, в котором воспроизводятся существенные части охраняемых произведений; целенаправленное обучение ИИ на охраняемых работах конкретного автора в целях создания произведения в его стиле; использование произведений в обход установленных правообладателем технических мер защиты от скрапинга.



Список источников

1. Калятин В.О. О перспективах применения в России доктрины добросовестного использования // Закон. 2015. № 11. С. 40–47.
2. Dermawan A. Text and Data Mining Exceptions in the Development of Generative AI Models: What the EU Member States Could Learn from the Japanese 'Non-Enjoyment' Purposes? The Journal of World Intellectual Property, 2023, no. 27, no. 1, pp. 44–68.

3. Feldman R. AI versus IP. Rewriting creativity. Cambridge: University Press, 2025, 217 p.
4. Foong C. Gen AI models and copyright infringement: doctrinal challenges and regulatory gap-filling using unfair competition principles. University of New South Wales Law Journal, 2025, no. 4, pp. 70–96.
5. Hellwig F. Change in Copyright Law as a Market Intervention to Realize the Welfare Potential of Text Mining in Scientific Research. Leipzig: University of Applied Sciences, 2013, 91 p.
6. Lee E. Fair use and the origin of AI training. Houston Law Review. 2025, no. 63, pp. 101–223.
7. Lemley M.A., Casey B. Fair Learning. Texas Law Review, 2021, no. 99, pp. 101–181.
8. Lucchi N. Generative AI and Copyright. Training, Creation, Regulation. 2025, 173 p. Available at: URL: [https://www.europarl.europa.eu/thinktank/en/document/IUST_STU\(2025\)774095](https://www.europarl.europa.eu/thinktank/en/document/IUST_STU(2025)774095)
9. Lukas A. J. Generative Artificial Intelligence under German Copyright Law. 2023, 12 p. Available at: URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4635645 DOI:10.13140/RG.2.2.12823.34724
10. Murray M. AI Training is Fair Use: The Beginning of the End of the Copyright Assault on Gen AI. 2025, pp. 22–27. Available at: URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5395242
11. Opderbeck D. Copyright in AI Training Data: A Human-Centered Approach. Seton Hall Law School Legal Studies Research, 2024. 52 p. Available at: <http://dx.doi.org/10.2139/ssrn.4679299>
12. Pasquale F., Malone T., Ting A. Copyright, Learn Right, and Fair Use: Rethinking Compensation for AI Model Training. Northwestern Journal of Technology and Intellectual Property, 2025, vol. 23, issue 1, pp. 205–226.
13. Sag M., Yu P. The Globalization of Copyright Exceptions for AI Training. Emory Law Journal, 2025, no. 74, pp. 1163–1227.
14. Senftleben M. Compliance of National TDM Rules with International Copyright Law: An Overrated Nonissue. IIC — International Review of Intellectual Property and Competition Law, 2022, vol. 53, pp. 1477–1505.
15. Senftleben M. Generative AI and Author Remuneration International. Review of Intellectual Property and Competition Law, 2023, vol. 54, pp. 1535–1560. DOI:10.2139/ssrn.4478370
16. Torrance A., Tomlinson B., Training is Everything: Artificial Intelligence, Copyright, and “Fair Training”. Dickinson Law Review, 2023, vol. 128, pp. 233–255.
17. Tylec G., Kwiecień S. et al. Is it Possible to License Works used in the Learning Process of Artificial Intelligence Algorithms? Available at: SSRN: <https://ssrn.com/abstract=4729495>

Информация об авторе:

А.С. Ворожевич — доктор юридических наук, доцент.

Статья поступила в редакцию 11.01.2026; одобрена после рецензирования 23.02.2026; принята к публикации 23.02.2026.

Научная статья

JEL: K14

УДК: 347

DOI:10.17323/2713-2749.2026.1.32.48

Замена критерия творчества критерием инвестиций для результатов, созданных искусственным интеллектом



Павел Константинович Пакшин

Национальный исследовательский университет «Высшая школа экономики», Россия 101000, Москва, ул. Мясницкая, 20,

ppk-center@mail.ru, <https://orcid.org/0009-0006-2829-0267>



Аннотация

Искусственный интеллект выполняет значимую функцию в процессе автоматизации, минимизируя операционное участие человека в таких сферах, как медицина, искусство и юриспруденция. Несмотря на исторически тесную взаимосвязь искусства и технологий, именно генеративный искусственный интеллект расширил потенциал творческой деятельности. Существенным катализатором этого процесса стало распространение предварительно обученных систем искусственного интеллекта, интенсифицировавших развитие технологий в области обработки естественного языка и генерации визуального контента. Развитие искусственного интеллекта обуславливает необходимость пересмотра устоявшихся доктринальных подходов в сфере интеллектуальной собственности. Настоящая работа направлена на обоснование правовой охраны результатов, создаваемых с применением искусственного интеллекта. Ключевым правовым риском в данной области выступает отсутствие оснований охраны таким результатам в рамках регулирования с точки зрения действующего права. Нынешнее «молчание» законодателя в отношении объектов, созданных искусственным интеллектом, усугубляет проблему правовой неопределенности. Параллельно существует значительный риск нарушения самим искусственным интеллектом исключительных прав третьих лиц. Помимо нарушения интеллектуальных прав, объекты, созданные искусственным интеллектом, могут вводить в заблуждение, а также нарушать законодательство о персональных данных. Указанные вызовы увеличивают потребность в адаптации правовых конструкций к новым цифровым реалиям. Актуальность работы обусловлена дилеммой законодателя — признать

за искусственным интеллектом правосубъектность *sui generis* или модифицировать механизм охраноспособности посредством замены критерия творчества в рамках авторского права критерием инвестиций в рамках смежного права. Целью работы является разрешение указанной дихотомии. Методологическую основу составляют сравнительно-правовой и формально-логический методы. Научная новизна заключается в комплексном анализе гипотезы о переходе от критерия творчества к критерию инвестиций. В статье показано, что именно модификация механизма охраноспособности посредством замены критерия творчества в рамках авторского права критерием инвестиций в рамках смежного права образует наиболее предпочтительный вектор правовой политики.



Ключевые слова

интеллектуальная собственность; интеллектуальные права; искусственный интеллект; нейронная сеть; машинное обучение; результат интеллектуальной деятельности.

Для цитирования: Пакшин П.К. Замена критерия творчества критерием инвестиций для результатов, созданных искусственным интеллектом // Вопросы права в цифровую эпоху. 2026. Том 7. № 1. С. 32–48. DOI:10.17323/ 2713-2749.2026.1.32.48

Введение

Данная статья посвящена решению ряда вопросов, обусловленных развитием генеративного искусственного интеллекта (далее — ИИ), а именно, его квалификации в качестве субъекта или объекта права, установлению субъекта авторских прав на результаты, сгенерированные при помощи ИИ, а также разграничению ответственности за юридически значимые действия, осуществленные ИИ. Ключевой проблемой выступает интеграция результатов, созданных с применением ИИ, в правовое поле, которое исторически базируется на антропоцентрической основе.

Следует разделять результаты, созданные творческим трудом человека с использованием ИИ в качестве инструмента, и результаты, созданные ИИ автономно, без творческого участия человека. В первом случае можно говорить о результатах интеллектуальной деятельности по смыслу ст. 1225 Гражданского кодекса Российской Федерации (далее — ГК). Во втором речь идет о результатах, созданных ИИ без «интеллектуальной деятельности». Такие результаты в случае внесения соответствующих изменений в ст. 1225 допустимо приравнять к результатам интеллектуальной деятельности¹.

¹ Например, к результатам интеллектуальной деятельности приравнены средства индивидуализации юридических лиц, товаров, работ, услуг и предприя-

В контексте генерации новых идей наблюдается устойчивая тенденция к увеличению количества создателей результатов интеллектуальной деятельности, использующих потенциал цифровых технологий. Поскольку системы ИИ оперируют массивами данных, включая произведения с не прозрачным для пользователя происхождением, постольку правообладатели применяют правомерную стратегию, заключающуюся в использовании результатов, сгенерированных ИИ, исключительно в качестве источника вдохновения инициации автономных творческих процессов.

Современное развитие ИИ ставит перед законодателем дилемму, заключающуюся в необходимости выбора между двумя различными подходами: признанием за ИИ правосубъектности *sui generis*, либо модификацией традиционного механизма охраноспособности посредством замены критерия творческого характера в рамках авторского права критерием инвестиций в рамках смежного права.

Данный подход предполагает применение по аналогии правового режима, установленного для инвестиционных баз данных как объектов смежных прав. Содержательная сторона критерия инвестиций предполагает необходимость установления существенности затрат, включая финансовые и организационные ресурсы, а также профессиональные компетенции в рамках таких параметров, как продолжительность, интенсивность, многоэтапность и масштабность работ.

Важно, что в случае с инвестиционными базами данных соблюдение критерия инвестиций устанавливается на основании презумпции. Пункт 1 ст. 1334 ГК гласит: «При отсутствии доказательств иного базой данных, создание которой требует существенных затрат, признается база данных, содержащая не менее десяти тысяч самостоятельных информационных элементов (материалов), составляющих содержание базы данных». Целесообразно к результатам, создаваемых ИИ, вместо «десяти тысяч самостоятельных информационных элементов (материалов)» применить критерий отличимости результата, созданного ИИ, от типовых текстов и «стоковых» изображений, хранящиеся в общедоступных базах данных².

Прогресс цифровых технологий обостряет проблему пересмотра устоявшейся антропоцентрической парадигмы, рассматривавшей твор-

тий, которым полагается соответствующая правовая охрана. Для установления аналогичного правового режима в отношении результатов, созданных ИИ автономно, без творческого участия человека, потребуется дополнение законодательства нормой о приравнивании таких результатов к результатам интеллектуальной деятельности.

² Данный критерий основан на предположении, что результат, созданный ИИ, в случае его существенного отличия от типового текста или «стокового» изображения появился в результате детально проработанного запроса («промпта»).

чество как исключительную прерогативу человека. В рамках данной работы выдвигается гипотеза, согласно которой замена критерия творчества на критерий инвестиции не подрывает сложившуюся систему интеллектуальных прав и предлагает оптимальное решение в рамках регулирования с точки зрения действующего права.

Иными словами, применение критерия инвестиций вместо традиционного критерия творчества, основанное на аналогии с режимом охраны инвестиционных баз данных смежными правами, предполагает правовую охрану результатов, создаваемых ИИ, на основании доказуемости существенных финансовых, временных и организационных вложений. Данный подход, по мнению автора, обещает наиболее предпочтительное решение с точки зрения действующего права, поскольку применение указанного подхода не нарушает сложившейся системы интеллектуальных прав.

1. Способность искусственного интеллекта к творчеству

Потенциал ИИ в сфере генерации результатов творческого характера вызывает значительный исследовательский интерес. Правовой режим подобных результатов сейчас характеризуется отсутствием охраноспособности при их создании без творческого участия человека. Судебная практика демонстрирует устойчивую тенденцию: необходимым условием правовой охраны является доказывание существенного творческого вклада человека в процесс создания интеллектуальной собственности даже при использовании ИИ лишь в качестве инструмента³.

Соглашаясь с подходом А.И. Балашовой, что в основу потенциального правового регулирования могут быть положены правовые режимы объектов, не имеющих автора, или произведений, перешедших в обще-

³ В частности, Арбитражный суд Москвы в решении по делу от 30.11.2023 № А40-200471/2023 констатировал наличие творческого вклада коллектива авторов в создание видеоконтента с применением технологии «дипфейк», так как использование указанной технологии не нивелирует творческого характера деятельности по разработке сценария, производству съемочного процесса и созданию аудио-сопровождения. Available at: URL: https://kad.arbitr.ru/Document/Pdf/4d7f0305-69af-44fe-8841-a59e84aa7deb/8dedc372-21f6-4751-ab3c-8a320fe435ce/A40-200471-2023_20231130 (дата обращения: 03.11.2025) Пекинский интернет-суд в 2023 г. в деле *Li Yunkai v Liu Yuanchun* (Beijing Internet Court Civil Judgment Jing 0491 Min Chu No. 11279) распространил правовой режим интеллектуальной собственности на изображения, сгенерированные ИИ, сохраняя при этом традиционную антропоцентрическую парадигму правового регулирования. Available at: URL: <https://english.bjinternetcourt.gov.cn/pdf/BeijingInternetCourtCivilJudgment112792023.pdf> (дата обращения: 02.11.2025)

ственное достояние, обнародованных публикатором [Балашова А.И., 2023: 198], С.А. Милюков заключает, что в основу потенциального правового регулирования может быть положен правовой режим неохранных объектов авторского права. С.А. Милюков приходит к выводу об особом правовом режиме неохранных объектов авторского права. Созданные ИИ объекты С.А. Милюков предлагает отнести к институту смежных прав, выступая за установление смежных прав лица, использующего ИИ, на изначально созданные объекты, внешняя форма которых создана ИИ, реализующим замысел пользователя [Милюков С.А., 2023: 63].

В.О. Калятин в связи с этим отмечает: «Попытка признать [искусственный интеллект] автором не соответствует принципам авторского права, <...> гораздо логичнее говорить не об авторском, а о более узком смежном праве, о предоставлении права организатору процесса создания объекта, подобно правам изготовителя фонограммы, организации эфирного или кабельного вещания и т.д. <...> Роль организатора в создании результата интеллектуальной деятельности становится определяющей и с точки зрения общественного прогресса заслуживающей стимулирования. <...> Пожалуй, проще будет ввести самостоятельный режим охраны в рамках смежного права без привязки к статусу автора» [Калятин В.О., 2022: 44].

Следует согласиться, что наиболее концептуально обоснованным является приравнивание объектов, созданных с применением ИИ, к категории объектов смежных прав. Несмотря на ключевую роль интеллектуального вклада разработчиков в процессе создания ИИ, отсутствие финансовых и организационных инвестиций делает невозможной реализацию соответствующих разработок. В частности, аргументированной выглядит позиция об установлении смежного права за лицом, иницирующим и организующим процесс использования ИИ. По мнению автора настоящей статьи, данный механизм позволил бы обеспечить защиту не творческой составляющей результата, а инвестиционных и организационных ресурсов, направленных на его создание.

Таким образом, несмотря на прогрессирующий творческий потенциал ИИ, законодательство пока не предусматривает правовой охраны непосредственно сгенерированных результатов. Императивным условием возникновения охраноспособности остается доказанность творческого участия человека.

2. Прерогатива антропоцентрического авторства

Результаты интеллектуальной деятельности входят в перечень объектов гражданских прав, закрепленных в ст. 128 ГК. В соответствии же со ст. 1228 ГК автором произведения признается человек, творческим трудом которого такой результат был создан. Указанные законодатель-

ные положения порождают комплекс правовых вопросов, включающих: (а) возможность признания ИИ в качестве субъекта—создателя охраняемого результата; (б) установление круга лиц, подлежащих привлечению к ответственности за нарушения интеллектуальных прав, связанные с применением ИИ.

С.А. Милуков утверждает, что есть два подхода к определению произведения: 1) любой результат мыслительной деятельности; 2) результат, представляющий собой совокупность мыслей, идей и образов, которые имеют внутреннюю структуру, форму и содержание [Милуков С.А., 2023: 73]. Существование идеи в голове создателя, предшествующее ее выражению в объективной форме, Г.У. Лукина и Е.Ю. Куприна называют «замыслом» — творческой стадией, которая предшествует фиксации произведения [Лукина Г.У., Куприна Е.Ю., 2023: 13].

Понятие «творчество» неразрывно связано с понятием «оригинальность». При анализе законодательства разных правовых систем выделяются следующие подходы к определению понятия «оригинальность»:

— в Европейском союзе (далее — ЕС) интеллектуальные права распространяются только на произведения, являющиеся результатом собственного интеллектуального творчества автора⁴;

— в Канаде — на самостоятельные произведения с привлечением собственных навыков и суждений автора;

— в Великобритании — на произведения, созданные собственными знаниями автора, его усилиями, суждениями и трудом [Огородникова К.С., 2021: 61];

— в США минимальная «творческая искра» или «капля творчества» должны быть созданы самостоятельным трудом автора⁵.

⁴ В деле *Infopaq International A/S v. Danske Dagblades Forening* (Court of Justice. Fourth Chamber (2009)), касающемся правового режима обзоров периодических изданий, сформулирована позиция: правовая охрана объектов в качестве произведений предполагает установление их соответствия критерию собственного интеллектуального творчества автора. Суд констатирует, что подтверждением наличия собственного интеллектуального творения автора служат такие объективные элементы произведения, как его форма, метод представления содержания и специфика языкового выражения. Available at: URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62008CJ0005:EN:HTML> (дата обращения: 02.11.2025)

⁵ В деле *Feist Pubs., Inc. v. Rural Tel. Svc. Co., Inc.* (499 U.S. 340 (1991)) сформулирована позиция, согласно которой для признания произведения охраноспособным объектом авторского права необходимо наличие минимальной степени творческой индивидуальности, описываемой как «творческая искра». В обоснование приводится ситуация, когда два поэта, действуя независимо друг от друга, создают идентичные поэтические произведения. Каждое из произведений признается оригинальным результатом самостоятельного творческого

Таким образом, автором произведения признается исключительно человек, творческим трудом которого был создан охраняемый результат. Данная норма порождает комплекс вопросов в контексте применения ИИ, включая вопросы о возможности признания его в качестве создателя произведения и установления субъекта ответственности за нарушение исключительных прав. Пока же результаты, сгенерированные ИИ при отсутствии прямого творческого участия человека, исключаются из сферы действия правовой охраны.

3. Целесообразность наделения искусственного интеллекта правосубъектностью

В связи с неспособностью компьютерных систем к творческому выбору встает проблема определения объективных оснований квалификации минимально необходимого уровня творчества. Правовая неопределенность критериев охраноспособности результатов, создаваемых ИИ, обуславливает рассмотрение следующих юридически значимых вопросов:

- допустимость создания произведений, имитирующих индивидуальный стиль конкретного правообладателя;
- оценка оригинальности переработок и компиляций, синтезированных из существующих охраняемых объектов, и их разграничение с актами плагиата;
- установление круга надлежащих субъектов интеллектуальных прав на результаты, созданные с применением ИИ.

В целях проверки гипотезы о функциональном соответствии ИИ традиционному субъекту права полезно рассмотреть ситуацию, при которой пользователь, аналогично отношениям в рамках служебного произведения или договора авторского заказа, делегирует ИИ выполнение заданий в качестве исполнителя. В указанном случае творческий вклад человека ограничивается исходной стадией формирования технического задания, при этом установлена прямая корреляция между степенью детализации таких указаний и вероятностью признания авторства за физическим лицом. Соответственно, обратная зависимость проявляется в ситуациях минимальной спецификации заданий и высокой автономности функционирования искусственного интеллекта.

В свете характера возникновения правосубъектности юридических лиц, в отношении перспективных разработок в области «сильного» ИИ выдвигалась концепция новой категории — «электронного лица», способного охватывать сложные автономные системы. В связи с этим

труда и, следовательно, подлежит правовой охране. Available at: URL: <https://tile.loc.gov/storage-services/service/ll/usrep/usrep499/usrep499340/usrep499340.pdf> (дата обращения: 02.11.2025)

рассматривалось введение для соответствующих систем ограниченной правосубъектности *sui generis*, основанной на юридической фикции по аналогии с конструкцией юридического лица, однако данный подход сопряжен с проблемой необоснованного расширения системы правовых категорий. Указанная концепция не получила широкой поддержки — Европарламент констатировал нецелесообразность наделения ИИ статусом юридического лица, аргументируя это негативным воздействием на стимулирование творческой деятельности человеческой личности.

Аналогичная позиция о недопустимости признания правосубъектности за ИИ доминирует в большинстве современных правовых систем. В действующих правовых системах большинства юрисдикций ИИ не наделяется свойствами правосубъектности. Его функциональное назначение определяется преимущественно в качестве инструментария, обладающего способностью к анализу значительных массивов информации.

В процессе обработки данных ИИ демонстрируют имитацию рационального поведения, формулируя логически обоснованные выводы на основе входных параметров, установленных алгоритмов и предписаний. При этом сохраняется правовой риск ситуаций, при которых заинтересованные лица могут оказаться лишенными адекватных средств судебной защиты⁶.

Центральной проблемой выступает правовая неопределенность критериев охраноспособности результатов, создаваемых ИИ. Вследствие неспособности вычислительных систем к творческому выбору формируются значительные трудности в квалификации минимально необходимого уровня творчества, что порождает правовые последствия относительно установления оригинальности произведений, разграничения их с плагиатом и определения субъекта авторства.

Большинство правовых систем отклоняет концепцию наделения ИИ статусом юридического лица, ссылаясь на необходимость сохранения стимулов человеческого творчества. При этом отсутствие специального правового режима создает опасность невозможности охраны результа-

⁶ В деле *IceTV Pty Limited v. Nine Network Australia Pty Limited* (HCA 14 [2009]) Высший Суд Австралии подтвердил приверженность антропоцентрической парадигме авторского права, последовательно отрицая возможность признания правосубъектности за системами ИИ. Суд установил, что субъектом авторских прав на произведение, созданное с применением компьютерных технологий, признается исключительно человек, осуществивший комплекс необходимых действий для генерации результата. Суд сохранил верность традиционной доктрине индивидуального авторства, воздержавшись при этом от определения правообладателя. Available at: URL: <https://www.hcourt.gov.au/sites/default/files/assets/publications/judgment-summaries/2009/hca14-2009-04-22.pdf> (дата обращения: 02.11.2025)

тов, объективно тождественных результатам интеллектуальной деятельности человека.

Таким образом, в нынешних условиях ключ к решению указанных проблем имеет смысл искать в рамках сложившегося правового регулирования, поскольку системы ИИ пока не достигли уровня автономии, предполагающего полный разрыв с деятельностью человека.

4. Казуальный подход к определению защищенности произведения в зависимости от степени творческого вклада лица

Антропоцентрический подход к интеллектуальной собственности в целом является в значительной степени позицией, закрепленной как в *acquis communautaire* ЕС, так и в законодательстве об интеллектуальных правах членов ЕС [Iglesias M., 2021: 14], а также в практике Суда ЕС в отношении понятий труда, личности и т.д. (например, в решении Суда ЕС *Levola v. Smilde* (2018) [Papadopoulou A., 2021: 417]. В целях предотвращения дисфункции правового регулирования в отношении результатов, не созданных с непосредственным человеческим участием, и преодоления правовой неопределенности критериев охраноспособности результатов, созданных с применением ИИ, вырисовываются две альтернативы: а) модификация правового режима посредством смягчения императивных требований о необходимости установления авторства за человеком [Picht P.G., Thouvenin F., 2023: 138]; б) замена традиционного критерия творческого характера критерием инвестиций.

Критерий инвестиций, в отличие от концепции признания правосубъектности ИИ, не требует кардинального пересмотра законодательства, что свидетельствует о его большей реализуемости в краткосрочной перспективе. В условиях господствующей правовой парадигмы, в которой критерий творческого характера предполагает обязательное участие человека в создании интеллектуальной собственности, обеспечение правовой охраны обусловлено доказуемостью степени творческого вклада человека. Применительно к произведениям, сгенерированным исключительно ИИ, в большинстве юрисдикций отсутствуют основания их признания охраноспособными объектами.

Ключевым элементом правовой квалификации является установление факта творческого воздействия лица на сгенерированный контент. В частности, при модификации результата, созданного ИИ, физическое лицо обязано документально фиксировать вносимые изменения для обоснования авторства.

В рамках традиционного казуального подхода, предполагающего индивидуальную судебную оценку человеческого вклада в каждом случае,

основной проблемой выступает отсутствие унифицированной методики измерения соответствующего вклада. Указанное обстоятельство создает опасность чрезмерной зависимости от судебного усмотрения и формирует практику искусственного внесения правообладателями формальных правок в объекты, созданные ИИ (например, ретушь изображений или применение фильтров), с исключительной целью формального соответствия критериям охраноспособности⁷.

Таким образом, в рамках традиционного подхода охраноспособность возникает исключительно при доказуемости творческого участия человека, что провоцирует преднамеренную искусственную модификацию контента, сгенерированного ИИ. Ключевой проблемой выступает отсутствие унифицированной методики оценки творческого вклада и прева-лирование субъективного судебного усмотрения при разрешении споров.

5. Основания замены критерия охраноспособности для результатов, созданных искусственным интеллектом

Ключевой проблемой правовой регламентации ИИ выступает доминирующая в юриспруденции субъектно-объектная парадигма. В качестве альтернативной доктринальной основы предлагается заимствование категорий из философии М. Хайдеггера — *Dasein* (экзистенциальное бытие) и *Das Man* (безличное существование). В рамках указанной парадигмы ИИ квалифицируется как *Das Man*, демонстрирующий механическую симуляцию творческого процесса («*Das Man*-творчество»), лишенную бытийного измерения и не способную к экзистенциальной рефлексии. При этом физическое лицо (субъект правоотношений — пользователь, разработчик) интерпретируется как *Dasein* — первоисточник подлинного творческого потенциала («*Dasein*-творчество»).

Экстраполяция хайдеггеровских категорий *Dasein* и *Das Man* позволяет найти ключ к теоретическому обоснованию замены критерия творчества критерием инвестиций. *Dasein* «вопрошает» о собственном бытии, тогда как *Das Man* — механическая симуляция, лишенная онтологической рефлексии. И.А. Иванюшкин квалифицирует ИИ как лишенное всякой онтологии техническое нечто, что подчеркивает его принципиальную инородность по отношению к экзистенциальному измерению человеческого бытия [Иванюшкин И.А., 2019: 15].

⁷ Примером служит практика Бюро по авторским правам США. Бюро исходит из того, что созданные произведения не подлежат охране авторских прав в связи с отсутствием в них творческого вклада человека, однако оно закрепило авторские права на генератор изображений *Invoke* в связи с сочетанием в нем человеческого творчества с генерацией и документированием творческих приемов.

В рамках классической «субъект-объектной парадигмы» функциональная способность ИИ к совершению юридически значимых действий создает формальные предпосылки его квалификации в качестве субъекта права по аналогии с человеком, однако при переходе к категориям *Dasein*-принадлежности и *Das Man*-принадлежности обнаруживается, что «подлинной правосубъектностью» обладает исключительно человек. В юридических лицах, например, существуют социальные отношения между участниками (которые не являются имитацией), чего нельзя сказать об ИИ.

Когнитивная деятельность ИИ являет собой механическую симуляцию творческого акта, т.е. *Das Man*-творчество. *Dasein*-творчество должно охраняться в рамках традиционного режима авторско-правовой охраны, тогда как производное *Das Man*-творчество как имитация подлежит регламентации в рамках смежных прав. Как отмечает А.В. Пушкарев, синтез искусственного с естественным конституирует потенциальное бытие в качестве необходимой предпосылки актуализации творческих смыслов и онтологического гаранта творческого существования, что указывает на производный характер творческого потенциала интеллектуальных систем [Пушкарев А.В., 2017: 10].

Для правовой охраны результатов, создаваемых ИИ, критерий творческого характера подлежит замене критерием инвестиций. По аналогии с правовым режимом инвестиционных баз данных охрана результатов «*Das Man*-творчества» должна осуществляться в рамках института смежных прав, субъектом которых признается *Dasein*, осуществивший инвестирование ресурсов в создание результата.

Гипотеза, выдвинутая в настоящей статье, тем самым находит подтверждение: предоставление ИИ правосубъектности не является необходимым; наиболее оптимальным решением признается модификация механизма охраноспособности посредством изменения критерия и введение смежных прав в отношении результатов, созданных с применением ИИ. Следовательно, признание за ИИ правосубъектности *sui generis* в рамках его квалификации как субъекта права методологически несостоятельно. Точно так же применение правовых конструкций авторского заказа или служебного произведения к результатам, созданным ИИ, наделяет искусственный интеллект атрибутами исполнителя (работника), т.е. качествами субъекта правоотношений.

В процессе применения ИИ генерация результатов осуществляется посредством систем, функционирующих на основе алгоритмических и математических моделей, обрабатывающих информационные массивы. В создании конечных результатов интеллектуальной деятельности принимает участие множество субъектов: разработчик алгоритмической системы; организатор (или инвестор) проекта; пользователь, инициирующий процесс генерации; непосредственно система ИИ как инстру-

мент создания. Каждый из указанных участников процесса обладает потенциальным правом претендовать на статус правообладателя полученных результатов, что формирует комплексную правовую проблему разграничения их правомочий.

Анализ позволяет констатировать нецелесообразность признания за ИИ правосубъектности. В связи с этим рассматриваются правовые модели, исключающие наделение ИИ статусом самостоятельного субъекта правоотношений. Что касается разработчика алгоритмических решений, инвестора и пользователя, то трудность состоит в том, что каждый из них может претендовать на определенный объем правомочий в отношении созданного результата.

6. Квалификация «пользовательских соглашений» об использовании онлайн-сервисов, создающих результаты с помощью искусственного интеллекта

Ныне появляется все больше онлайн-сервисов, позволяющих создавать результаты, сопоставимые с результатами интеллектуальной деятельности человека, с помощью ИИ. При этом чаще всего документ, с которым пользователь знакомится перед началом использования указанных сервисов, именуется «пользовательским соглашением». В связи с этим встает проблема правовой квалификации «пользовательского соглашения». Отметим, что поскольку действующее законодательство не содержит указанной категории, к «пользовательскому соглашению» следует применять правила о том или ином договоре, поименованном в ГК⁸.

При изучении особенностей «пользовательского соглашения», сопряженного с цифровой средой, М.А. Рожкова отмечает: «Основная сущность любого цифрового сервиса именно в сервисе <...>, в любом случае речь будет идти о смешанных договорных конструкциях, или даже непоименованных» [Рожкова М.А., 2024: 128]. Следовательно, поскольку ценностное ядро любого онлайн-сервиса коренится в его сервисной составляющей, постольку особенность онлайн-сервисов обуславливает использование либо гибридных договорных схем, сочетающих элементы разных договоров, либо полностью оригинальных, законодательно не описанных договорных моделей (*contractus innominati*). М.А. Рожкова тем самым приходит к выводу, что правовая природа «пользовательского соглашения» может включать либо классический договор возмездного оказания услуг, либо смешанный договор, включающий элементы

⁸ Далее в тексте под «пользовательским соглашением» подразумевается исключительно «пользовательское соглашение» на использование онлайн-сервисов, позволяющих создавать результаты с помощью ИИ.

лицензионного договора и договора возмездного оказания услуг, что не является лицензионным договором в чистом виде.

Анализируя возможное отнесение «пользовательского соглашения» к лицензионным договорам, А.Е. Щукина указывает, что такая квалификация оправдана только при признании сервиса интеллектуальной собственностью. Если же договор фактически регулирует лишь доступ к сервису без передачи прав на результат интеллектуальной деятельности, он должен рассматриваться как договор возмездного оказания услуг, а точнее — услуг информационных⁹.

Развивая эту мысль, М.А. Рожкова отмечает: «Договор оказания информационных услуг <...> не относится к лицензионным соглашениям, а является разновидностью договора возмездного оказания услуг, определяющим признаком которого признается отсутствие материального результата действия или деятельности» [Рожкова М.А., 2024: 128]. Следовательно, договор оказания информационных услуг, указанный в п. 2 ст. 779 ГК — особый вид возмездного оказания услуг, а не лицензионный договор, поскольку его ключевым признаком является нематериальный характер результата осуществляемой деятельности.

Относительно понимания «пользовательского соглашения» как смешанного договора А.Е. Щукина отмечает: «Можно заключать договор смешанного типа, который будет в себе содержать и условия предоставления лицензии и условия оказания услуг»¹⁰. Судебная практика подтверждает указанную позицию¹¹. П. 47 Постановления Пленума Верховного Суда Российской Федерации (далее — ВС) от 25.12.2018 № 49 указывает, что при правовой квалификации соглашения в соответствии с п. 2 и 3 ст. 421 ГК следует учитывать сущность правового регулирования соответствующих обязательств.

При этом формальные аспекты (наименование договора, обозначение сторон, терминология, используемая для описания исполнения и т.п.) не имеют определяющего значения. Е.Б. Подузова отмечает: «Помимо существенных условий <...> в [„пользовательском соглашении“] должны содержаться условия о порядке предоставления и обработки

⁹ Щукина А.Е. Пользовательское соглашение: лицензионный договор vs договор оказания услуг // Zakon.ru. 2020. Available at: URL: https://zakon.ru/blog/2020/06/18/polzovatel'skoe_soglasenie_licenzionnyj_dogovor_vs_dogovor_okazaniya_uslug (дата обращения: 02.11.2025)

¹⁰ Там же.

¹¹ См.: Постановление Арбитражного суда Московского округа от 18.06.2015 № Ф05-7093/2015 по делу № А40-91072/14. Available at: URL: https://kad.arbitr.ru/Document/Pdf/277fdd53-f30b-4de4-a282-732bc448297e/cab5453e-c3de-4d99-bdf3-5d162236b2e0/A40-91072-2014_20150618_Reshenija_i_postanovlenija.pdf?isAddStamp=True (дата обращения: 02.11.2025)

информации пользователей с помощью технологий искусственного интеллекта, <...> условия о правовом режиме такой информации» [Подузова Е.Б., 2023: 75].

В качестве вывода на первый взгляд целесообразно признать гибридную природу «пользовательских соглашений», что обусловлено особенностями функционирования онлайн-платформ, сочетающих оказание и услуг и генерацию результатов интеллектуальной деятельности. Кажется очевидным, что использование сервисов, основанных на генеративном ИИ, одновременно включает элементы лицензионного договора и договора возмездного оказания услуг.

Между тем необходимо помнить, что в России результаты, созданные с помощью технических средств в отсутствие творческого характера деятельности человека, объектами авторского права не являются¹². В силу позиции ВС независимо от того, что будет указано в «пользовательском соглашении», результаты по причине отсутствия творческого вклада человека ввиду использования автоматизированной генерации без человеческого вмешательства будут признаваться неохраноспособными. Следовательно, на такие результаты будет распространяться правовой режим свободного использования, и никто не сможет получить интеллектуальные права на них.

Таким образом, в России в рамках текущего правового регулирования «пользовательское соглашение» будет являться исключительно договором возмездного оказания услуг или непоименованным в ГК договором безвозмездного оказания услуг. В данном случае лицензионные правоотношения не возникают, поскольку отсутствие охраноспособности и правообладателя у результатов, созданных искусственным интеллектом, исключает возникновение таких правоотношений. Вместе с тем при внесении в законодательство предлагаемых автором настоящей статьи изменений, связанных с введением смежно-правовой охраны результатов, созданных ИИ, рассмотренные выше «пользовательские соглашения» будут квалифицироваться в качестве смешанного договора и тем самым позволят лицензировать смежное право.

Заключение

Искусственный интеллект выполняет коммуникативную функцию между создателями исходных данных и субъектом, формулирующим целенаправленный запрос. Наиболее релевантной правовой аналогией в

¹² Пункт 10 постановления Пленума Верховного Суда Российской Федерации от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации». Available at: URL: <https://www.vsrp.ru/documents/own/27773/> (дата обращения: 02.11.2025)

данном контексте выступает правовой режим баз данных, однако ИИ демонстрируют более высокий уровень функциональности, генерируя производные данные на основе восприятия исходной информации, без необходимости модификации концепции правосубъектности. По мнению автора, при квалификации правового режима результатов, созданных с применением ИИ, критерий творческого характера подлежит замене критерием инвестиции по аналогии с правовой охраной инвестиционных баз данных.

В рамках данной работы выделено два вида «творчества»:

«*Dasein*-творчество» — процесс, при котором результат первоначально формируется в сознании человека-творца, получая правовое признание через критерий творческого характера и охрану в рамках авторско-правового режима.

«*Das Man*-творчество» — процесс генерации результата посредством математической симуляции интеллектуальной деятельности, подлежащий правовой квалификации через критерий инвестиций с охраной в рамках института смежных прав.

Субъектом смежных прав на такие результаты должен признаваться *Dasein*, обеспечившее организационные, технические и инвестиционные условия их создания. Здесь ИИ выполняет роль «информационного посредника», обрабатывая массивы данных и обеспечивая коммуникацию между субъектами, однако, в отличие от последних, он лишен способности к экзистенциальной рефлексии. Эмпирически установлено, что на производительность ИИ негативно влияет отсутствие человеческого участия в коммуникативной цепи.

Следовательно, ранее выдвинутая гипотеза находит подтверждение: для результатов *Das Man*-творчества целесообразна замена критерия творчества критерием инвестиций. Параллельно требуется совершенствование нормативного регулирования коммерческого использования систем ИИ, включая вопросы использования генерируемых результатов и распределения доходов между правообладателями [Watiktinnakorn С., 2023: 9].

Результаты, сгенерированные с применением ИИ, обладают потенциалом непреднамеренного нарушения исключительных прав третьих лиц. Субъект, использующий систему ИИ и получающий соответствующий результат, как правило, признается ответственным лицом в случае причинения ущерба. ИИ должен функционировать в качестве инструмента расширения человеческих возможностей, а не их ограничения.

В процессе работы проверен тезис: замена критерия творчества критерием инвестиции — оптимальное решение в рамках регулирования в русле действующего права. Экстраполяция философской категории *Das Man* Хайдеггера на правовую природу ИИ позволила сформулировать

философско-правовое обоснование для замены критерия творчества критерием инвестиций. Установлено, что правовая охрана посредством предоставления режима смежных прав подлежит распространению на результаты, генерируемые системами ИИ, которые в рамках концепции данной работы определяются как «*Das Man*-творчество».

Немаловажен и вопрос срока правовой охраны смежного права на результат, созданный ИИ:

В случае с результатами, созданными творческим трудом человека, где ИИ использовался лишь в качестве инструмента, срок правовой охраны должен быть приравнен к сроку действия исключительного права на произведение и действовать в течение всей жизни создателя и 70 лет после.

В случае с результатами, созданными ИИ автономно, без творческого участия человека, срок правовой охраны должен быть приравнен к сроку действия исключительного права изготовителя базы данных и действовать в течение 15 лет.

Таким образом, предлагается заменить критерий творчества критерием инвестиции для охраны результатов, созданных ИИ. Искусственный интеллект в любом случае рассматривается как инструмент, а смежное право на его результаты должно принадлежать человеку, вложившему ресурсы в создание такого результата. Данное решение технически обосновано и оптимально, поскольку оно снижает правовую неопределенность и не требует кардинальных изменений в законодательстве.



Список источников

1. Балашова А.И. Правовой режим результатов деятельности искусственного интеллекта: единство и дифференциация подходов. Журнал Суда по интеллектуальным правам. 2023. № 3. С. 190–206.
2. Иванюшкин И.А. Искусственный интеллект: перспективы социокультурных трансформаций. Вестник Московского городского педагогического университета. Философские науки. 2019. № 4. С. 10–20.
3. Калятин В.О. Определение субъекта прав на результаты интеллектуальной деятельности, созданные с использованием искусственного интеллекта и его влияние на развитие гражданского законодательства. Право. Журнал Высшей школы экономики. 2022. Том 15. № 4. С. 24–50.
4. Лукина Г.У., Куприна Е.Ю. Рассуждение о понятии «художественный замысел». Художественная культура. 2023. № 4. С. 12–33.
5. Милюков С.А. Объекты, созданные с использованием искусственного интеллекта как объекты авторских и смежных прав. Журнал Суда по интеллектуальным правам. 2025. №1. С. 63–73.
6. Огородникова К.С. Проблема оригинальности произведения в авторском праве. Вопросы российского и международного права. 2021. № 11. С. 60–67.

7. Подузова Е.Б. Пользовательское соглашение, соглашение о конфиденциальности: особенности содержания в контексте использования технологий искусственного интеллекта. Актуальные проблемы российского права. 2023. № 2. С. 71–78.
8. Пушкарев А.В. Философские основания искусственного интеллекта: автореф. дис. ... к. ф. н. Уфа, 2017. 19 с.
9. Рожкова М.А. О различиях между лицензионным договором и пользовательским соглашением. Журнал Суда по интеллектуальным правам. 2024. № 4. С. 121–133.
10. Русаков С.С. Ранний Хайдеггер и проблема соотношений субъекта и Dasein. Известия Тульского государственного университета. Гуманитарные науки. 2024. С. 143–151.
11. Щукина А.Е. Пользовательское соглашение: лицензионный договор vs договор оказания услуг. Available at: URL: https://zakon.ru/blog/2020/06/18/polzovatelskoe_soglashenie_licenzionnyj_dogovor_vs_dogovor_okazaniya_uslug (дата обращения: 03.11.2025).
12. Iglesias M. Intellectual Property and Artificial Intelligence. A Literature Overview. Luxembourg: Publications Office of EU, 2021. Available at: URL: <https://publications.jrc.ec.europa.eu/repository/handle/JRC119102> (дата обращения: 03.11.2025)
13. Papadopoulou A. Creativity in Crisis: Are the Creations of Artificial Intelligence Worth Protecting? Journal of Intellectual Property, Information Technology and Electronic Commerce Law. 2021, no. 3, pp. 408–418.
14. Picht P.G., Thouvenin F. AI and IP: Theory to Policy and back again — Policy and Research Recommendations at the Intersection of Artificial Intelligence and Intellectual Property. International Review of Intellectual Property and Competition Law. 2023, vol. 54, no. 4, pp. 123–145.
15. Watiktinnakorn C. Blurring the Lines: How AI is Redefining Artistic Ownership and Copyright. Discover AI, 2023, pp. 1–10.

Информация об авторе:

П.К. Пакшин — аспирант.

Статья поступила в редакцию 03.11.2025; одобрена после рецензирования 15.12.2025; принята к публикации 15.12.2025.

Научная статья

JEL: K00

УДК: 378.1:004.8:174

DOI:10.17323/2713-2749.2026.1.49.70

Этическое регулирование применения искусственного интеллекта в университетском образовании



**Саид Саидахрарович Гулямов¹,
Исламбек Рустамбекович Рустамбеков²**

^{1, 2} Ташкентский государственный юридический университет, Узбекистан
100047, Ташкент, ул. Сайилгох, 35,

¹ said.gulyamov1976@gmail.com, <https://orcid.org/0000-0002-2299-2122>

² i.rustambekov@tsul.uz, <https://orcid.org/0000-0002-8869-8399>



Аннотация

Статья содержит всесторонний анализ Кодекса этики искусственного интеллекта (ИИ) в образовании, разработанного в Ташкентском государственном юридическом университете (TSUL). Кодекс знаменует заметное отклонение от устоявшихся запретительных подходов к управлению ИИ в высшем образовании, основываясь на принципе приоритета образования и наставничества над ограничительными мерами. Через детальное рассмотрение тридцати одной статьи в четырех разделах (общие положения, использование ИИ в образовательном процессе, использование ИИ в исследовательской деятельности, управление и надзор), дополненных методологическими критериями оценивания ИИ и структур управления, авторы раскрывают намеченную Кодексом комплексную систему, ставящую образование выше запретов при сохранении академической целостности. Анализ выявляет инновационные механизмы управления, включая Советы по этике ИИ (преподаватели, технические специалисты и студенты) и функции, протоколы комплексной оценки рисков, адаптивные стратегии поэтапного внедрения и методологические подходы к оцениванию академической работы с помощью ИИ, основанные на параллельной системе анализа соотношения человеческого участия и помощи со стороны ИИ. Кодекс опирается на международные стандарты, включая Реко-

мендацию ЮНЕСКО по этике искусственного интеллекта, принципы GDPR и ценности Международного центра академической честности, адаптируя их к специфике образовательного контекста. Авторы рассматривают как намеченные Кодексом потенциальные преимущества образовательных учреждений (развитие компетенций ИИ, подготовка к профессиональной среде, упрочение критического мышления), так и значительные проблемы внедрения Кодекса, требующие тщательного рассмотрения (ресурсные требования, управление изменениями, методологические вызовы верификации работ, выполняемых с помощью ИИ). Особое внимание уделяется вопросам масштабирования модели в учреждениях с различными уровнями ресурсных возможностей, механизмам международного сотрудничества и обеспечению равного доступа к технологиям. Значимость Кодекса заключается в создании детальной, практически применимой модели для образовательных учреждений по всему миру, решающих проблемы ответственной интеграции ИИ при сохранении академических этических стандартов и человекоцентричного подхода к образованию в условиях технологического прогресса.



Ключевые слова

искусственный интеллект; образовательная этика; академическая честность; управление; высшее образование; технологическая политика; человекоцентричное образование; Совет по этике.

Для цитирования: Гулямов С.С., Рустамбеков И.Р. Этическое регулирование применения искусственного интеллекта в университетском образовании // Вопросы права в цифровую эпоху. 2026. № 1. С. 49–70. DOI:10.17323/ 2713-2749.2026.1.49.70

Введение

Интеграция искусственного интеллекта (далее — ИИ) в образовательные системы знаменует трансформацию высшего образования, кардинально изменяя способы передачи знаний и природу процессов обучения¹. По мере того, как технологии ИИ становятся все более развитыми и доступными, образовательные учреждения во всем мире сталкиваются с вызовами в балансировании инноваций с академической целостностью, благополучием студентов и этической ответственностью, одновременно готовя студентов к тем профессиональным средам, в которых компетенции в области ИИ становятся важными.

¹ Трапезников В., Зиновьева Е. Нейросети и генеративный ИИ в высшем образовании: международный опыт и российская практика. Российский совет по международным делам. Available at: URL: https://russiancouncil.ru/analytics-and-comments/analytics/neyroseti-generativnyy-ii-v-vyshhem-obrazovanii-mezhdunarodnyy-opyt-i-rossiyskaya-praktika/?sphrase_id=150634182 (дата обращения: 28.01.2026)

Традиционные ответы на технологии в образовании часто базируются на запретительных мерах, что создает напряжение на стыке технологических нововведений и привычных образовательных ценностей². Этот подход часто оказывался неадекватным, поскольку он не признает ни потенциала новых технологий, ни необходимости подготовки студентов к технологически интегрированным профессиональным средам, где компетентность в рабочих средах с помощью ИИ становится все более ценной [Кошель А.С. и др., 2025: 58].

Кодекс этики ИИ в образовании, разработанный в Ташкентском государственном юридическом университете, предлагает переход от запретительного к образовательно-ориентированному управлению искусственным интеллектом в академических условиях³. Полноценно со всеми документами можно ознакомиться на официальном сайте университета (www.tsul.uz). Этот всеобъемлющий документ, включающий 31 статью в четырех разделах, сопровождается стратегиями внедрения, методологическими критериями и структурами управления. Он означает систематизированную попытку создать этическую систему управления ИИ в образовательных учреждениях, которая ставит наставничество и развитие навыков выше ограничительных мер.

Данная статья содержит детальный анализ Кодекса этики ИИ и сопровождающих документов, исследуя его основополагающие принципы, операционные рамки, методологические подходы и последствия через систематический обзор каждого компонента. Исследование обращается к пробелам в литературе об управлении ИИ, образуя при этом реализуемое руководство для образовательных учреждений, стремящихся ответственно интегрировать технологии ИИ.

1. Исторический контекст и этика образовательного искусственного интеллекта

1.1. Ограничения запретительных подходов

Образовательные учреждения исторически отвечали на разрушительные технологии различной степенью сопротивления и постепенного приспособления, в общем следуя паттернам запретительных подходов. Появление интернет-технологий в 1990-х годах сначала вызвало опасения академических нарушений, что привело многие учреждения к ограничению интернет-доступа в образовательных условиях. Аналогично, распространение платформ социальных медиа в 2000-х годах поро-

² Digital learning and ICT in education. Available at: URL: https://digital-strategy.ec.europa.eu/en/policies/digital-learning?utm_source=chatgpt.com (дата обращения: 01.12.2025)

³ TSUL AI Ethics Code in Education (2024). Tashkent State University of Law.

дило опасения относительно «отвлечения внимания» студентов и «неподходящего контента», что привело к широкому блокированию этих платформ. Внедрение мобильных устройств создало дополнительные волны запретов, пытающихся поддерживать традиционные основы учебного класса [Rodgers D., 2012: 88].

Каждая технологическая волна следовала похожими траекториями: первоначальный запрет, основанный на опасениях рисков: постепенное признание образовательного потенциала; неохотное приспособление; в конечном итоге — интеграция, когда учреждения признавали как потребность в ограничениях и запретах, так и необходимость подготовки студентов к технологически интегрированным профессиональным средам. Однако эти переходы обычно происходили в течение длительного времени, поэтому учреждения, поддерживающие запретительные подходы, часто ставили своих студентов в невыгодное положение относительно тех, кто принимал продуманные стратегии интеграции.

Пандемия COVID-19 ускорила цифровую трансформацию в образовании, сжав постепенные изменения в быструю адаптацию⁴. Эта трансформация раскрыла как потенциал технологически улучшенного образования, так и назревшую необходимость формирования этических рамок масштабного внедрения технологий. Учреждения, которые ранее инвестировали в цифровые педагогики и этические рамки для использования технологий, были лучше подготовлены к поддержанию качества образования во время перехода, в то время как полагавшиеся на запретительные подходы оказались менее подготовленными к технологически опосредованному образованию.

1.2. Вызовы генеративного ИИ в образовательных контекстах

Появление систем генеративного ИИ, особенно больших языковых моделей, создает вызовы, отличающиеся от предыдущих образовательных технологий в нескольких измерениях. В отличие от предыдущих технологий, которые в первую очередь влияли на доступ к информации и коммуникацию, системы генеративного ИИ могут производить контент, который напоминает созданную человеком работу в академических дисциплинах, поднимая вопросы об авторстве, оригинальности, адекватности оценки и природе обучения⁵.

⁴ European Commission. Directorate-General for Education, Youth, Sport and Culture. PPMI Group: Farnell T., Skledar M. et al. The impact of COVID-19 on higher education. A review of emerging evidence. Luxembourg, 2021. Available at: URL: <https://data.europa.eu/doi/10.2766/069216> (дата обращения: 01.12.2025)

⁵ Руководство по использованию генеративного искусственного интеллекта в образовании и научных исследованиях. Available at: URL: <https://unesdoc.unesco.org/ark:/48223/pf0000389639> (дата обращения: 01.12.2025)

Способность современных систем ИИ производить последовательный, контекстуально подходящий текст по широкому кругу предметов делает прежние механизмы обнаружения плагиата недостаточными, поскольку они были разработаны для идентификации копирования из существующих источников, а не генерации нового контента [Weber-Wulff D., 2023: 15]. Быстрое улучшение способностей ИИ означает, что статичные подходы быстро устаревают, требуя адаптивных рамок управления, которые могут эволюционировать с технологическими способностями при поддержании этических стандартов⁶. Потенциальные преимущества обучения с помощью ИИ значительны и документированы, что делает общие запреты контрпродуктивными [Luckin R., 2016: 23].

Исследования показывают, что студенты университетов широко используют технологии ИИ в своей работе независимо от институциональных политик, с паттернами использования, варьирующимися по дисциплинам, академическим уровням и культурным контекстам [Perkins M., 2023: 1]. Исследования студентов обнаружили, что значительный их процент экспериментировал с инструментами письма ИИ, многие отмечали разрыв между институциональными ограничениями и профессиональными ожиданиями [Johnston H., 2024: 1]. Это подчеркивает ограниченность запретительных подходов и негативность их результатов, поскольку они создают среды, где студенты развивают компетенции ИИ без этического руководства или институциональной поддержки.

1.3. Правовой и регулятивный контекст

Разработка Кодекса этики ИИ происходит в правовой и регулятивной среде, которая включает международные рамки и национальные политические инициативы. Кодекс согласуется с Рекомендацией ЮНЕСКО об этике искусственного интеллекта 2021 года; она обозначает глобальные принципы развития ИИ при признании суверенитета государств-членов в его внедрении⁷. Это согласование полезно, поскольку Кодекс переводит широкие принципы ЮНЕСКО в руководства для образовательных контекстов.

Ссылки Кодекса на Всеобщую декларацию прав человека (1948)⁸, особенно на ст. 26 о признании права на образование и ст. 19 о защи-

⁶ STOA. 2020. The ethics of artificial intelligence: Issues and initiatives. European Parliament Research Service. Available at: URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU%282020%29634452_EN.pdf (дата обращения: 03.12.2025)

⁷ Рекомендации ЮНЕСКО по этике искусственного интеллекта. 23.11.2021. Available at: URL: <https://unesdoc.unesco.org/ark:/48223/pf0000385082> (дата обращения: 01.12.2025)

⁸ Всеобщая декларация прав человека. Available at: URL: <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (дата обращения: 03.12.2025)

те свободы выражения, устанавливают его основание в международном праве прав человека. Это обоснование позиционирует этику ИИ в образовании как вопрос прав человека с последствиями для доступа к образованию, равенства и человеческого достоинства.

На национальном уровне Кодекс включает ссылки: на Конституцию Узбекистана⁹ (прежде всего на ст. 51 о праве на образование), на Закон об образовании¹⁰, на Стратегию развития нового Узбекистана на 2022–2026 годы¹¹, на стратегию «Цифровой Узбекистан-2030»¹² и на Концепцию развития системы высшего образования до 2030 года¹³. Эта интеграция демонстрирует понимание составителями Кодекса отношений между международными принципами и национальными требованиями к внедрению ИИ.

Приверженность Кодекса политической нейтральности при уважении национального суверенитета отражает признание того, что в то время как этические принципы для ИИ в образовании выигрывают от глобальной координации, их внедрение должно быть адаптировано к национальным образовательным традициям, правовым системам и культурным контекстам.

2. Основополагающие принципы

2.1. Сфера применения и цели

Открывающая Кодекс статья устанавливает его основополагающую цель: Кодекс «устанавливает этические принципы и руководящие указания для ответственного использования искусственного интеллекта в образовательной деятельности» (ст. 1.1). Эта формулировка отличает Кодекс от чисто запретительных актов, позиционируя его как руководя-

⁹ Конституция Узбекистана (08.12.1992 с изм. от 30.04.2023). Available at: URL: <https://lex.uz/docs/6445147> (дата обращения: 01.12.2025)

¹⁰ Закон Республики Узбекистан от 23.09.2020 № ЗРУ-637 об образовании. Available at: URL: <https://lex.uz/ru/docs/5013009> (дата обращения: 01.12.2025)

¹¹ Указ Президента Республики Узбекистан от 28.01.2022 № УП-60 о стратегии развития нового Узбекистана на 2022–2026 годы. Available at: URL: <https://lex.uz/ru/docs/5841077> (дата обращения: 01.12.2025)

¹² Указ Президента Республики Узбекистан от 05.10.2020 № УП-6079 об утверждении Стратегии «Цифровой Узбекистан-2030» и мерах по ее эффективной реализации. Available at: URL: <https://lex.uz/docs/5031048> (дата обращения: 03.12.2025)

¹³ Указ Президента Республики Узбекистан от 08.10.2019 № УП-5847 об утверждении Концепции развития системы высшего образования Республики Узбекистан до 2030 года. Available at: URL: <https://lex.uz/ru/docs/4545887> (дата обращения: 03.12.2025)

щий документ, направленный на обеспечение этического и ответственного подхода к интеграции ИИ в образовательный процесс.

Цели, сформулированные в ст. 1.2 — максимизация образовательного потенциала ИИ при защите человеческого достоинства, воспитание компетенций ИИ и обеспечение равного доступа к образовательным возможностям—отражают понимание многогранных последствий ИИ для образовательных учреждений. Эти цели структурированы, чтобы избежать ложных дихотомий между технологическим прогрессом и этической ответственностью, позиционируя их как дополнительные элементы образовательного превосходства.

Статья 1.3 содержит основополагающий принцип Кодекса: «Образование и наставничество эффективнее запретительных мер в достижении этического использования ИИ». Этот принцип означает отход от политизированных подходов и устанавливает философское основание для рамок. Вместо рассмотрения ИИ как угрозы, требующей сдерживания, Кодекс толкует его как инструмент, требующий мастерства руководства и развития навыков. Этот подход отражает исследования поведения и принятия технологий, указывающие, что стратегии позитивного вовлечения часто плодотворнее санкций в достижении соответствия этическим стандартам.

2.2. Всеобъемлющее институциональное покрытие

Сфера применения статьи обращена к ограничению политик ИИ, которые часто применяются только к студентам или к одному их направлений академической деятельности. Охватывая «всех членов академического сообщества: студентов, преподавателей, исследователей, административный персонал и внешних партнеров» (ст. 2.2), Кодекс исходит из того, что этическое использование ИИ требует общеинституциональной приверженности, а не изолированного соответствия групп.

Инклюзивный подход отражает признание того, что этика ИИ в образовании не может быть достигнута только политикой, ориентированной на студентов. Преподаватели, использующие ИИ в исследованиях и преподавании, должны понимать этические практики. Административный персонал, развертывающий системы ИИ, должен обеспечивать работу этих систем в соответствии с этическими принципами. Внешние партнеры, оказывающие услуги ИИ, должны согласовывать свои действия с институциональными ценностями. Всеобъемлющее покрытие Кодекса обеспечивает последовательные этические стандарты во всех этих взаимодействиях.

Положение об адаптации к «различным образовательным контекстам при поддержании основных этических принципов» (ст. 2.3) демонстрирует понимание институционального разнообразия. Вместо навязывания жестких требований Кодекс предлагает гибкие рамки, по-

звolyающие контекстуальную адаптацию при поддержании этических стандартов. Этот баланс отвечает на вызовы предыдущих усилий по управлению технологиями, которые часто терпели неудачу из-за чрезмерной жесткости или повышенной гибкости, подрывающей последовательные стандарты¹⁴.

2.3. Определения

Статья 3 трактует ключевые концепции, которые часто не имеют точности в документах управления ИИ. Определение ИИ как «систем, способных обрабатывать данные и информацию способами, которые включают элементы рассуждения, обучения, восприятия, предсказания, планирования или контроля» (ст. 3.1), согласуется с современными исследованиями ИИ при сохранении доступности для нетехнических аудиторий¹⁵.

Определение академической честности (ст. 3.2) ссылается на ценности Международного центра академической честности¹⁶: честность, доверие, справедливость, уважение, ответственность и мужество. Это обоснование академической честности обеспечивает преимущество с образовательными ценностями при признании их применения в контекстах с усилением ИИ. Вместо рассмотрения ИИ как чего-то фундаментально разрушительного для академической честности, Кодекс позиционирует его как новый контекст, в котором должны применяться установленные ценности.

Концепции «участия человека» и «значимого человеческого вклада» (ст. 3.3 и 3.4) устанавливают различия, которые обращаются к опасениям относительно роли ИИ в образовании. Эти определения предотвращают рассмотрение ИИ как полного решения или полной угрозы, а позиционируя ИИ как инструмент, требующий продуманного человеческого вовлечения. Определение значимого человеческого вклада как «интеллектуальной деятельности, которая включает формулировку задач, критический анализ результатов, окончательное принятие решений и творческое развитие идей», создает руководство для оценки того,

¹⁴ Gai P., Kemp M. et al. Regulatory complexity and the quest for robust regulation. Reports of the Advisory Scientific Committee No. 8, 2019. European Systemic Risk Board. Available at: URL: https://www.esrb.europa.eu/pub/pdf/asc/esrb.asc190604_8_regulatorycomplexityquestrobustregulation~e63a7136c7.en.pdf (дата обращения: 01.12.2025)

¹⁵ Например, с определением согласно Regulation (EU) 2024/1689 on laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), Article 3(1). Available at: URL: <https://artificialintelligenceact.eu/article/3/> (дата обращения: 03.12.2025)

¹⁶ International Center for Academic Integrity, n.d. Available at: URL: <https://academicintegrity.org/> (дата обращения: 02.12.2025)

поддерживают ли конкретные использования ИИ подходящую человеческую агентность.

2.4. Восемь основополагающих принципов

Восемь принципов составляют философское ядро подхода Кодекса к управлению ИИ. Они согласуются с этическими руководящими принципами по использованию ИИ и данных в обучении преподавателей, разработанными Европейской комиссией в 2022 году¹⁷. Эти принципы заслуживают рассмотрения как индивидуально, так и совокупно.

Образование выше запретов (4.a). Принцип бросает вызов традиционным политическим подходам, которые ставят избегание рисков выше развития возможностей. Исследования технологий в образовании убеждают, что запретительные подходы часто оказываются бесплодными, порождают антагонистические отношения при неспособности развивать компетенции, необходимые для этического использования технологий. Принцип отражает признание того, что этическое использование ИИ — сложная компетенция, требующая развития, а не принуждения или ограничения.

Человекоцентричный подход (4.b). Принцип «ИИ укрепляет человеческий интеллект, но не заменяет его», устраняет опасения относительно технологического смещения при признании потенциала ИИ. Этот принцип рассматривает ИИ как вспомогательную технологию, разработанную для развития человеческих способностей, а не как автономную технологию, работающую независимо от человеческого надзора. Человекоцентричный подход требует, чтобы внедрение ИИ поддерживало значимое участие человека в принятии решений и в творческом развитии.

Прозрачность и подотчетность (4.c). Прозрачное раскрытие использования ИИ посвящено опасениям насчет обмана при обучении паттернам использования. Требования прозрачности служат множественным функциям: это предотвращение неправильного представления работы с помощью ИИ, обеспечение учреждениям понимания паттернов использования и создание возможностей обмена достижениями. Механизмы подотчетности обеспечивают, что индивидуумы остаются ответственными за работу, даже когда принимают помощь ИИ.

Академическая честность (4.d). Интеграция ИИ в рамки академической честности предотвращает создание параллельных этических систем при

¹⁷ European Commission. 2022, October 25. Ethical guidelines on the use of artificial intelligence and data in teaching and learning for educators. European Education Area. Available at: URL: <https://education.ec.europa.eu/news/ethical-guidelines-on-the-use-of-artificial-intelligence-and-data-in-teaching-and-learning-for-educators> (дата обращения: 04.12.2025)

признании вклада технологии. Этот принцип позиционирует ИИ как новый контекст, в котором должны применяться установленные ценности, а не как фундаментально разрушительный для академической честности.

Справедливость (4.e). Приверженность недискриминации и равным возможностям отражает опасения предвзятости ИИ и неравенства в образовании. Справедливость требует, чтобы системы ИИ не создавали или не увековечивали недостатков на основе защищенных характеристик при поддержании равного доступа к технологическим способностям.

Пропорциональность (4.f). Требование, чтобы использование ИИ было пропорционально образовательным целям, предотвращает как зависимость от ИИ, так и неиспользование технологических способностей. Пропорциональность требует соответствия интенсивности использования ИИ целям обучения и потребностям развития.

Устойчивость (4.g). Соображения экологической и социальной ответственности признают обширные социальные последствия ИИ. Принцип устойчивости требует рассмотрения вероятных экологических затрат и проработки социальных последствий применения систем ИИ.

Прозрачность и объяснимость (4.h). Требование контекстуально-подходящей прозрачности обращается к техническим вызовам при поддержании доступности ИИ. Этот принцип напоминает, что различные заинтересованные стороны требуют различных уровней объяснения о системах ИИ.

2.5. Права и обязанности

Статьи 5 и 6 устанавливают параметры прав и обязанностей, формируя тем самым баланс между индивидуальной автономией и коллективными обязательствами. Рамка прав ст. 5 обращается к группам заинтересованных сторон при поддержании универсальных принципов. Право на «равный доступ к образовательным возможностям независимо от уровня владения технологией ИИ» (ст. 5.1) обращается к опасениям цифрового разрыва, который способен усугубить существующее неравенство.

Права студентов (ст. 5.2) включают: руководство по использованию ИИ, наставничество по развитию компетенций, справедливую оценку работы с ИИ и поддержку доступа студентов к технологиям независимо от экономических обстоятельств. Права преподавателей (ст. 5.3) включают академическую свободу в процессе интеграции ИИ, возможности профессионального развития, участие в разработке и защите интеллектуальной собственности.

Обязательства в ст. 6 подчеркивает общую ответственность за этическое использование ИИ при избегании карательного подхода. Рекомендация «активного развития компетенций ИИ» в сочетании с положением о

том, что «отсутствие таких компетенций не может служить основанием дискриминации» (ст. 6.3) демонстрирует понимание переходных вызовов, с которыми сталкиваются образовательные сообщества.

2.6. Операционные основы

Данные статьи устанавливают правила защиты данных, недискриминации, академической свободы и международного сотрудничества. Положения ст. 7 о защите данных согласуются с международными стандартами, включая принципы GDPR¹⁸. Пункт о недискриминации ст. 8 обращается к опасениям предвзятости ИИ при установлении параметров институциональной поддержки. Пункт о защите академической свободы в ст. 9 требует, чтобы интеграция ИИ служила образовательным целям, а не ограничивала их. Положения о международном сотрудничестве ст. 10 отражает признание того, что вызовы управления ИИ выходят за институциональные границы при уважении национального суверенитета.

3. Искусственный интеллект в образовательной деятельности: рамки внедрения

3.1. Подходы к интеграции и оценке

Эти статьи переводят основополагающие принципы в руководство образовательной деятельности. Они обращены к вызовам преподаванию, порожденным интеграцией ИИ, при сосредоточении внимания на результатах обучения. Интеграционный контекст ст. 11 подчеркивает приоритет педагогической целесообразности перед технологическими возможностями, требуя, чтобы внедрение ИИ было «методологически подходящим, прозрачным, взвешенным и этически оправданным». Акцент на измерении «результатов обучения, а не паттернов использования ИИ» отражает понимание того, что ценность технологии лежит в ее образовательном воздействии, а не в ее присутствии (ст. 11.1).

3.2. Развитие студентов

Упор ст. 12 на грамотности студентов в области ИИ означает повышенное внимание к данному компоненту, часто упускаемому из виду при управлении ИИ. Критерии компетенций включают техническое понимание, этическую осведомленность, навыки критической оценки и способности творческого применения. Этот подход признает, что интеграция ИИ требует активного вовлечения студентов, а не пассивного потребления ими контента, генерируемого ИИ.

¹⁸ General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 (2016). Available at: URL: <https://gdpr-info.eu/> (дата обращения: 01.12.2025)

Человеко-ориентированная образовательная модель, установленная в ст. 12, строится на трех компонентах: это развитие технологической грамотности, существенное человеческое интеллектуальное участие и соблюдение стандартов академического качества (ст. 12.1).

3.3. Академическая честность в контекстах с помощью ИИ

Статьи 13 и 14 посвящены поддержанию академической честности при разрешении применения ИИ. Требования к документации ст. 13 намечают практический подход к прозрачности, обеспечивающий обучение при поддержании отчетности. Требование, чтобы студенты документировали инструменты и методы использования, их роль в достижении результатов и принятие ответственности за конечный продукт (ст. 13.2) создает границы ожиданий вместо общих запретов.

Ст. 14 посвящена критической оценке потенциальной зависимости студентов от систем ИИ. Подобная оценка результатов ИИ согласно ст. 14.2 включает проверку фактов, оценку логической последовательности, идентификацию предвзятости, определение релевантности полученных данных и сравнение с альтернативными источниками. Эти требования обеспечивают, что использование ИИ упрочивает навыки критического мышления, а не заменяет их.

3.4. Методология оценки

Статья 15 посвящена оценке обучения студентов при использовании помощи ИИ. Фокус на «качестве мышления, понимании и развитии навыков», включая «глубину понимания, качество критического мышления, полезность использования ИИ, оригинальность решения проблем и способность улучшать результаты ИИ», создает базис оценки работы с помощью ИИ (ст. 15.1). Однако внедрение этих критериев оценки связано с трудностями, устранять которые учреждениям нужно на путях развития преподавателей и распределения ресурсов.

Методология Кодекса устанавливает параллельную систему оценки, предусматривающую независимый «анализ участия ИИ/человека» и «анализ оригинальности». Этот двухтрековый подход позволит учреждениям поддерживать академическую честность, хотя действенность этой методологии требует эмпирической валидации опытом внедрения.

3.5. Развитие преподавателей и их поддержка

Статьи 17 и 18 посвящены роли преподавателей в образовательных средах, интегрированных с ИИ. Характеристика ст. 17.1 преподавателей как «активных наставников в этичном использовании ИИ» отражает пере-

ход от ограничительных подходов к образовательным подходам при признании компетенций, требуемых для интеграции ИИ. Определение роли преподавателей (ст. 17.2) включает: обучение ответственному использованию ИИ; установление пределов ожиданий; разработку методов оценки; моделирование использования ИИ; поддержку критического мышления.

Положение о профессиональном развитии ст. 18 гласит, что интеграция ИИ требует развития способностей преподавателей. Адаптивный программный подход, рассматривающий роли участников, технические и этические аспекты, практические навыки и сообщества практики демонстрируют понимание принципов профессионального развития¹⁹. Однако требования к ресурсам всеобъемлющего развития преподавателей поставит учреждения с ограниченными бюджетами в затруднительное положение.

4. Искусственный интеллект в исследовательской деятельности: научное применение

4.1. Этика исследований

Указанные статьи очерчивают рамки использования ИИ в исследовательской деятельности, обращаясь к опасениям относительно честности исследований при инновациях. Принципы ст. 19 поддерживают традиционные стандарты этики исследований при признании исследовательского потенциала ИИ. Акцент на том, что «ИИ используется для упрочения, а не замещения человеческого суждения, творчества и экспертизы» (ст. 19.2) напоминает, чтобы исследования оставались человекоцентричными при использовании любых технологических способностей.

Требование, чтобы «исследователи поддерживали экспертизу для понимания и оценки результатов ИИ» (ст. 19.3) посвящено опасениям возникновения зависимости человека от систем ИИ. Это положение ориентирует на то, чтобы при использовании возможностей ИИ исследователи сохраняли интеллектуальную ответственность.

4.2. Подходы к интеграции исследований

Пункт об интеграции ст. 20 посвящен применению ИИ на протяжении жизненного цикла исследования; это обзор литературы, выдвижение гипотез, сбор данных, их анализ и распространение (ст. 20.1). Требование, чтобы интеграция была «методологически подходящей, прозрачной,

¹⁹ European Commission. 2023. April 18. Commission staff working document on digital education and training (SWD(2023) 205 final). Available at: URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023SC0205> (дата обращения: 01.12.2025)

адекватной, соответствующей дисциплинарным стандартам и этически оправданной» (ст. 20.2) создает критерии оценки итогов исследований.

4.3. Стандарты оригинальности и вклада

Статья 21 трактует вопросы об оригинальности в исследованиях с расширением участия ИИ, устанавливая стандарты новизны при использовании ИИ. Условие поддержания новизны при помощи «уникальных инновационных методов, новых интерпретаций, творческого использования ИИ и значимых вкладов в знания» (ст. 21.1) помогает понимать, как создается ценность исследований. Требование, чтобы «исследователи документировали роль ИИ и демонстрировали собственные интеллектуальные вклады» (ст. 21.2) обеспечивает отчетность при инновациях.

4.4. Воспроизводимость исследований

Пункт о воспроизводимости ст. 22 посвящен методологическим опасениям относительно исследований с помощью ИИ. Требования к документации, включая «инструменты ИИ, версии программного обеспечения, наборы данных и методы оценивания» (ст. 22.1), направлены на проверяемость исследований, несмотря на всю их технологическую сложность. Положение о совместном использовании «кода, данных и методологий в этически допустимой степени» (ст. 22.2) синтезирует требования прозрачности с законными соображениями конфиденциальности.

4.5. Совместные исследования

Статьи 24 и 25 посвящены совместным исследованиям и соображениям интеллектуальной собственности. Принципы «взаимного уважения, инновационного развития, прозрачности и этической ответственности» обеспечивают основание для исследовательских партнерств, вовлекающих технологии ИИ. Пункт об интеллектуальной собственности, «применимом национальном законодательстве и институциональных подходах» (ст. 25.1) при обеспечении «подходящей атрибуции участникам» посвящен вопросам собственности, встающим, когда системы ИИ вносят вклад в результаты исследований.

5. Управление и институциональное внедрение

5.1. Архитектура Совета по этике ИИ

Названные статьи устанавливают рамки управления, переводящие этические принципы в институциональную практику. Требование ст. 26 о Совете по этике ИИ с составом, включающим преподавателей, технических специалистов, студентов и администраторов, обеспечивает рас-

крытие перспектив при поддержании правил технической экспертизы (ст. 26.2). Многосторонний состав Совета отражает признание того, что управление ИИ требует множества типов экспертизы.

Положение, что этические комитеты должны быть «оснащены для оценки исследовательских предложений ИИ, включая экспертизу в технологиях ИИ, понимание стандартов и способность оценивать этические вопросы» (ст. 26.3) посвящено потребностям выявления талантов, часто упускаемым в рутине управления. Функции Совета включают руководство решениями о внедрения, этический обзор предложений, разработку стратегии, мониторинг соответствия и разрешение жалоб.

5.2. Требования к ресурсам и инфраструктуре

Пункт о ресурсах ст. 27 фиксирует, что этическая интеграция ИИ требует институциональных инвестиций при гибкости и выявлении способностей. Упор на «справедливость доступа, обучения, безопасной инфраструктуры и оценки эффективности» напоминает, что интеграция ИИ требует систематической поддержки (ст. 27.2). Однако требования к ресурсам могут быть невыполнимыми в учреждениях с ограниченными бюджетами или слабой технической инфраструктурой.

5.3. Системы мониторинга и адаптации

Пункт о мониторинге в ст. 28 намечает подходы к оценке и улучшению управления ИИ. Отслеживание «базовых показателей и благополучия участников» в рамках доступных ресурсов означает практицизм подходов к отчетности (ст. 28.1). Механизмы обратной связи, включая «консультации с сообществом, обзор стратегии и анализ инцидентов», создают ориентированные на обучение системы управления.

Трехлетний цикл обзора с участием международных экспертов создает возможности внешней оценки, чтобы управление не отставало от технологических разработок (ст. 31). Ввиду быстрого темпа развития ИИ могут оказаться необходимыми частые циклы обзора.

5.4. Соображения внедрения и равенства

Статьи 29 и 30 посвящены опасениям насчет утраты равенства при внедрении ИИ. Поэтапный подход к внедрению через «кампании осведомленности, пилотные программы и интеграцию организационной культуры» отражает понимание принципов управления изменениями (ст. 29.1). Стратегия вовлечения студентов, признающая их «партнерами в интеграции ИИ», опирается на принципы вовлечения заинтересованных сторон (ст. 29.2).

Положения ст. 30, направленной против дискриминации, обеспечивают, чтобы внедрение ИИ не создавало новых неравенств при признании различий в способностях личностей. Положение об «альтернативных подходах через механизмы международного сотрудничества» для учреждений с ограниченными ресурсами подчеркивает приверженность доступности при поддержании этических стандартов (ст. 30.2).

6. Сравнительный анализ с международными актами

6.1. Согласование с принципами ЮНЕСКО

Согласование Кодекса с Рекомендацией ЮНЕСКО по этике искусственного интеллекта образует детальное руководство для образовательных контекстов. Если Рекомендация ЮНЕСКО устанавливает принципы развития ИИ в различных секторах, Кодекс предлагает механизмы, обращенные к образовательным вызовам и возможностям.

Основные принципы Рекомендации ЮНЕСКО (человеческого достоинства, прав человека, равенства и антидискриминации) находят выражение в принципах и операционных рамках Кодекса. Однако Кодекс выходит за эти пределы, предлагая механизмы внедрения, обращаясь к уникальным образовательным контекстам. Подход Кодекса к прозрачности и объяснимости адаптирует принципы ЮНЕСКО к образовательным потребностям, специфицируя различные уровни объяснения, необходимые различным заинтересованным сторонам.

6.2. Интеграция права прав человека

Опора Кодекса на международное право прав человека, особенно на Всеобщую декларацию прав человека, рассматривает этику ИИ в образовании как вопрос прав человека, а не административно-управленческий вопрос. Признание образования фундаментальным правом обеспечивает основание повышенного внимания Кодекса к равному доступу и к антидискриминации, переведенному в требования, декларирующие, что интеграция ИИ не создает новых барьеров для участия в образовании.

6.3. Соответствие регулированию защиты данных

Согласование Кодекса с принципами GDPR при адаптации их к образовательным контекстам знаменует прогресс в понимании того, как защиты данных применяется к использованию ИИ в образовании. Принципы GDPR законности, справедливости, прозрачности, ограничения цели, минимизации данных, точности, ограничения хранения и

отчетности находят выражение в положениях защиты данных Кодекса. Однако Кодекс выходит за пределы регулятивного соответствия, обращаясь к образовательным последствиям требований защиты данных.

6.4. Интеграция стандартов академической честности

Интеграция Кодексом основных ценностей Международного центра академической честности — честности, доверия, справедливости, уважения, ответственности и мужества со специфическим руководством по ИИ означает прогресс в понимании академической честности в технологических контекстах. Вместо рассмотрения ИИ как разрушителя академической честности Кодекс показывает, как установленные ценности могут быть применены к новым технологическим обстоятельствам.

7. Критическая оценка: сильные стороны и ограничения

7.1. Сильные стороны

Кодекс этики ИИ имеет сильные стороны, отличающие его от предыдущих попыток управления образовательными технологиями. Всеобъемлющая интеграция этических принципов с практическим руководством по внедрению создает базис, являющийся как философски когерентным, так и детальным [Barthwal A., 2025: 22]. Образовательно-ориентированный подход выходит за пределы дихотомии запрет/разрешение, создавая основу позитивного вовлечения с технологиями ИИ, служащими образовательным целям [Rasul T., 2024: 1].

Принцип вовлечения заинтересованных сторон обеспечивает, что управление остается отзывчивым к потребностям сообщества при поддержании институционального лидерства и этических стандартов [Karran A.J., 2024: 2]. Методологические инновации, особенно параллельная система оценки академической работы с помощью ИИ, образуют вклады в подходы к образовательной оценке [Deer P., 2025: 3]. Архитектура управления, особенно модель Этического совета, создает институциональные механизмы, специально разработанные для ответа на вызовы, связанные с ИИ.

7.2. Вызовы внедрения и ограничения

Несмотря на сильные стороны Кодекса, его применение сталкивается с трудностями внедрения, которые учреждения, рассматривающие его принятие, должны решать. Всеобъемлющая природа Кодекса требует институциональной способности и готовности ко внедрению его

положений, включая техническую инфраструктуру, программы развития преподавателей, службы поддержки студентов и механизмы управления, которые могут превышать текущие способности многих образовательных учреждений.

Требования к ресурсам внедрения существенны и постоянны, речь не идет об одноразовых инвестициях. Учреждения должны развивать техническую инфраструктуру, способную поддерживать интеграцию ИИ при поддержании стандартов безопасности и конфиденциальности. У преподавателей требуют развития профессиональных компетенций, необходимых для интеграции ИИ. Студенты нуждаются в службах поддержки для развития грамотности в области ИИ. Системы управления требуют экспертизы и постоянного внимания к возникающим проблемам [Xu X., 2025: 7].

Вызовы управления изменениями, вовлеченными в трансформацию институциональной культуры, не следует недооценивать [Bond M., 2024: 41]. Сдвиг от запретительных к образовательно-ориентированным подходам требует изменений в подходе учреждений к управлению технологиями, в способах вовлечения преподавателей и студентов в отношения академической честности, в понимании студентами их обязанностей в обучении и развитии [Felani H. et al., 2024: 11214].

7.3. Методологические опасения

Хотя параллельная методология оценки Кодекса — инновация, несколько опасений заслуживают внимания. Полезность анализа участия ИИ/человека зависит от инструментов обнаружения, которые могут быть недоступны всем учреждениям [Kamali J., 2024: 8]. Интерпретация результатов требует экспертизы, которой может не быть во многих образовательных учреждениях. Потенциал ложных положительных или негативных результатов в обнаружении ИИ способен создать несправедливые преимущества или недостатки для студентов.

Полагание на документацию и самоотчетность для прозрачности может быть недостаточным для адекватной оценки использования ИИ [Ateriya N., 2025: 4–5]. Студенты могут не понимать, что составляет подходящую документацию; они могут быть стимулированы занижать использование ИИ, чтобы избежать потенциальных штрафов. Преподаватели могут не иметь в распоряжении экспертизы для оценки работы с помощью ИИ.

7.4. Вопросы масштабируемости и адаптации

Всеобъемлющий подход Кодекса может затруднить его широкое принятие. Требования к ресурсам, потребности в экспертизе и требо-

вания к институциональной способности могут ограничить принятие учреждениями даже с хорошими ресурсами, потенциально усугубляя, а не уничтожая неравенства в доступе к образованию и качеству.

Модель добровольного принятия, уважающая институциональную автономию, может ограничить общее влияние Кодекса на управление ИИ в образовании. Без регулятивных требований, структур, стимулов принятие может остаться ограниченным учреждениями, уже приверженными этичной интеграции ИИ, уменьшая потенциал дальнейшего распространения Кодекса.

Культурное и институциональное разнообразие в глобальных образовательных системах может потребовать значительной адаптации принципов и механизмов внедрения Кодекса. Правовые рамки значительно варьируются по юрисдикциям, создавая почву конфликтов между требованиями Кодекса и национальными или местными регулированиями.

7.5. Потребности в будущих исследованиях

Внедрение Кодекса создает возможности исследований качества управления, технологического воздействия и образовательных результатов, которые способны способствовать пониманию интеграции ИИ в образование. Продольные исследования результатов внедрения в различных институциональных контекстах могли бы создать стимулы понимания для теории и практики управления.

Эмпирическая валидация методологий Кодекса необходима для определения их вклада в поддержание академической честности при подходящем применении ИИ. Исследования воздействия различных подходов к внедрению могли бы формировать лучшие практики для передачи знаний через учреждения и культурные контексты.

Заключение

Кодекс этики искусственного интеллекта в образовании, разработанный в Ташкентском государственном юридическом университете, устанавливает всеобъемлющую позицию, которая стремится сбалансировать инновации с ответственностью, соединить институциональные потребности с индивидуальными правами и глобальные принципы — с их местной адаптацией. Кодекс — это попытка создать системное этическое управление ИИ в образовательных учреждениях.

Образовательный подход. Поворот Кодекса от запрета к образовательным ориентациям составляет его первичный вклад в подходы к управлению. Позиционируя ИИ как инструмент, требующий мастерства, а не как требующую сдерживания угрозу, Кодекс призывает образовательные учреждения пользоваться трансформативными технологи-

ями при поддержании этических стандартов. Этот подход признает как распространенность использования ИИ, так и возможность его этического внедрения путем постоянного внимания к развитию компетенций и обучению.

Образовательный подход трансформирует потенциально антагонистические отношения студентов и учреждений в партнерства, сосредоточенные на обучении и развитии. Вместо развертывания систем мониторинга, сосредоточенных на выявлении нарушений, Кодекс устанавливает базис развития компетенций и наставничества, которые служат целям образования при поддержании его целостности.

Методологические вклады. Методологические подходы Кодекса, особенно параллельная система оценивания академической работы с помощью ИИ, знаменуют попытки решить проблемы оценки в образовательных средах с повышением роли ИИ. Качественные критерии оценки, сосредоточенные на глубине понимания, качестве критического мышления, технологической интеграции, творческой оригинальности и оценке результатов ИИ, создают почву оценки качества обучения студентов при помощи ИИ.

Однако практический вклад этих методологий требует эмпирической валидации на базе опыта их внедрения. Трудность различения между вкладами ИИ и человека может оказаться большей, чем предполагает Кодекс, хотя он и требует постоянного совершенствования и адаптации.

Инновации в управлении. Всеобъемлющая архитектура управления, особенно модель Этического совета ИИ с намеченным в Кодексе составом и обязанностями создает институциональные механизмы, разработанные для ответов на вызовы, связанные с ИИ. Сочетание консультативных и надзорных функций Совета нацелено на отчетность при поддержании институциональной автономии и академической свободы.

Интеграция процессов этического обзора проектов внедрения ИИ стремится обеспечить систематическое рассмотрение этических последствий до развертывания технологий. Однако отдача от этих механизмов управления зависит от институциональной приверженности и распределения ресурсов, которые доступны не во всех контекстах.

Глобальные последствия. Потенциальное глобальное воздействие Кодекса заложено в его детальном подходе к внедрению международных принципов в образовательные контексты. Предложены механизмы, отвечающие на образовательные вызовы и согласованные с международными стандартами. Акцент на адаптации, а не единообразном принятии позволяет контекстуальное внедрение при поддержании основных этических принципов.

Однако добровольность принятия Кодекса и высокие требования к ресурсам его внедрения способны ограничить его воздействие. Без регу-

лятивных рамок, структур, стимулов его принятие может остаться сконцентрированным в пределах учреждений, уже приверженных этической интеграции ИИ.

Внедрение Кодекса способствует пониманию новых подходов к управлению в быстро изменяющихся технологических средах. Адаптивные механизмы в состоянии создать обучающиеся системы, могущие эволюционировать вместе с технологическим прогрессом при поддержке этической приверженности.

Всеобъемлющая интеграция перспектив заинтересованных сторон и приспособление к разнообразным институциональным способностям предлагают подходы к управлению, которые могли бы консолидировать международные усилия в развитии этических рамок для новейших технологий. Однако практические вызовы будут тестировать адаптивность и вклад Кодекса.

Кодекс означает существенный этап ответов на вызовы интеграции ИИ в образовании через механизмы всеобъемлющего этического управления. Хотя он предлагает потенциальные преимущества образовательным учреждениям, стремящимся ответственно интегрировать технологии ИИ, его окончательная ценность будет зависеть от успеха внедрения и эмпирической валидации его подходов. Кодекс способствует дискуссиям об этическом управлении ИИ в образовании. Он предлагает модель, выходящую за пределы запретительных подходов при ответах на вызовы, вовлеченные в балансирование технологических инноваций с образовательными ценностями.



Список источников

1. Кошель А.С., Кузьминов Я.И., Кручинская Е.В., Лесив Б.В. Опыт зарубежного и отечественного регулирования деятельности цифровых платформ: поиск регуляторного оптимума // Право. Журнал Высшей школы экономики. 2025. Том 18. № 2. С. 4–58. DOI:10.17323/2072-8166.2025.2.4.58
2. Ateriya N. et al. Exploring the ethical landscape of AI in academic writing. *Egyptian Journal of Forensic Science*, 2025, vol. 15, no. 36, pp. 1–9. <https://doi.org/10.1186/s41935-025-00453-1>
3. Barthwal A., Campbell M., Shrestha A.K. Privacy ethics alignment in AI: A stakeholder-centric framework for ethical AI. *Systems*, 2025, vol. 13, no. 6, pp. 1–22. <https://doi.org/10.3390/systems13060455>
4. Bond M. et al. A meta systematic review of artificial intelligence in higher education: a call for increased ethics, collaboration, and rigour. *International Journal of Educational Technology and Higher Education*, 2024, vol. 21, no. 4, pp. 1–41. <https://doi.org/10.1186/s41239-023-00436-z>
5. Deep P.D., Edgington W.D. et al. Evaluating effectiveness and ethical implications of AI detection tools in higher education. Basel: MDPI Press, 2025, 23 p. Available at: URL: <https://www.mdpi.com/2078-2489/16/10/905>

6. Felani H. et al. The influence of learning-oriented organizational culture on innovation and firm performance in the creative industry. *Eduvest–Journal of Universal Studies*, 2024, vol. 4, no. 12, pp. 11214–11225. <https://doi.org/10.59188/eduvest.v4i12.1507>
7. Johnston H., Wells R. et al. Student perspectives on the use of generative artificial intelligence technologies in higher education. *International Journal of Education Integration*, 2024, vol. 20, no. 2, pp. 1–21. <https://doi.org/10.1007/s40979-024-00149-4>
8. Kamali J. et al. AI ethics as a complex and multifaceted challenge: decoding educators' AI ethics alignment through the lens of activity theory. *International Journal of Educational Technology for High Education*, 2024, vol. 21, no. 62. 20 pp. <https://doi.org/10.1186/s41239-024-00496-9>
9. Karran A.J., Charland P. et al. Multi-stakeholder perspective on responsible artificial intelligence and acceptability in education, 2025, 28 p. Available at: URL: <https://www.nature.com/articles/s41539-025-00333-2#citeas>
10. Luckin R., Holmes W. et al. *Intelligence unleashed: an argument for AI in education*. London: Pearson, 2016, 58 p.
11. Perkins M. Academic integrity considerations of AI Large language models in the post-pandemic era: ChatGPT and beyond. *Journal of University Teaching & Learning Practice*, 2023, vol. 20, no. 2, pp. 1–17.
12. Rasul T. et al. Enhancing academic integrity among students in Gen AI era: A holistic framework. *International Journal of Management Education*. 2024, vol. 22, no. 3, article 101041. <https://doi.org/10.1016/j.ijme.2024.101041>
13. Rodgers D.J. *The social media dilemma in education: Policy design, implementation and effects*. PhD Thesis. Los Angeles, 2012, 193 pp.
14. Weber-Wulff D. et al. Testing of detection tools for AI-generated text. *International Journal for Educational Integrity*, 2023, vol. 19, no. 1, pp. 1–39.
15. Xu X., Meng F., Gou Y. From theoretical navigation to intelligent prevention: constructing a full-cycle AI ethics education system in higher education. *Education Sciences*, 2025, vol. 15, no. 9, pp. 1–18. <https://doi.org/10.3390/educsci15091199>

Информация об авторах:

С.С. Гулямов — доктор юридических наук, профессор.

И.Р. Рустамбеков — доктор юридических наук, профессор.

Статья поступила в редакцию 22.09.2025; одобрена после рецензирования 17.11.2025; принята к публикации 12.12.2025.

Научная статья

JEL: K31

УДК: 352.075

DOI:10.17323/2713-2749.2026.1.71.95

Социально-трудовые права в условиях платформенной занятости: на примере пассажирских перевозок легковым такси



**Юлия Дмитриевна Жукова¹,
Анна Сергеевна Подмаркова²,**

^{1,2} Национальный исследовательский университет «Высшая школа экономики», Россия 101000, Москва, Мясницкая ул., 20,

¹Julia-jukova@yandex.ru, <https://orcid.org/0000-0002-4455-1096>

²apodmarkova@hse.ru, <https://orcid.org/0000-0003-4549-4588>



Аннотация

Цифровизация экономики породила принципиально новые формы организации труда и занятости, среди которых особое место занимают платформенная занятость и самозанятость*. Отсутствие законодательных дефиниций и полноценного регулирования данных явлений актуализирует вопрос разграничения трудовых и гражданско-правовых отношений, заставляет задуматься о правовом статусе платформенных занятых и самозанятых и необходимости предоставить им социально-трудовые права и гарантии, особенно ввиду множественности типов платформ и специального регулирования отдельных сфер деятельности. В статье обозначенные вопросы рассматриваются на примере регулирования сферы перевозок пассажиров и багажа легковым такси. Авто-

* В отсутствие законодательного закрепления этого понятия в свете правоприменительной практики и мнений доктрины авторы понимают под самозанятыми гражданами, не являющихся индивидуальными предпринимателями (ИП) и применяющих специальный налоговый режим «Налог на профессиональный доход».

ры анализируют сложившиеся в мировой практике направления регулирования нестандартных форм занятости и модели регулирования платформенной занятости и самозанятости, а также предлагаемое российским законодателем регулирование нестандартных форм занятости и имеющееся регулирование платформенной экономики и перевозок пассажиров и багажа легковым такси. Особое внимание авторы уделяют вопросам квалификации деятельности самозанятых перевозчиков и распределения ответственности между участниками отношений по перевозке пассажиров и багажа легковым такси, в том числе подходам, сложившимся в судебной практике до действующего регулирования. Авторы приходят к нескольким выводам. Во-первых, о выборе законодателем для имеющегося регулирования модели, исходящей из предпринимательского характера деятельности самозанятых перевозчиков и прочих платформенных занятых. Во-вторых, об осознании законодателем необходимости наделения этих и иных физических лиц с нестандартной занятостью некоторыми социально-трудовыми правами и гарантиями. В-третьих, о возможности будущей дифференциации регулирования путем внедрения категории «зависимых самозанятых».



Ключевые слова

платформенная занятость; самозанятые граждане; налог на профессиональный доход; перевозки легковым такси; владелец агрегатора информации о товарах (услугах); ответственность в сфере перевозок легковым такси.

Благодарности: статья подготовлена с использованием справочно-правовой системы Консультант Плюс.

Для цитирования: Жукова Ю.Д., Подмаркова А.С. Социально-трудовые права в условиях платформенной занятости: на примере пассажирских перевозок легковым такси. Вопросы права в цифровую эпоху. 2026. Том 7. № 1. С. 71–95. DOI: 10.17323/ 2713-2749.2026.1.71.95

Введение

Цифровизация экономики породила принципиально новые формы организации труда и занятости, среди которых особое место занимает платформенная занятость. Она предполагает опосредованное взаимодействие исполнителя услуги и ее заказчика через цифровые платформы, которые выступают организаторами рынка и агрегаторами спроса и предложения на нем. Данный феномен бросает вызов традиционным моделям трудовых и гражданско-правовых отношений, требуя адаптации правового регулирования.

В России важным шагом в легитимации гибких форм экономической активности стало введение в абз. 2 п. 1 ст. 23 Гражданского кодекса Российской Федерации (далее — ГК РФ) положения, допускающего

при соблюдении ряда условий, предусмотренных законом, осуществление некоторых видов предпринимательской деятельности без государственной регистрации в качестве индивидуального предпринимателя (далее — ИП). Реализацией этой нормы стал Федеральный закон от 27.11.2018 № 422-ФЗ «О проведении эксперимента по установлению специального налогового режима «Налог на профессиональный доход» (далее — Закон о НПД)¹.

Разрешение законами предпринимательской деятельности без государственной регистрации в качестве ИП и отсутствие законодательного понятия «самозанятый гражданин» повлекли на практике появление новой категории субъектов предпринимательства с неопределенным правовым статусом и неоднозначной квалификацией характера их деятельности.

Специфика деятельности самозанятых граждан прежде всего заключается в ее осуществлении ими вне статуса работника и в отсутствии у них наемных работников наряду с возможностью привлечения к исполнению своих обязательств третьих лиц на основании гражданско-правовых договоров; в ограничении видов деятельности, для которых допустимо применение режима НПД и установлении предельного размера доходов, налогооблагаемых в рамках НПД (2,4 млн. руб. за календарный год)².

Применение этого режима невозможно при осуществлении видов деятельности, ведение которых в соответствии с федеральными законами, регулирующими их, требует обязательной регистрации в качестве ИП (ч. 6 ст. 2 Закона о НПД). К таковым до 2022 г.³ относились и перевозки легковым такси.

Предоставление Законом № 580-ФЗ самозанятым гражданам возможности получить с 1.09.2023 разрешение на перевозки легковым такси наряду с ИП и юридическими лицами, с одной стороны, позволяет выдвинуть гипотезу об обоснованности квалификации ГК РФ их деятельности в качестве предпринимательской, с другой — ставит вопрос о необходимости учета специфики их деятельности и создания особого правового режима ее осуществления в рамках регулирования перевозок легковым такси, в том числе с точки зрения предоставления им некоторых социально-трудовых прав и гарантий.

¹ СПС Консультант Плюс.

² Ч. 7 ст. 2, пп. 5, 8 ч. 2 ст. 4 Закона о НПД.

³ До вступления в силу Федерального закона от 29.12.2022 № 580-ФЗ «Об организации перевозок пассажиров и багажа легковым такси в Российской Федерации, о внесении изменений в отдельные законодательные акты Российской Федерации и о признании утратившими силу отдельных положений законодательных актов Российской Федерации» (далее — Закон № 580-ФЗ).

В связи с этим актуально рассмотреть предусмотренные Законом № 580-ФЗ особенности допуска самозанятых граждан к перевозкам легковым такси и модель организации отношений в данной сфере, установить, учитывает ли новое регулирование специфику деятельности таких лиц путем закрепления для самозанятых по сравнению с иными перевозчиками и водителями-работниками ее особого режима. Важен также анализ распределения ответственности между участниками отношений по перевозке легковым такси с целью установления характера деятельности самозанятых граждан как перевозчиков-водителей. Определив подходы российского законодателя к регулированию перевозок легковым такси, рассмотрев сложившиеся в мировой практике направления регулирования нестандартных форм занятости и модели регулирования платформенной занятости и самозанятости, проанализировав предлагаемое в российском правовом порядке регулирование нестандартных форм занятости и имеющееся регулирование платформенной экономики, можно прийти к выводам о необходимости и возможности обеспечения самозанятых перевозчиков социально-трудовыми правами.

1. Получение самозанятыми права на осуществление перевозок легковым такси

Особенность допуска самозанятых к перевозкам легковым такси заключается в том, что в силу необходимости получения ими разрешения на эту деятельность⁴ и ее личного осуществления⁵ самозанятые одновременно должны соответствовать требованиям, предъявляемым Законом № 580-ФЗ как к перевозчикам (ст. 11 Закона), так и к водителям легкового такси (ст. 12 Закона). Несоответствие физического лица требованиям, предъявляемым к водителю такси, является основанием отказа в разрешении на перевозки легковым такси (пп. 3 ч. 9 ст. 5 Закона).

Законодатель значительно увеличил по сравнению с предшествующим регулированием⁶ количество требований к водителям легкового

⁴ Разрешение предоставляется уполномоченным органом субъекта Российской Федерации, на территории которого расположено место нахождения (место жительства) заявителя (ч. 1 ст. 5 Закона № 580-ФЗ). Например, в Москве таким органом является Департамент транспорта и развития дорожно-транспортной инфраструктуры Москвы (п. 2.3.1 Административного регламента предоставления государственной услуги города Москвы, утв. Постановлением Правительства Москвы от 29.08.2023 № 1665-ПП).

⁵ Передача самозанятым управления транспортным средством для перевозки по договору фрахтования легковым такси другому лицу является основанием аннулирования разрешения (пп. 7 ч. 4 ст. 8 Закона № 580-ФЗ).

⁶ Пп. 2 ч. 16 ст. 9 Закона от 21.04.2011 № 69-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» в ред. от 21.12.2021. Статья утратила силу с 1.09. 2023.

такси, по сути установив для самозанятых, как и для работников перевозчиков и ИП, осуществляющих перевозки легковым такси, три их категории: к физическому состоянию (здоровью), знаниям (навыкам) и законопослушности (правомерности предшествующего поведения) без какой-либо дифференциации в зависимости от характера деятельности и правового статуса этих лиц.

Несколько иной подход законодатель избрал при установлении требований к самозанятым гражданам как к перевозчикам. Самозанятый, как и другие перевозчики, самостоятельно соблюдает все установленные законом требования, если выполнение некоторых из них не возлагается им по договору на иного участника отношений в соответствующей сфере (ч. 4 и ч. 5 ст. 11 Закона № 580-ФЗ). Таким участником, во-первых, является служба заказа легкового такси, т.е. ИП или юридическое лицо, имеющее право на осуществление деятельности по получению от потенциального фрахтователя (пассажира) и (или) передаче потенциальному фрахтовщику (перевозчику) заказа легкового такси в целях последующего заключения ими публичного договора фрахтования легкового такси.

Законодатель сделал заключение договора со службой заказа такси, деятельность которой осуществляется с использованием Интернета⁷, условием допуска самозанятых граждан к перевозкам легковым такси (ч. 2 ст. 3 Закона № 580-ФЗ). Договор заключается самозанятым до получения разрешения (ч. 3 ст. 20 Закона). Его отсутствие служит основанием для приостановления последнего (пп. 3 ч. 1 ст. 8 Закона). В случае расторжения договора с самозанятым служба заказа такси должна направить в уполномоченный орган уведомление об этом (пп. 14 ч. 3 ст. 19 Закона).

Таким образом, специфика получения самозанятым права на перевозки пассажиров и багажа легковым такси и его выхода на этот рынок состоит в использовании «технического посредника» и обязательном заключении с ним договора. Такую модель организации отношений по перевозке легковым такси законодатель (согласно пояснительной записке к законопроекту, ставшему Законом № 580-ФЗ) изначально выбрал с целью возложить на службы заказа легкового такси обязанности по сбору и передаче сведений о самозанятых перевозчиках уполномоченным органам⁸ или в соответствующие информационные реестры⁹ для контроля за их деятельностью. Она позволяет участникам отношений

⁷ То есть по сути являющейся оператором посреднической цифровой платформы.

⁸ Органам исполнительной власти субъектов РФ, осуществляющим региональный государственный контроль (надзор) в сфере перевозок пассажиров и багажа легковым такси.

⁹ В частности, в региональный реестр перевозчиков легковым такси.

по собственному усмотрению на основе договора перераспределить между собой обязанности по соблюдению предусмотренных законом требований к перевозчикам и ответственность за их неисполнение.

По сравнению с иными перевозчиками для самозанятых может сократиться большее количество соблюдаемых ими при перевозках требований путем возложения их выполнения на службы заказа легкового такси. Соблюдение переданных требований законодатель не оставляет на добрую волю перевозчиков-самозанятых, а подкрепляет их выполнение возложением соответствующих обязанностей на службы заказа такси.

Например, служба заказа обязана не передавать заказы самозанятому в случае его несоответствия требованиям, установленным Законом № 580-ФЗ к водителям легкового такси при неисполнении им требования по оформлению путевого листа¹⁰ (если у службы заказа есть возможность получить из информационных систем сведения о таких случаях, и она уведомлена о такой возможности) (пп. 13 ч. 8 ст. 19 Закона). Служба заказа обязана не допускать передачу заказов перевозчику-самозанятому, если выполнение заказов им как водителем приведет к нарушению установленных Правительством РФ требований к периоду передачи заказов¹¹, а также если такие сведения службе заказа не предоставлены, или при поступлении сведений о нарушении водителем указанных требований (пп. 3 ч. 8 ст. 19 Закона № 580-ФЗ).

На службу заказа такси возлагается обеспечение на основании данных мониторинга соблюдения установленных законодательством РФ норм рабочего времени, времени отдыха, норм времени управления транспортным средством (пп. 15 ч. 3 ст. 19 Закона). Ей предписано не допускать передачи заказов самозанятому водителю-перевозчику в случае превышения им указанных норм. Положения Закона свидетельствуют, что законодатель принимает во внимание специфику деятельности самозанятых в виде ее личного осуществления и что режим деятельности самозанятого перевозчика несколько отличается от режима деятельности иных перевозчиков — предпринимателей, имеющих водителей-работников.

¹⁰ Документ, служащий для учета и контроля работы транспортного средства, водителя (пп. 14 п. 1 ст. 2 Федерального закона от 08.11.2007 № 259-ФЗ «Устав автомобильного транспорта и городского наземного электрического транспорта»).

¹¹ Это временной интервал, в течение которого осуществляется передача заказа легкового такси службами заказа легкового такси перевозчику легковым такси. Он должен находиться в пределах норм рабочего времени, времени отдыха, норм времени управления транспортным средством, устанавливаемых Правительством РФ (Постановление Правительства РФ от 30.05.2023 № 872 «Об утверждении требований к периоду передачи заказов легкового такси перевозчикам легковым такси службами заказа легкового такси»).

В то же время в отличие от водителей-работников перевозчиков самозанятые перевозчики обладают имущественной и организационной самостоятельностью (например, определяют режим своего рабочего времени в рамках предусмотренных нормативов), несут риски, связанные с деятельностью по перевозке легковым такси.

В части имущественной самостоятельности законодатель учел, что на практике самозанятый может и не владеть транспортным средством, подходящим для использования в качестве легкового такси, поэтому предусмотрел возможность его предоставления самозанятому юридическим лицом или ИП (исполнителем) на основе договора об осуществлении деятельности по перевозке пассажиров и багажа легковым такси (далее — договор об обеспечении легковым такси) (ч. 6 ст. 5 Закона).

Предмет этого договора определен путем фиксации его пяти существенных условий (ст. 13 Закона). К их числу отнесено не только предоставление в пользование легкового такси, сведения о котором внесены в реестр, но и обеспечение прохождения водителем такси предрейсовых (предсменных) и послерейсовых (послесменных) медицинских осмотров, предрейсового (предсменного) контроля технического состояния транспортного средства, а также содержание и техническое обслуживание легкового такси. Кроме этого, условием этого договора является обеспечение предоставления заказчиком до начала деятельности по перевозке уполномоченному органу или в региональную информационную систему уведомления о предоставлении физическому лицу в пользование легкового такси и о сроке такого предоставления. Кроме того, предусмотрено условие о передаче в региональную информационную систему легковых такси информации об использовании или неиспользовании заказчиком возможности прохождения им как водителем медицинских осмотров и о возможности контроля технического состояния легкового такси.

Нарушение исполнителем по договору об обеспечении легковым такси последних трех условий является основанием для исключения сведений о транспортном средстве из регионального реестра легковых такси (ч. 5 ст. 10 Закона № 580-ФЗ).

В данном Законе исчерпывающее правовое регулирование договора об обеспечении легковым такси (впрочем, как и договора со службой заказа легкового такси) отсутствует. В связи с этим вероятны трудности с выбором применимых норм права. Следует согласиться с мнением В.В. Тощенко, что «вопрос правовой квалификации договора об обеспечении легковым такси в качестве договора аренды имеет не праздный характер»¹², а его квалификация «исключительно как договора возмезд-

¹² Речь о применении норм об ответственности арендодателя за недостатки сданного в аренду имущества, за нарушение обязанности по предупреждению

ного оказания услуг позволит применять положения об одностороннем отказе от его исполнения, об оплате услуг в случае невозможности его исполнения», и «пока есть все основания говорить о смешанном характере договора, содержащем элементы договоров аренды и возмездного оказания услуг» [Тощенко В.В., 2023: 16–19].

Недостаточность правового регулирования этих договоров не только не решит практических проблем (например, исполнимости заказа в виде неприбытия или несвоевременного прибытия легкового такси к пассажиру или приостановления доступа к сервису службы заказа в случае снижения рейтинга водителя (перевозчика) ниже определенных баллов¹³), но может повлечь появление новых, сопряженных с определением применимых норм права при разрешении споров по этим договорам в судах.

Сейчас трудно предсказать их масштабы поскольку, например, с одной стороны, заключать договор об обеспечении легковым такси смогут ИП и юридические лица, у которых эта деятельность будет как основной, так и дополнительной по отношению к перевозкам легковым такси¹⁴. С другой стороны, в силу отсутствия законодательного запрета у самозанятых остается возможность заключить иные договоры, предусматривающие получение ими во временное владение и пользование транспортных средств для использования в качестве легкового такси, в том числе и с гражданами, что имело место до вступления в силу Закона № 580-ФЗ.

Таким образом, законодатель допускает различные варианты формирования имущественной базы деятельности перевозчиков-самозанятых. При этом получение по договору об обеспечении легковым такси этого имущества в пользование от профессионалов-предпринимателей сопряженно с возложением на этих лиц по аналогии со службами заказа легкового такси выполнения ряда требований, изначально адресованных законодателем самозанятым перевозчикам. Возможность переложения выполнения предъявляемых Законом требований на иных участников соответствующих отношений является существенным отли-

о наличии прав третьих лиц на него, о досрочном расторжении договора, его пролонгации, реализации права на его преимущественное заключение на новый срок.

¹³ На практике суды преимущественно поддерживают службы заказа такси, ссылаясь на следующее из договора их право контроля оказания услуг: например, Апелляционное определение Московского городского суда от 24.08.2021 по делу № 33-33780/2021, Определение Второго кассационного суда общей юрисдикции от 15.02.2022 по делу № 88-681/2022. Основания ограничения доступа к сервису такси, как и прекращения договора со службой заказа такси должны найти регулирование в законе.

¹⁴ Определение Четвертого кассационного суда общей юрисдикции от 21.05.2024 по делу № 88-15341/2024 свидетельствует, что такие договоры начали заключать.

чием режима деятельности самозанятыми от режима деятельности иных перевозчиков.

Другим отличием является срок действия разрешения на осуществление этой деятельности. Закон № 580-ФЗ предусматривает, что физическим лицам разрешение предоставляется на пять лет либо меньший срок, если физическое лицо указало его в заявлении о разрешении (ч. 4 ст. 5). Юридическим лицам и ИП разрешение предоставляется на срок, установленный нормативным актом субъекта РФ, но не менее чем на пять лет. Право выбора срока действия разрешения обуславливается личным осуществлением самозанятыми деятельности по перевозке легковым такси, а также экспериментальным характером самого режима НПД и деятельности осуществляемой в его рамках.

Введение особого режима деятельности перевозчиками-самозанятыми не опровергает и не подтверждает гипотезы об обоснованности квалификации по ГК РФ деятельности самозанятых в качестве предпринимательской. Это делает актуальным дальнейший анализ характера их деятельности и правового статуса в части определения ответственности этих лиц и выявления ее соотношения с ответственностью иных участников отношений по перевозке легковым такси.

2. Распределение ответственности между участниками отношений

Закон № 580-ФЗ прямо не определяет характера перевозки легковым такси как вида деятельности самозанятых. Однако при закреплении запрета ее осуществления лицами, не имеющими на нее разрешения, Закон дает понять, что перевозка легковым автомобилем пассажиров и багажа за плату может носить предпринимательский характер (ч. 7 ст. 3)¹⁵. Эта же норма запрещает распространение информации, содержащей предложение о перевозке в отсутствие действующего разрешения, за исключением перевозок по заказу и других случаев, предусмотренных законодательством. Служба заказа такси обязана ежедневно осуществлять проверку сведений о разрешениях в реестре перевозчиков и реестре легковых такси, об их приостановлении или аннулировании (пп. 7 ч. 3 ст. 19). Таким образом, законодатель возложил на службы заказа контроль за допуском к фактическому осуществлению перевозок легковым такси лиц, имеющих разрешение, через передачу им заказов.

¹⁵ Следует отметить, что с 1.09. 2024 ст.5 Федерального закона от 08.11.2007 № 259-ФЗ «Устав автомобильного транспорта и городского наземного электрического транспорта» прямо относит перевозки пассажиров и багажа легковыми такси к видам предпринимательской деятельности по перевозке пассажиров и багажа, грузов.

Проблема перевозок пассажиров и багажа легковыми такси в отсутствие соответствующего разрешения тесно связана с вопросом об ответственности за вред, причиненный пассажиру во время такой перевозки. По сути он сводится к распределению ответственности между водителями, перевозчиками и службами заказа такси, к основаниям ответственности последних и ее пределам.

Еще в 2018 году в Определении от 09.01.2018 № 5-КГ17-220 Судебная коллегия по гражданским делам Верховного Суда Российской Федерации (далее — ВС РФ) нашла возможным привлечь службу заказа такси к ответственности как агента, оказывающего услуги по поиску пассажиров, поскольку в соответствии с п. 1 ст. 1005 ГК РФ «по сделке агента с третьим лицом от своего имени и за счет принципала обязанным становится агент, хотя бы принципал и был назван в сделке или вступил с третьим лицом в непосредственные отношения по ее исполнению».

Такое решение коллегия вынесла при том, что водитель являлся работником перевозчика — ИП, владеющего транспортным средством. Последнего со службой заказа такси связывал договор оказания информационных услуг, по которому ответственность за вред, причиненный третьим лицам в связи с перевозкой клиента нес заказчик — перевозчик. Суд решил, что вступление в отношения с работником принципала¹⁶ — водителем такси и возможность получить информацию о принципале не влияют на обязанности агента, вступившего в отношения с третьим лицом от своего имени. В результате ответственность в виде компенсации морального вреда и возмещения расходов на погребение перед родственниками погибшего пассажира несли водитель, перевозчик и служба заказа.

При возложении ответственности на службу заказа было учтено, что ее основным видом деятельности (согласно уставу организации, информации службы защиты прав потребителей и фонда социального страхования) наряду с оказанием информационных услуг являлась также деятельность такси. Суд принял во внимание предъявленную родственниками рекламную продукцию данного общества, информирующую об оказании им именно услуг такси, а также снимок SMS-сообщения, направленный данным обществом на мобильный телефон фрахтователя, с указанием цены услуги и благодарностью за пользование ею. Истцы считали, что, предлагая услуги такси и принимая заказ, служба заказа действовала от своего имени.

Позднее изложенная позиция (правда, уже без ссылки на ст. 1005 ГК РФ) нашла развитие в п. 18 Постановления Пленума ВС РФ от 26.06.2018 № 26 «О некоторых вопросах применения законодательства о договоре

¹⁶ То есть стороны агентского договора, которая поручает другой стороне (агенту) совершение юридических и иных действий.

перевозки автомобильным транспортом грузов, пассажиров и багажа и о договоре транспортной экспедиции». Ее суть сводится к тому, что служба такси отвечает перед пассажиром за причиненный вред, если договор перевозки заключен от ее имени либо из обстоятельств заключения договора (например, рекламные вывески, информация на сайте в Интернете, переписка сторон при заключении договора и т.п.) у добросовестного гражданина-потребителя могло сложиться мнение, что договор перевозки заключается непосредственно с этим лицом, а фактический перевозчик является его работником либо третьим лицом, привлеченным к исполнению обязательств по перевозке. Таким образом, условия наступления ответственности служб заказа такси были определены на уровне разъяснений ВС РФ.

Практически сразу после их появления были внесены изменения в Закон о защите прав потребителей¹⁷ в части введения понятия «агрегатор информации о товарах (услугах)», установления обязанности его владельца по доведению до потребителей информации о себе и о продавце товара, а также в части распределения между ними ответственности за ненадлежащую информацию о товарах (услугах). Закон о ЗПП установил, что владелец агрегатора информации¹⁸ не несет ответственности за убытки, причиненные потребителю вследствие сообщения ему недостоверной или неполной информации о товаре (услуге), если он не изменяет информацию, предоставленную продавцом (исполнителем) и содержащуюся в предложении о заключении договора. Ответственность за исполнение договора и соблюдение прав потребителей несет продавец (исполнитель), а не владелец агрегатора информации если иное не предусмотрено их соглашением или не вытекает из существа их отношений.

Появление этих положений привело к рассмотрению судами вопроса о возможности признания служб заказа такси владельцами агрегаторов

¹⁷ Федеральный закон от 29.07.2018 № 250-ФЗ «О внесении изменений в Закон Российской Федерации «О защите прав потребителей» (далее — Закон о ЗПП).

¹⁸ Закон о ЗПП понимает под ним организацию независимо от организационно-правовой формы либо индивидуального предпринимателя, которые являются владельцами программы для электронных вычислительных машин и (или) владельцами сайта и (или) страницы сайта в информационно-телекоммуникационной сети Интернет и которые предоставляют потребителю в отношении определенного товара (услуги) возможность одновременно ознакомиться с предложением продавца (исполнителя) о заключении договора купли-продажи товара (договора возмездного оказания услуг), заключить с продавцом (исполнителем) договор купли-продажи (договор возмездного оказания услуг), а также произвести предварительную оплату указанного товара (услуги) путем наличных расчетов либо перевода денежных средств владельцу агрегатора в рамках применяемых форм безналичных расчетов (абз. 13 преамбулы Закона о ЗПП). С 01.10.2026 для целей Закона о ЗПП к нему будет приравнен оператор посреднической цифровой платформы.

информации. До середины 2022 года суды давали утвердительный ответ в делах, связанных с привлечением служб заказа такси к административной ответственности по ч. 2 ст. 14.7 Кодекса об административных правонарушениях Российской Федерации (далее — КоАП РФ) за введение потребителей в заблуждение относительно качества и безопасности услуг по перевозке при недоведении до потребителей информации о наличии или отсутствии у водителя разрешения на осуществление перевозок такси¹⁹. Однако осенью 2022 года в нескольких решениях суды не признали службы заказа такси владельцами агрегаторов информации и субъектами ответственности по ч. 2 ст. 14.7 и ч. 1 ст. 14.8 КоАП РФ²⁰. «Общество не отвечает определению владельца агрегатора информации, поскольку мобильное приложение не позволяет произвести предварительную оплату, перевозчику разместить предложение о заключении договора фрахтования, исполнителям/потребителям заключить договор возмездного оказания услуг (перевозки)», — следует из решения АС Московского округа²¹.

Однако с такой позицией судов в отсутствие внесения изменений в КоАП РФ и установления ответственности служб заказа такси за передачу заказов лицам, не имеющим разрешения на перевозку, не согласился ВС РФ. Он исходит из того, что служба заказа такси, «информируя население о возможности получить услугу и принимая соответствующие заявки, формируя базу указанных заявок, оповещая о поступлении заявок перевозчиков, создает у потребителя впечатление, что услуга по перевозке пассажиров и багажа легковым такси будет оказана лицом, имеющим разрешение на осуществление такой деятельности»²². Таким образом, отсутствие информирования потребителя, что услуга может быть оказана лицом, не имеющим всех разрешительных документов на данного вида деятельность, создает основания для ответственности по

¹⁹ Постановление АС ВСО от 02.03.2020 № Ф02-443/2020 по делу № А10-4822/2019; АС СЗО от 17.06.2020 № Ф07-6188/2020 по делу № А56-111312/2019; АС ВСО от 26.01.2021 № Ф02-6845/2020 по делу № А10-2634/2020; АС ДО от 22.09.2021 № Ф03-4427/2021 по делу № А73-16600/2020; АС ЦО от 23.12.2021 № Ф10-5703/2021 по делу № А68-2686/2021; 9 ААС от 01.06.2022 № 09АП-24510/2022-ГК по делу № А40-285054/2021.

²⁰ Постановление АС МО от 31.10.2022 № Ф05-26986/2022 по делу № А40-37711/2022 (отменено), 9 ААС от 14.11.2022 № 09АП-61837/2022 по делу № А40-94657/2022 (отменено).

²¹ Постановление АС МО от 14.02.2023 № Ф05-839/2023 по делу № А40-94657/2022 (постановление отменено Определением Судебной коллегии по экономическим спорам ВС РФ от 30.08.2023 № 305-ЭС23-8620 по делу № А40-94657/2022).

²² Определение ВС РФ от 31.05.2023 № 305-ЭС22-29622 по делу № А40-37711/2022, от 27.07.2023 N 305-ЭС23-8620 по делу № А40-94657/2022.

ч. 2 ст. 14.7 КоАП РФ. При этом ВС РФ исходит из необходимости установления нижестоящими судами наличия у общества статуса владельца агрегатора информации о товарах (услугах)²³.

Неоднозначность подходов к квалификации служб заказа такси в качестве владельцев агрегаторов информации имеет в своей основе ряд причин. Во-первых, в силу свободы договора владельцы агрегаторов информации могут выбирать различные модели построения отношений с продавцами товаров (исполнителями услуг) и их покупателями (заказчиками), на что обращали внимание многие представители доктрины [Иванов А.А., 2017: 145–156]; [Белов В.А., 2022: 68–82]. Такая возможность не ограничивалась и для служб заказа такси. Как отмечала А.А. Ананьева, «востребованными и актуальными могут быть различные формы взаимодействия сервисов с непосредственными перевозчиками и нет смысла ограничивать такие формы взаимодействия; главное при этом, чтобы не нарушалось право пассажира на получение достоверной информации о непосредственном исполнителе и не происходило смешения различных моделей сервисов» [Ананьева А. А., 2020: 20–23]. Л.В. Кузнецова заметила, что на практике службы заказа такси выбрали модель оказания информационных услуг, т.е. роль «посредников в экономическом смысле», «создающих лишь техническую возможность размещения информации и совершения сделки, но не участвующей в ней в качестве стороны, агента, комиссионера или представителя» [Кузнецова Л.В., 2019: 39–65]. С этой попыткой снятия с себя ответственности в итоге не согласился ни ВС РФ, ни законодатель. При этом в доктрине и сейчас продолжают анализировать правовую природу правоотношений службы заказа легкового такси с перевозчиком [Скварко У.А., 2024: 51–55].

Во-вторых, затрудняет квалификацию и само понятие «агрегатор информации о товарах (услугах)», требующее одновременного наличия всех признаков и в силу своей универсальности не учитывающее специфику размещения заказов на перевозку легковым такси. Так С.М. Миронова и Д.И. Кожемякин обращали внимание, что «в отличие... от товарных агрегаторов, потребитель не выбирает сам водителя, который будет оказывать ему услугу, то есть во многом условия договора определяются именно агрегатором» [Миронова С.М., Кожемякин Д.И., 2022: 11–18].

В-третьих, актуальность квалификации снижает привязка ответственности владельца агрегатора к предоставлению ненадлежащей ин-

²³ Определение Судебной коллегии по экономическим спорам ВС РФ от 13.07.2023 N 305-ЭС22-29622 по делу № А40-37711/2022, от 30.08.2023 № 305-ЭС23-8620 по делу № А40-94657/2022. Из изложенной позиции стали исходить суды нижестоящих инстанций при новом рассмотрении этих дел (Постановление Девятого арбитражного апелляционного суда от 25.04.2024 № 09АП-6572/2024 по делу № А40-37711/2022, от 21.05.2024 N 09АП-5451/2024 по делу № А40-94657/2022).

формации. До вступления в силу ФЗ № 580-ФЗ и разъяснения ВС РФ ряд нижестоящих судов считал, что в отсутствие у служб заказа такси прямо закрепленной законом обязанности и технической возможности проверять наличие разрешения на перевозку обвинять их в сообщении пассажирам недостоверной или неполной информации, во введении их в заблуждение нельзя.

Наконец, не способствует квалификации в качестве владельца агрегатора информации о товарах (услугах) отсутствие единого доктринального мнения о возможности возложения на них ответственности перед потребителями. Л.В. Кузнецова считает, что «пытаться полностью или в части переложить на агрегаторов электронной коммерции ответственность по сделкам, совершаемым пользователями соответствующих интернет-сервисов/платформ, — ошибочный путь» [Кузнецова Л.В., 2019: 39–65]. Е.Д. Суворов полагает, что «аргументы в пользу ответственности владельца агрегатора перед потребителем имеются в достаточном количестве». По его мнению, «вопрос о том, по какой модели должна строиться такая ответственность (дополнительная к ответственности товаровладельца по модели поручительства или ответственность агрегатора как стороны по договору), должен составить предмет отдельного исследования» [Суворов Е.Д., 2019: 57–67]. В.А. Белов, анализирувавший еще до принятия Директивы Евросоюза «Об онлайн-посреднических платформах» положения ее проекта, пришел к выводу, что «закрепление солидарной ответственности за операторами платформы по обязательствам, возникающим из договоров, заключенных между поставщиками и клиентами, является в ряде случаев весьма оправданным и адекватным правовым решением, которое находит свое подтверждение в зарубежной и отечественной судебной практике» [Белов В.А., 2022: 116–125].

Самозанятый как перевозчик, по общему правилу, самостоятельно несет ответственность за вред, причиненный при перевозке легковым такси жизни, здоровью и имуществу пассажира (ч. 1 ст. 29 Закона № 580-ФЗ). Однако из этого правила есть исключения, и тогда ответственность перед пассажиром несут иные участники отношений по перевозке.

3. Ответственность иных участников отношений по перевозке

3.1. Ответственность службы заказа легкового такси

Служба заказа легкового такси несет полную ответственность за причиненный пассажиру вред, если он не был уведомлен надлежащим образом о наименовании перевозчика. Это положение соответствует подходу ВС РФ о возможности возложить ответственность на службу заказа такси в случае добросовестного заблуждения пассажира в личности

перевозчика. В случае недоведения службой заказа такси до пассажира информации о перевозчике презюмируется, что последний считает себя связанным договором именно со службой заказа легкового такси. Ответственность самозанятого перевозчика за причиненный вред в этом случае не предполагается.

Служба заказа такси несет солидарную ответственность за вред, причиненный лицом, осуществившем перевозку без разрешения или в случае его приостановления или аннулирования. Единственным обстоятельством, исключающим ответственность службы заказа, является отсутствие у нее технической возможности получить сведения об изменениях в региональном реестре перевозчиков легковым такси и не-передача этих сведений службе такси уполномоченным органом в машиночитаемом виде ранее чем за сутки до дня причинения вреда при перевозке. Возложением солидарной ответственности законодатель подкрепил исполнение службой заказа легкового такси ее обязанности по проверке разрешений на перевозку и соблюдение запрета перевозок лицами, их не имеющими. Логика законодателя ясна: пассажир имеет право на безопасную и качественную перевозку себя и своего багажа профессионалом, имеющим соответствующее разрешение²⁴. В случае причинения вреда он вправе требовать его возмещения и с лица, не обеспечившего ему такую перевозку.

Служба заказа легкового такси несет субсидиарную ответственность по отношению к ответственности перевозчиков-самозанятых в части возмещения реального ущерба пассажира, не покрытого суммой страхового возмещения, выплаченной в соответствии с законодательством об обязательном страховании гражданской ответственности перевозчика или владельца транспортного средства за причинение вреда. Наличие договора обязательного страхования гражданской ответственности (далее — ОСАГО) владельцев транспортных средств для перевозок легковым такси является требованием, предъявляемым к перевозчику. Наряду с ним Закон № 580-ФЗ упоминает и договор обязательного страхования гражданской ответственности перевозчика за причинение вреда жизни, здоровью, имуществу пассажиров (пп. 10 ч. 1 ст. 6, пп. 2 ч. 1, пп. 6 ч. 4 ст. 8 Закона).

С 01.09.2024 на перевозки легковым такси распространено действие Закона № 67-ФЗ²⁵. Перевозчики в течение 60 дней с этой даты обязаны

²⁴ В Постановлении 9 ААС от 11.05.2022 № 09АП-19630/2022 по делу № А40-263181/2021, правда, выражено мнение, что «само по себе наличие у перевозчика разрешения не является гарантией безопасности услуг по перевозке пассажиров и багажа легковым такси, поскольку процедура выдачи разрешений не включает в себя исследования и оценки факторов, непосредственно влияющих на безопасность перевозок».

²⁵ Федеральный закон от 14.06.2012 № 67-ФЗ «Об обязательном страховании гражданской ответственности перевозчика за причинение вреда жизни, здоро-

заключить договор ОСАГО перевозчика в отношении каждого транспортного средства, сведения о котором внесены в региональный реестр легковых такси, и дать информацию о нем в уполномоченный орган исполнительной власти субъекта²⁶. В противном случае действие разрешения приостанавливается, а после аннулируется.

В случае заключения договора его последующее прекращение не освобождает страховщика от обязанности выплатить страховое возмещение по страховым случаям, наступившим в течение срока его действия²⁷. Страховщик будет вправе в порядке регресса требовать у перевозчика возмещения произведенной пассажиру страховой выплаты при наступлении страхового случая вследствие нарушения перевозчиком—самозанятым режима своего труда и отдыха или вследствие использования им при перевозке технически неисправного легкового такси, эксплуатация которого с соответствующими неисправностями запрещена. Аналогичная ситуация имеет место при осуществлении самозанятым перевозки в период приостановления действия разрешения на ее осуществление или в период отсутствия договора со службой заказа легкового такси. Аналогично — при осуществлении перевозки самозанятым за пределами субъекта РФ в котором им получено разрешение, за исключением предусмотренных Законом № 580-ФЗ случаев допущения такой перевозки²⁸. Указанное регулирование, с одной стороны, по мнению доктрины, защитит интересы пассажиров легковых такси [Каримуллина А.Э., 2023: 13–16], с другой — не позволит переложить не соблюдающим требования Закона № 580-ФЗ перевозчикам—самозанятым свою ответственность за причинение вреда пассажиру на страховые организации.

Установление солидарной и субсидиарной ответственности службы заказа такси не снижает ответственности перевозчика—самозанятого, поскольку ч. 3 ст. 29 Закона № 580-ФЗ позволяет службе заказа в порядке регресса взыскать с него (как с лица, виновного в причинении вреда пассажиру) выплаченные суммы в полном объеме. При этом Закон допускает учет вины службы заказа легкового такси в причинении вреда пассажиру путем определения доли, которая может быть взыскана с перевозчика.

Служба заказа легкового такси несет ответственность в соответствии с законодательством РФ за передачу заказа с нарушением установленного Постановлением Правительства РФ периода передачи заказов.

вью, имуществу пассажиров и о порядке возмещения такого вреда, причиненного при перевозках пассажиров метрополитеном» (далее — Закон № 67-ФЗ).

²⁶ Ст. 4 ФЗ от 24.06.2023 № 278-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации».

²⁷ Ч. 3 ст. 9 Закона № 67-ФЗ.

²⁸ Ст. 19 Закона № 67-ФЗ.

В данном случае речь, по-видимому, должна идти об административной ответственности, состав правонарушения которой в настоящее время отсутствует.

3.2. Ответственность исполнителя по договору об обеспечении легковым такси

Она наступает за вред, причиненный пассажиру в результате непередачи самозанятым до начала перевозки пассажиров и багажа уведомления уполномоченному органу или в региональную информационную систему легковых такси о предоставлении легкового такси в его пользование, а также о сроке такого предоставления (ч. 4 ст. 13 Закона № 580-ФЗ). По сути, в отсутствие такого уведомления для иных лиц легковое такси как будто остается в фактическом владении его собственника — владельца источника повышенной опасности, что и обуславливает его ответственность.

Также ответственность наступает в результате неисполнения этим лицом обязанности по техническому обслуживанию и содержанию легкового такси. Часть 4 статьи 29 данного Закона устанавливает солидарную ответственность исполнителя, перевозчика — самозанятого и службы заказа такси за причиненный пассажиру вред, что влечет ряд вопросов: следует ли рассматривать эту норму как специальную по отношению к ч. 4 ст. 13 Закона № 580-ФЗ при понимании, что в последней речь идет о вреде не только пассажирам, но и третьим лицам; будет ли ответственность солидарной по умолчанию в силу закона или же зависеть от положений договора?

Несмотря на неясности норм Закона № 580-ФЗ об ответственности за вред, причиненный жизни, здоровью и имуществу пассажира при перевозке легковым такси, допустим вывод, что между участниками соответствующих отношений она распределена обоснованно. Самостоятельное несение самозанятым в полном объеме ответственности за причиненный пассажиру вред в целом подкрепляет гипотезу о предпринимательском характере деятельности самозанятых перевозчиков легковым такси.

Вместе с тем исключительно личное осуществление ими перевозки, возможное отсутствие собственного имущества для нее и его предоставление иным лицом, обязательное посредничество службы заказа между этими лицами и их клиентами, возможность переложения по договору соблюдения части обязательных требований на иных участников отношений по перевозке призывают задуматься о социальной уязвимости этих лиц и необходимости предоставления им некоторых социально-трудовых прав и гарантий.

4. Регулирование платформенной и иных нестандартных форм занятости

В мировой практике возможны два направления регулирования нестандартных форм занятости: 1) включение лиц с такой занятостью в сферу действия трудового законодательства; 2) точечное решение вопросов, касающихся отдельных аспектов обеспечения им достойного труда [Головина С.Ю., Серова А.В., 2022: 62].

Первое направление по сути предполагает разграничение гражданско-правовых и трудовых отношений, выявление их соотношения через анализ признаков последних. Некоторые юристы отмечают, что цифровизация и развитие нестандартных форм занятости требуют пересмотра критериев разграничения гражданско-правовых и трудовых отношений, заложенных законодателем и выведенных правоприменителями²⁹. Кроме классической организационной зависимости от работодателя, зависимый характер труда должен обуславливаться финансовой (экономической) и информационной зависимостью или асимметрией экономических возможностей сторон [Черных Н.В., 2023: 104 – 113].

Эти критерии трудно критиковать применительно к сфере перевозок легковым такси, когда в отсутствие какого-либо трудоустройства единственным источником дохода самозанятого перевозчика становится данная деятельность, особенно при обязательности заключения им договора со службой заказа и отсутствии возможности влиять на условия ее оферты. Второе направление регулирования реализуется, например, в предоставлении нестандартно занятым возможности создавать профсоюзы, в регулировании вопросов охраны их труда и иных отдельных аспектов, с ним связанных.

Российский законодатель исходя из проекта нового Трудового кодекса Российской Федерации (далее — ТК РФ)³⁰ планирует включить нестандартно занятых в сферу действия трудового законодательства путем закрепления некоторых правовых механизмов гарантий таких лиц, например, их права на объединение в профсоюзы. К сожалению, в целом он делает это весьма фрагментарно, нечетко и непоследовательно в свете выделения им видов и форм нестандартной занятости. В частности,

²⁹ De Stefano V. The Rise of the ‘Just-in-Time Workforce’: On-Demand Work, Crowd Work and Labour Protection in the ‘Gig-Economy’ (October 28, 2015). Comparative Labor Law & Policy Journal, Bocconi Legal Studies Research Paper No. 2682602. Available at: URL: <https://ssrn.com/abstract=2682602> (дата обращения: 20.09.2025)

³⁰ Проект Федерального закона № 858157-8 «Трудовой кодекс Российской Федерации» (ред., внесенная в ГД ФС РФ, текст по состоянию на 06.03.2025) (далее Проект) // СПС Консультант Плюс.

трудно определить, когда и какие нестандартные формы занятости подпадают под действие общих норм трудового и иного, содержащего нормы трудового права, законодательства.

Законодатель исходит из того, что нестандартные формы занятости представляют собой систему социально-трудовых отношений, по тем или иным признакам отклоняющуюся от законодательно установленных норм трудовой деятельности. Это вид трудовой деятельности, при которой наступают общественно полезные последствия и создаются общественные блага, но субъекты которой не находятся в формальных трудовых отношениях так как отсутствует трудовой договор между работником и работодателем. К основным критериям определения нестандартных форм занятости наряду с продолжительностью рабочего времени и взаимоотношениями с работодателями—заказчиками работ, услуг (в частности, дистанционные, на дому) относится и форма оформления отношений, в том числе занятость в рамках гражданско-правового договора, применение специального налогового режима «Налог на профессиональный доход», т.е. самозанятость. К видам нестандартной занятости проектом отнесена и платформенная занятость, определяемая как использование онлайн-платформы (цифровой платформы) в качестве посредника между поставщиками услуг (исполнителями работ) и потребителями (клиентами). Таким образом, предлагаемый Проект позволяет однозначно убедиться, что самозанятость и платформенная занятость относятся к нестандартной занятости и что законодатель задумывается о предоставлении лицам, имеющим такую занятость, некоторого объема социально-трудовых прав и гарантий.

В доктрине условно выделяют три модели правового регулирования платформенной занятости и самозанятости в зарубежных странах [Головина С.Ю., Серова А.В., 2022: 76]. В качестве первой определено создание специальных правовых решений для платформенных трудящихся, например, возможность признания в судебном порядке их отношений с платформой трудовыми несмотря на заключенный между ними гражданско-правовой договор. В российском правопорядке в сфере перевозки легковым такси данный подход не нашел применения, так как на практике имеет место переквалификация отношений самозанятых водителей именно с перевозчиками — юридическими лицами и ИП, обеспечившими их легковым такси по гражданско-правовому договору аренды, но фактически определяющими условия их деятельности. Следует согласиться с мнением Н.Е. Савенко, что «шансов на переквалификацию гражданско-правового договора в трудовой намного больше у самозанятого лица, чем у платформенного занятого» [Савенко Н.Е., 2024: 26]. Такой подход не отражен и в Проекте, в целом допускающем переквалификацию отношений нестандартно занятых на основании гражданско-правового договора в трудовые. Вместе с тем

на наш взгляд требуется конкретизация предлагаемого регулирования в части переквалификации применительно к платформенной занятости со вниманием к регулированию проблемы законами о платформенной экономике³¹ и об организации перевозок легковым такси.

В рамках этой же модели регулирования возможна квалификация платформенных занятых как субъектов гражданского права, на которых ограниченно распространяются трудовое и социальное законодательства. Недавно принятый Закон о платформенной экономике одновременно пошел и не пошел по этому пути. Прежде всего он определил платформенную экономику как совокупность имущественных отношений, складывающихся в результате взаимодействия неограниченного круга лиц посредством цифровых платформ для предпринимательской деятельности или в иных целях, в том числе не связанных с нею. Иные, непредпринимательские цели прежде всего связаны с обслуживанием интересов потребителей, приобретающих с помощью платформ товары, работы и услуги. Целью самих операторов платформ и партнеров платформы, к которым закон относит не только юридических лиц и ИП, но и плательщиков НДС (за исключением физических лиц, совершающих между собой на цифровой платформе сделки, не связанные с их предпринимательской деятельностью) является именно получение прибыли. Из этого следует, что Закон о платформенной экономике по умолчанию исходит из предпринимательского характера деятельности самозанятых граждан, выполняющих работы или оказывающих услуги при посредничестве цифровой платформы, что в целом соотносится с подходом Закона об организации перевозок легковым такси.

Глава 3 Закона о платформенной экономике предусматривает особенности взаимодействия операторов цифровых платформ, пользователей-заказчиков и партнеров-исполнителей, являющихся физическими лицами, и квалифицирует отношения с исполнителем—физическим лицом при их соответствии ряду требований³² как гражданско-правовые, не предусматривая при этом еженедельных выходных дней и отпуска в соответствии с трудовым законодательством, а также дополнительных социальных гарантий (если иное не предусмотрено самим законом) (пп. б и в п. 5 ст. 15 Закона). В то же время предусматривается, что указанное положение не ограничивает партнера-исполнителя в осуществлении перерывов в работе и пользовании временем для отдыха, устанавливает

³¹ Федеральный закон от 31.07.2025 № 289-ФЗ «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации», который вступит в силу с 1.10. 2026 (далее — Закон о платформенной экономике).

³² Например, отсутствие режима (графика) работы и соблюдения партнером — исполнителем, являющимся физическим лицом правил внутреннего трудового распорядка и содержащих нормы трудового права локальных нормативных актов оператора и (или) пользователя-заказчика.

обязанность оператора по предоставлению преференций партнерам-исполнителям, являющимся физическими лицами, вступившим в отношения по обязательному пенсионному, социальному страхованию, по добровольному медицинскому или пенсионному страхованию, предусматривает право оператора полностью или частично возмещать расходы партнеров-исполнителей, сопряженные с таким страхованием. Таким образом, положения этого Закона так же, как и Проект, свидетельствуют о понимании законодателем необходимости социальной защиты физических лиц — партнеров посреднических цифровых платформ, чего в настоящее время не хватает Закону № 580-ФЗ и практике.

Второй моделью правового регулирования платформенной занятости и самозанятости в зарубежных странах является нормативное обособление промежуточной между работниками и самозанятыми предпринимателями категории «зависимых самозанятых», которое, например, имеет место в Австрии, Германии, Испании и Италии³³. Основными критериями такой непредпринимательской самозанятости выступают личное, непрерывное, рабочее сотрудничество, методы выполнения которого организуются клиентом, в том числе с привязкой ко времени и месту работы, а также получение не менее 50 или 75% дохода самозанятого от такого клиента. Заслуживает внимание мнение Н.Е. Савенко, по которому самозанятые — лица, самостоятельно осуществляющие доходную деятельность, которая не является ни трудовой, ни предпринимательской, так как по своим признакам и критериям не соответствует в полной мере названным режимам деятельности [Савенко Н.Е., 2024: 41].

Пока в российском правовом порядке законодатель не демонстрирует готовности к нормативному выделению промежуточной категории и исходит в рассмотренном выше правовом регулировании из дихотомии трудовых и гражданско-правовых отношений, связанных с предпринимательской деятельностью. Дихотомия несколько сглаживается с появлением в Проекте нового ТК РФ категории нестандартных форм занятости и конструированием особых режимов для партнеров платформ или перевозчиков, являющихся физическими лицами — плательщиками НПД, т.е. самозанятыми.

Вероятно в сфере перевозок легковым такси есть фактические основания применения к самозанятым перевозчикам категории «зависимых самозанятых», т.е. внедрения промежуточной между работниками и независимыми подрядчиками категории (как это предлагают в зарубежной доктрине) [Harris S., Krueger A., 2015]; [Stewart A., Stanford J., 2017]. К таким основаниям, например, относятся обязательное заключение

³³ В Испании, например, такое выделение происходит на уровне Закона о статусе индивидуальной трудовой деятельности. Available at: Ley 20/2007, de 11 de julio, del Estatuto del trabajo autónomo (дата обращения: 20.09.2025)

договора с являющейся оператором цифровой платформы службой заказа легкового такси, невозможность самозанятого влиять на условия ее оферты и определение ею размера его вознаграждения за перевозку, возможность ограничения службой заказа такси допуска самозанятого к получению заказов. Также к таким основаниям относится получение такси как необходимого для данной деятельности имущества третьих лиц, зачастую организующих процесс его использования, а также частое использование перевозок легковым такси как единственного источника трудового дохода. При таких условиях возложение всех рисков, связанных с осуществлением этой деятельности, на самозанятого гражданина в отсутствие закрепления за ним социально-трудовых прав и гарантий выглядит неоправданным.

Вместе с тем третья мировая модель регулирования, которую, по сути, выбрал российский законодатель и которая типична для постсоветских государств, например, для Азербайджана и Беларуси, исходит из формирования комплекса правовых норм, регламентирующих правовой статус самозанятых как субъектов предпринимательской деятельности, осуществляющих ее без привлечения третьих лиц. Из этой модели исходят законы о платформенной экономике и об организации перевозок легковым такси, в целом не обеспечивающие самозанятых перевозчиков какими-либо социально-трудовыми правами и гарантиями. Само по себе регулирование самозанятости в нашем правовом порядке все еще носит фрагментарный характер. Как отмечается в доктрине, неопределенность статуса самозанятых лиц и платформенных занятых до настоящего времени не устранена, поскольку определение самозанятости и платформенной занятости в Закон о занятости 2023 года³⁴ из соответствующего законопроекта так и не попали [Савенко Н.Е., 2024: 40]. В этом контексте несомненно позитивно принятие Закона о платформенной экономике, вскоре вступающего в силу. Вместе с тем анализ имеющегося регулирования демонстрирует, что и после этого регулирование самозанятости и платформенной занятости преимущественно будет оставаться в рамках третьей модели без наделения их субъектов социально-трудовыми правами и гарантиями.

Заключение

Закон об организации перевозок легковым такси дал участникам этих отношений право выбора различных моделей деятельности в соответствующей сфере. Так, гражданин вправе стать водителем—работником перевозчика и тем самым существенно уменьшить собственные риски и объем ответственности, спрятавшись за работодателя, но под-

³⁴ Федеральный закон от 12.12.2023 № 565-ФЗ «О занятости населения в Российской Федерации».

чиняясь при этом установленному им режиму рабочего времени и в целом находясь под его контролем. Может он стать и самостоятельным независимым перевозчиком-самозанятым, который при обязательном техническом посредничестве службы заказа такси с использованием собственной имущественной базы или имущества другого лица будет работать на себя, самостоятельно соблюдая все требования, неся все риски и ответственность за исключением тех, которые Закон № 580-ФЗ переносит или позволяет перенести на других участников соответствующих отношений.

Перевозчики ИП (за исключением самостоятельно осуществляющих управление легковым такси) или юридические лица теперь вправе осуществлять такие перевозки только силами своих работников-водителей, прибегая для получения заказов к услугам служб заказа или находя их самостоятельно и самими становясь службами заказов в силу выводимого из ч. 1 ст. 21 Закона запрета передачи исполнения заказов другим перевозчикам. Как и другие предприниматели, перевозчики ИП и юридические лица могут создавать условия для деятельности перевозчиков-самозанятых в части предоставления им в пользование легковых такси и оказания некоторых услуг, связанных с их эксплуатацией и обеспечением соблюдения требований к перевозчикам.

Деятельность служб заказа легкового такси Законом сведена к созданию ими технической возможности для оказания услуг по получению заказов от пассажиров и их передаче перевозчикам с целью заключения этими лицами публичного договора фрахтования, т.е. по сути, к «техническому посредничеству», налагающему, однако, на них публично-правовые обязанности и влекущему в определенных случаях их ответственность.

В целом деятельность перевозчиков-самозанятых в русле разрешительного режима ее осуществления и положений абз. 2 п. 1 ст. 23 ГК РФ может быть квалифицирована в качестве предпринимательской. Такую квалификацию подкрепляет самостоятельное несение перевозчиками — самозанятыми многих рисков и ответственности за вред, причиненный пассажиру легкового такси, возложение ответственности на иных участников отношений преимущественно с целью соблюдения публично-правовых запретов и требований в этой сфере, а также защиты прав и законных интересов пассажиров, а не уменьшения ответственности перевозчиков-самозанятых.

Вместе с тем законодатель, понимая специфику осуществления самозанятыми перевозок легковым такси, создал им по сравнению с иными перевозчиками-предпринимателями несколько отличающийся режим осуществления данной деятельности, характеризующийся возможностью выбора объема лично соблюдаемых требований и использованием «контрагентов-посредников», обеспечивающих ее фактическое

осуществление. При этом заключение договора со службой заказа такси (оператором посреднической цифровой платформы) для самозанятых перевозчиков обязательно.

Рассмотрение сложившихся в мировой практике направлений регулирования нестандартных форм занятости и модели регулирования платформенной занятости и самозанятости, оценка предлагаемого российским законодателем регулирования нестандартных форм занятости, нынешнее регулирование платформенной экономики и перевозок пассажиров и багажа легковым такси приводят к нескольким выводам. Во-первых, о выборе законодателем модели регулирования, исходящей из предпринимательского характера деятельности самозанятых перевозчиков и платформенных занятых. Во-вторых, об осознании законодателем необходимости наделения их некоторыми социально-трудовыми правами и гарантиями. В-третьих, о возможности дифференциации регулирования в будущем путем внедрения категории «зависимых самозанятых».



Список источников

1. Ананьева А.А. Совершенствование правового и индивидуального регулирования работы сервисов заказа услуг такси как одна из мер, направленных на защиту прав пассажиров // Транспортное право. 2020. № 4. С. 20–23.
2. Белов В.А. Онлайн-посреднические платформы: обсуждаемые подходы и отечественная система правового регулирования // Закон. 2022. № 6. С. 116–125. DOI: 10.37239/0869-4400-2022-19-6-116-125.
3. Белов В.А. Цифровое посредничество и потребительские отношения: правовая природа и ответственность // Актуальные проблемы российского права. 2022. № 8. С. 68–82. DOI: 10.17803/1994-1471.2022.141.8.068-082.
4. Гаганов А.А. Правовые аспекты противодействия нелегальным перевозкам пассажиров и багажа легковыми транспортными средствами. Некоторые вопросы правового регулирования перевозок легковым такси // Административное и муниципальное право. 2015. № 3. С. 256–262. DOI: 10.7256/2454-0595.2015.3.12519.
5. Головина С.Ю., Серова А.В. Модели правового регулирования новых форм трудовой занятости // Журнал российского права. 2022. № 8. С. 62–76. DOI: 10.12737/jrl.2022.084.
6. Долгов С.Г. Гражданско-правовая ответственность агрегаторов такси // Гражданское право. 2021. № 1. С. 3–7. DOI: 10.18572/2070-2140-2021-1-3-7
7. Иванов А.А. Бизнес-агрегаторы и право // Закон. 2017. № 5. С. 145–156.
8. Каримуллина А.Э. Проблемы компенсации вреда жизни и здоровью пассажиров легкового такси // Транспортное право. 2023. № 2. С. 13–16. DOI 10.18572/1812-3937-2023-2-13-16.
9. Кузнецова Л.В. Вопросы гражданско-правовой ответственности агрегаторов электронной коммерции. В: E-commerce и взаимосвязанные области (правовое регулирование): сборник статей. Отв. ред. М.А. Рожкова. М.: Статут, 2019. 446 с.

10. Миронова С.М., Кожемякин Д.В. Правовые подходы к ответственности владельцев агрегаторов такси перед потребителями // *Гражданин и право*. 2022. № 2. С. 11–18.
11. Скварко У.А. Правовая природа правоотношений службы заказа легкового такси с перевозчиком легковым такси // *Право и экономика*. 2024. № 6. С. 51–55.
12. Савенко Н.Е. Занятость, самозанятость и платформенная занятость граждан в свете законопроекта о занятости населения в Российской Федерации // *Хозяйство и право*. 2024. № 2. С. 26–41. DOI: 10.18572/0134-2398-2024-2-26-41.
13. Суворов Е.Д. Некоторые проблемы электронной торговли: к вопросу об ответственности владельцев агрегаторов перед потребителями // *Вестник экономического правосудия Российской Федерации*. 2019. № 9. С. 57–67.
14. Тощенко В.В. К вопросу о системе договоров перевозок пассажиров и багажа легковыми такси // *Транспортное право*. 2023. № 2. С. 16–19. DOI 10.18572/1812-3937-2023-2-16-19.
15. Тощенко В.В. Место договора фрахтования легкового такси в системе договоров перевозки пассажиров автомобильным транспортом // *Транспортное право*. 2024. № 1. С. 18–21. DOI 10.18572/1812-3937-2024-1-18-21.
16. Черных Н.В. Трансформация труда как объекта общественных отношений и распространение нетипичных форм занятости // *Актуальные проблемы российского права*. 2023. № 12. С. 104–113. DOI: 10.17803/1994-1471.2023.157.12.104-113.
17. De Stefano V. The Rise of the 'Just-in-Time Workforce': On-Demand Work, Crowd Work and Labour Protection in the 'Gig-Economy'. October 28, 2015. Bocconi Legal Studies Research Paper No. 2682602. Available at: URL: <https://ssrn.com/abstract=2682602> (дата обращения: 20.09.2025)
18. Harris S., Krueger A. A proposal for modernizing labor laws for twenty-first-century work: The «independent worker». Hamilton Project. 2015. Available at: URL: https://www.hamiltonproject.org/assets/files/modernizing_labor_laws_for_twenty_first_century_work_krueger_harris.pdf (дата обращения: 20.09.2025)
19. Stewart A., Stanford J. Regulating work in the gig economy: What are the options? *The Economic and Labour Relations Review*, 2017, vol. 28, no. 3, pp. 420–437.

Информация об авторах:

Ю.Д. Жукова — кандидат юридических наук, доцент.

А.С. Подмаркова — кандидат юридических наук, доцент.

Статья поступила в редакцию 09.07.2025; одобрена после рецензирования 29.09.2025; принята к публикации 30.10.2025.

Научная статья

JEL: K2

УДК: 34.09

DOI:10.17323/2713-2749.2026.1.96.120

Перспективы цифрового здравоохранения



Александр Амиранович Карцхия

Российский государственный университет нефти и газа имени И.М. Губкина, Россия 119991, Москва, Ленинский просп., 65,
arhz50@mail.ru, <https://orcid.org/0000-0002-8041-0055>



Аннотация

Целью исследования является определение особенностей процесса цифровизации, перспектив ее развития в сфере здравоохранения. Автор рассматривает актуальные аспекты специфики применения современных цифровых технологий в медицине, особенности правового регулирования цифровизации отечественного здравоохранения, а также анализирует возможности использования современных технологий в формировании ценностно-ориентированной медицины для оптимизации системы здравоохранения и ее ориентации на интересы пациента. При анализе правового регулирования цифровизации здравоохранения в статье использованы комплексно-аналитический метод исследования и сравнительно-правовой подход. Также применен метод моделирования цифровизации и перспектив технологического развития здравоохранения, в том числе в свете угроз и рисков, которые сопровождают активное применение современных технологий — искусственного интеллекта, биоинженерии, цифровых двойников, которые помогают создать персонализированные методы лечения, адаптированные под индивидуальные особенности пациента, анализировать геномные данные с использованием большого объема биометрических и иных данных пациентов и медицинских учреждений. Автор приходит к выводу, что современная система здравоохранения находится на пороге революционных преобразований, вызванных быстрой интеграцией цифровых технологий. Формирующаяся парадигма здравоохранения — цифровое здравоохранение создает уникальные перспективы и требует правового регулирования и безопасного применения новых медицинских цифровых технологий, благодаря которым появляются принципиально новые возмож-

ности диагностики, лечения, реабилитации, разработки неизвестных ранее медицинских препаратов, а также персонализированные подходы к лечению. Цифровые технологии не только модернизируют методы лечения, а коренным образом меняют способы медицинской помощи, оказывая существенное влияние на пути развития здравоохранения. В перспективе формулируется задача создания цифровой экосистемы здравоохранения, под которой понимается цифровая инфраструктура информационных технологий (включая обмен медицинскими данными), используемая всеми медицинскими учреждениями, органами здравоохранения, поставщиками медицинских услуг и пациентами.



Ключевые слова

цифровизация в здравоохранении; телемедицина; искусственный интеллект; цифровые лекарства; диагностика заболеваний; безопасность данных; цифровая медицина; удаленный мониторинг и диагностика.

Благодарности: исследование проведено в рамках НИР «Совершенствование механизмов защиты прав на объекты интеллектуальной собственности в странах ЕАЭС» по заданию Российской государственной академии интеллектуальной собственности № 2-ГЗ-2024-2.

Для цитирования: Карцхия А.А. Перспективы цифрового здравоохранения // Вопросы права в цифровую эпоху. 2026. Том 7. № 1. С. 96–120. DOI: 10.17323/2713-2749.2026.1.96.120

Введение

Система здравоохранения находится на пороге революционных преобразований, обусловленных быстрой интеграцией цифровых технологий и искусственного интеллекта (ИИ). По данным Всемирного экономического форума 2024 г.¹, ценностно-ориентированная медицина имеет решающее значение для оптимизации здравоохранения во всем мире. Цифровые решения являются ключевым инструментом улучшения здоровья, а цифровые технологии совместно с большими данными и ИИ в своем развитии играют всевозрастающую роль в здравоохранении. Для раскрытия потенциала этих инструментов участники системы здравоохранения (пациенты, поставщики услуг, медицинские и фармацевтические компании, инвесторы, регулирующие органы, технологические компании и разработчики) должны координировать действия в русле цифровой трансформации здравоохранения.

¹ WEF 2024. Transforming Healthcare: Navigating Digital Health with a Value-Driven Approach. Available at: URL: https://www.developmentaid.org/api/frontend/cms/file/2025/04/WEF_Transforming_Healthcare_2024.pdf (дата обращения: 13.11.2025)

Цифровые технологии — ключевой фактор, способный ускорить прогресс в охране здоровья, но они не панацея; для оптимизации здравоохранения важно улучшить его социальные детерминанты: доступность здравоохранения, увеличение инвестиций в данную сферу, включая поддержку медицинских работников, ускоренно внедрять био-медицинские инновации, совершенствовать доступа к лекарствам и медицинским устройствам.

Цифровое здравоохранение, как отмечается в документах ООН², нацелено на равноправный и всеобщий доступ к качественным и недорогим медицинским услугам, а также на развитие профилактики, диагностики и лечения, реабилитации и паллиативной помощи в системе, способствующей конфиденциальности и безопасности информации о здоровье пациентов, в целом — на повышение полезности и устойчивости национальных систем здравоохранения. Отмечается, что данные о здоровье следует приравнивать к конфиденциальным персональным данным человека. Такие данные требуют соблюдения высоких стандартов безопасности и защиты, что предполагает развитие нормативной базы. Она призвана защищать неприкосновенность частной жизни, конфиденциальность, кибербезопасность, а также целостность, доступность и надлежащую процедуру обработки персональных данных о здоровье. Прирост почти 30% мирового массива данных будет приходиться на здравоохранение, где используются методы визуализации, диагностики и носимые устройства, что обуславливает необходимость упрочения безопасности инфраструктуры, которой требуются надежные аналитические платформы и интеллектуальные технологии, способные оперативно преобразовывать необработанные данные в полезную информацию.

Неоспоримое всеобщее значение цифровизации здравоохранения, в том числе и в свете Целей устойчивого развития ООН, было подтверждено Всемирной Ассамблеей здравоохранения WHA78 (22), одоббившей продление на 2020–2027 годы глобальной стратегии цифрового здравоохранения³. Концепция глобальной стратегии заключается в улучшении здоровья народонаселения планеты путем ускорения разработки и внедрения соответствующих, доступных по цене, масштабируемых и устойчивых цифровых решений, ориентированных на предотвращение, выявление эпидемий и пандемий и на реагирование на них, на развитие

² World Health Organization. 2021. Global strategy on digital health 2020–2025. Available at: URL: <https://iris.who.int/handle/10665/344249> (дата обращения: 13.11.2025); WHO guideline recommendations on digital interventions for health system strengthening: evidence and recommendations. Geneva, 2019. Available at: URL: <https://iris.who.int/handle/10665/311980> (дата обращения: 13.11.2025)

³ Global strategy on digital health 2020–2027. World Health Organization 2025. Available at: URL: <https://www.who.int/publications/i/item/9789240116870> (дата обращения: 12.12.2025)

инфраструктуры и приложений, позволяющих использовать медицинские данные для укрепления здоровья и благополучия, для достижения устойчивого развития. Концепция также направлена на активизацию исследований и разработок, инноваций и сотрудничества в сфере здравоохранения.

1. Передовые технологии — основа современной цифровой здравоохранения

В здравоохранении, медтехнике и фармацевтике наступил переломный момент выбора между быстрой трансформацией системы или продолжением постепенного ее совершенствования. Новаторские медицинские решения с использованием новейших технологий, включая ИИ, телемедицину, новейшие методы лечения и профилактики, обладают потенциалом снижения затрат и улучшения результатов в области здравоохранения. ИИ является частью более широкой цифровой революции, могущей во многом изменить сферу здравоохранения. Внедрение цифровых технологий способно обеспечить улучшение работы здравоохранения и повышение доступности медицины. При этом реализация концепции цифровой медицины потребует преодоления рисков и вызовов, связанных с конфиденциальностью, кибербезопасностью, повышением квалификации врачей и пациентов, справедливым доступом к медицинским услугам. Практика показывает, что темпы цифровизации в здравоохранении выше, чем в других отраслях.

Ныне образовались исключительные возможности ускорения цифровой трансформации здравоохранения путем расширения использования цифровых технологий и данных, что открывает новую эру здравоохранения, ориентированного на повышение ценности медицины. Цифровая трансформация здравоохранения включает ряд ключевых факторов, в частности: использование ориентированных на пациента цифровых приложений и инструментов для улучшения медицинской помощи; внедрение передовых цифровых технологий, платформ и систем; широкое использование технологий в области науки о жизни и фармацевтики; применение цифровых приложений для сбора массива медицинских данных, позволяющих улучшить и ускорить разработку и поставку лекарственных средств, а также обеспечивают портативную, быструю и более точную терапию и диагностику.

Эти факторы создают новую значимость медицины. Оцифровка приложений в работе с пациентами, использование цифровых технологий, больших данных и ИИ направлено прежде всего на оказание более качественной медицинской помощи. Пока же большинство систем здравоохранения имеет фрагментированную ИТ-инфраструктуру, несовместимые стандарты обработки данных и устарелые способы обмена

данными, а также множество цифровых решений, которые препятствуют их использованию. В целом здравоохранение по-прежнему отстает от других секторов с точки зрения цифровой зрелости.

Новая парадигма медицины связана с цифровизацией здравоохранения. Цифровое здравоохранение означает медицинскую деятельность, оказание медицинской помощи (услуг) с использованием цифровых информационно-коммуникационных технологий (ИКТ). При этом понимание цифрового здравоохранения (медицины) значительно шире понятия «телемедицинские технологии», обеспечивающие дистанционное взаимодействие) в понимании ст. 2 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»⁴.

Формирование цифрового здравоохранения явилось результатом цифровизации, при которой в диагностике, лечении и профилактике применяются современные информационные технологии (ИТ). Под цифровым здравоохранением также понимается область знаний и деятельности, связанная с разработкой и применением цифровых технологий для улучшения здоровья населения. Допустимо говорить об экосистеме цифрового здравоохранения — инфраструктуре функционально совместимых ИТ, используемых медицинским сообществом во всех сферах здравоохранения. Цифровизация направлена на создание цифровой экосистемы здравоохранения, под которой следует понимать цифровую интероперабельную инфраструктуру ИТ, которая объединит медицинские учреждения и пациентов, органы общественного здравоохранения, университеты и научные центры в целях обмена данными между пользователями, поставщиками медицинских услуг, руководителями систем здравоохранения и службами обработки данных.

Наиболее широко применяются в цифровой медицине разнообразные модели искусственного интеллекта.

Цифровые двойники (Digital twins, DTS) с использованием технологий ИИ — это цифровые воплощения систем, позволяющие проводить расширенное моделирование, прогнозное моделирование и оптимизацию в реальном времени в различных областях, включая здравоохранение. Цифровые двойники — цифровые копии физических объектов, процессов или систем, которые динамически обновляются с помощью данных для фиксации состояния их реальных аналогов. Они обеспечивают прогностическое моделирование, поддержку принятия решений и персонализированное моделирование. Цифровые двойники часто изображаются в виде 3D-моделей или информационных панелей. Например, цифровой двойник выглядит визуальной симуляцией сердца пациента. Медицинские приложения DTs дают возможности моделирования сложных сценариев лечения пациентов, поддерживают прогностическую

⁴ Собрание законодательства РФ. 2011. № 48. Ст. 6724; 2025. № 23. Ст. 3009.

диагностику и позволяют планировать индивидуальное лечение в режиме реального времени на основе данных о здоровье. Цифровые двойники в области здравоохранения охватывают широкий спектр клинических и операционных применений на различных стадиях разработки, начиная с теоретических моделей и заканчивая продвинутыми экспериментальными этапами [Zhou H. et al., 2024: 2–17]⁵.

Моделирование процессов в медицине на основе технологий ИИ. К примеру, генеративный ИИ помогает в разработке дизайна исследования и составлении протокола, автоматически сопоставляя клинические концепции со стандартизированными определениями исследований, критериями отбора и выбором переменных на основе электронных медицинских карт. ИИ способен моделировать сценарии, концептуально схожие с цифровыми двойниками или медицинскими моделями, что позволяет исследователям рассчитывать клинические результаты при альтернативных стратегиях лечения, сроках или режимах дозирования, которые невозможно напрямую наблюдать в реальных данных. Генерация синтетических данных используется для повышения статистической значимости и объективности, что помогает преодолеть ограничения, связанные с размером выборки, и улучшить репрезентацию редких заболеваний и недостаточно защищенных групп населения [Azarfar G. et al., 2025: 2–5]. Технологии генеративного ИИ применяются при изучении смертности и основных заболеваний для анализа специализированных клинических изображений, таких, как изображения сетчатки глаза [Nusinovi S. et al., 2022: 4–5] и рентгеновские снимки грудной клетки [Raghu V., Weiss J., 2021: 6–7], а также в прогнозировании биологического возраста пациентов на основании большой группы изображений лиц с указанием возраста, пола и этнической принадлежности при тестировании на четырех различных клинических группах, включая пациентов с различными видами рака [Bontempi D., 2025: 2–3].

В обработке больших данных и биометрических персональных данных ИИ позволяет не только обрабатывать и моделировать процессы и их результат на основе фактических данных, но и создавать «синтетические данные», т.е. искусственно сгенерированную информацию, предназначенную для имитации характеристик и статистических свойств реальных данных. В сфере здравоохранения синтетические данные часто используются для дополнения или расширения наборов данных, которые генерируются на основе реальных наборов данных (например, электронных медицинских карт или реестров), для решения проблем конфиденциальности и расширения ограниченных наборов реальных данных [Koul A., 2025: 1–2].

⁵ Ringevea M., Armel F. et al. Advancing Health Care With Digital Twins: Meta-Review of Applications and Implementation Challenges. Available at: URL: <https://www.jmir.org/2025/1/e69544> (accessed: 13.11.2025)

Новая тенденция — использование блокчейнов для обработки массива информации о пациентах и данных об их здоровье, включающих различные анализы, оценки качества и опросы о самочувствии, а также безопасный обмен данными о пациенте (имя, дата рождения, диагноз, лечение и история болезни и др.) для поставщиков медицинских услуг в формате электронных медицинских карт (ЭМК), обычно хранимых в облачных вычислительных средах или традиционных базах данных, а также сбор и обработка обезличенных данных для точной настройки рецептурных препаратов и услуг для пациентов. Блокчейн также обеспечивает бесперебойную коммуникацию и обмен информацией между различными организациями экосистемы здравоохранения посредством распределенного реестра, повышая безопасность и прозрачность такого обмена. Пользователи могут обмениваться данными и действиями в системе, а также отслеживать их без необходимости дополнительных решений для поддержания целостности и конфиденциальности.

Создание биобанков и использование биоданных является новым направлением цифровой медицины. Большинство традиционных инструментов оценки риска основаны на клинических параметрах (возраст, пол и семейный анамнез), а также на ограниченном наборе базовых биомаркеров, характерных для изучаемого заболевания. Однако эти инструменты не могут охватывать всего спектра биологических процессов, лежащих в основе многих болезней. Появление биобанков, объединяющих ЭМК и мультимедийные данные, такие как результаты стандартных анализов крови, протеомики и метаболомики, открывает беспрецедентные возможности поиска новых биомаркеров и их наборов для более уточненного прогнозирования начала заболевания [Garg M., Karpinski M., 2024: 1821–1831]. Биобанк содержит данные о фенотипе, включая постоянно обновляемые медицинские карты, биометрические измерения, показатели образа жизни, биомаркеры, а также изображения.

Британский биобанк [Backman J., 2021: 628–634] — один из крупнейших биобанков, включающий медицинские карты и данные генетического секвенирования полумиллиона человек в возрасте 40–69 лет, что позволяет выявлять множество генетических ассоциаций и вероятных терапевтических мишеней. Банк также дает возможность выявлять комбинации биомаркеров, могущих прогнозировать начало болезни лучше любого отдельного биомаркера. Помимо прогнозирования болезни и обнаружения биомаркеров, основанные на последних прогнозы для лиц с заболеванием также способны дополнить анализ генетических открытий. Одним из ограничений большинства биобанков является то, что определения фенотипа часто основаны на расчетных кодах и самоотчетах, могущих приводить к неверной классификации участников, к отсутствию данных и вариабельности в определении когорт «случай-контроль». Выявление лиц, которые могут быть пациентами, но либо не

кодированы должным образом, либо не были клинически диагностированы, остается проблемой [Cortes A., Johnston I., 2023: 699].

В медицине в настоящее время создается новое направление — инженерная живая терапия, т.е. применение передовых пробиотических систем, то есть микробов, клеток и грибов, связанных со здоровьем человека, которые разрабатываются для производства терапевтических веществ (лекарств, ферментов и гормонов). Эти способы лечения стали возможны благодаря синтетической биологии и генной инженерии. Для этого в системы вводится генетический код, способствующий созданию биологических механизмов контроля, которые регулируют выработку терапевтических препаратов внутри организма пациента, обеспечивая точную и безопасную активацию. Такая терапия обещает преодолеть серьезные недостатки традиционных лекарств, особенно дорогостоящих биофармацевтических препаратов. Ныне такие препараты производятся в лабораториях с использованием модифицированных клеточных линий с последующей тщательной очисткой, обработкой и формированием рецептур. Производство терапевтических препаратов непосредственно в организме позволяет избежать последующих стадий, на которые обычно приходится до 70% производственных затрат. Кроме того, лекарствам, требующим частого введения с помощью инъекций, устойчивое их производство в организме пациента обеспечит длительное и стабильное их поступление и повысит адаптацию пациента к лечению, что особенно важно, например, при лечении диабета. К примеру, компания NEC проводит клинические испытания I/II фазы с использованием ослабленного штамма бактерий сальмонеллы, чтобы активировать иммунную систему пациента в борьбе с раковыми клетками.

При этом безопасность находится в центре внимания, и активно решаются такие проблемы, как непреднамеренный перенос генов, иммунные реакции и выброс в окружающую среду. Перспективными подходами, которые в настоящее время находятся в стадии исследований, являются метаболические и генетические программы, предотвращающие рост бактерий или убивающие их по команде; безопасная инкапсуляция в контейнеры на полимерной основе [Zalatan J., Petrini L., 2024: 2–7].

Развивается технология автономных биохимических датчиков (биосенсоров), заключающаяся в подключении биологических датчиков для информации в режиме реального времени. Автономные биохимические датчики—это аналитические устройства, которые непрерывно определяют и количественно оценивают биохимические параметры (маркеры) для индивидуального подхода к лечению пациентов или химические изменения в почве или воде для контроля состояния природы. Такие датчики определяют контролируемое химическое вещество с помощью специализированных физико-химических преобразователей или биологических датчиков, использующих ферменты, антитела или даже мо-

дифицированные живые клетки. Датчики предназначены для работы и передачи данных без участия человека, они используют беспроводную связь и сбор энергии с помощью автономных источников питания (биотопливные элементы) [Maity D., Guha P., 2023: 1–14] для непрерывного мониторинга. Поскольку данные с этих датчиков можно получать дистанционно, они подходят для использования в труднодоступных или удаленных местах. Это позволяет непрерывно отслеживать состояние здоровья лиц и природы.

В отличие от обычных одноразовых датчиков (тесты на COVID-19), задача автономного биохимического мониторинга—обеспечить непрерывный мониторинг и сбор электронных данных. В силу таких технических ограничений автономные биохимические датчики используются только в очень специфических областях. Самым полезным является носимый датчик уровня глюкозы, который измеряет концентрацию глюкозы и обменивается данными со смартфоном, который управляет инсулиновой помпой для стабилизации уровня глюкозы. Благодаря одновременному развитию материаловедения, нанотехнологий, биомиметики и беспроводных технологий автономные биохимические датчики начинают использоваться в решении других задач и в других областях [Zargartalebi H., 2024: 1146–1153]. Новые формы этой технологии способны изменить жизнь многих пациентов, которым требуется мониторинг их состояния. Однако срок службы многих датчиков невелик, их приходится регулярно заменять. По сравнению с обычными медицинскими или экологическими датчиками, микробные цельноклеточные биосенсоры сталкиваются с дополнительными нормативными препятствиями и этическими проблемами, поскольку являются генетически модифицированными биологическими организмами, которые могут попасть в окружающую среду.

Децентрализация диагностики с помощью носимых устройств и биосенсоров, устанавливаемых в местах медицинской помощи, позволит проводить тестирование не только в медицинских учреждениях, но и на дому, в отдаленных населенных пунктах. Такое распространение диагностических данных может в корне изменить подход к лечению, обеспечив более раннее вмешательство и генерируя огромные потоки данных о здоровье населения [Lino C., 2022: 2–9]. Помимо конструкции физических датчиков, интеграция данных образует еще одну важную область развития. Поскольку автономные сенсорные сети генерируют непрерывный поток молекулярной информации в различных областях, для обработки этих данных потребуются новые аналитические системы и модели управления. Вопросы конфиденциальности и безопасности, особенно в сфере мониторинга здоровья, требуют подходов к регулированию, которые позволят сочетать инновации с защитой конфиденциальной информации. Объединение возможностей непрерывного

мониторинга в сферах охраны окружающей среды, безопасности пищевых продуктов и здравоохранения предполагает, что в будущем молекулярное обнаружение станет интегрированным уровнем повседневной инфраструктуры, а не специализированной функцией [Floreaga L., Diamond D., 2022: 1–7]. Расширение возможностей технологий подключенных систем больших биометрических данных для сбора, обработки и принятия решений в контексте использования различных датчиков, снимающих показания, обеспечивает их повсеместное использование на рабочих местах и позволяет интегрировать с системами, применяющими искусственный интеллект.

Технологии воспроизведения искусственных катализаторов позволяют получать в лаборатории или изготавливать наноматериалы (нанозимы – Nanozymes), обладающие свойствами природных ферментов (наноферменты). Наноферменты, в отличие от ферментов, которые вырабатываются живыми организмами или синтезируются химическим путем, обладают повышенной стабильностью, невысокой себестоимостью и упрощенными процессами синтеза. Они состоят из наночастиц металлов, оксидов металлов, углерода и других материалов, действуют как катализаторы и способствуют тем же химическим реакциям, что и ферменты. Благодаря прочности они могут функционировать в гораздо более разнообразных средах, что расширяет возможности их применения в биомедицине, экологии и промышленности. Используя передовые методы проектирования и производства на наноуровне, можно создавать многофункциональные наноферменты. Стремительное развитие наноферментной технологии в последние два десятилетия привлекло к ним внимание крупных фармацевтических компаний, что привело к увеличению инвестиций в исследования и разработки в данной области. Рост финансирования ускорил темпы инноваций и расширил возможности применения наноферментов в различных областях медицины (лечения рака и нейродегенеративных заболеваний) в качестве средства адресной доставки лекарств, повышая эффективность химиотерапии и снижая побочные эффекты [Sen A., 2024: 25].

Наноферменты обещают революцию в диагностике и лечении, особенно в таких областях, как раннее выявление заболеваний и адресная доставка лекарств, а также в диагностике, восстановлении окружающей среды и целевой терапии. Наноферменты требуют интеграции ИИ, вычислительного проектирования и специальных знаний [Cao X., 2024: 27].

Цифровые технологии, по оценкам специалистов [Thirumal M., Monika S., 2024: 1–4]; [Lee B., Ghovanloo M., 2019: 74–80], позволяют решать многие задачи. В частности, цифровые измерительные инструменты позволяют получать объективные и непрерывные данные, снижают вероятность предвзятости и ошибок традиционных методов сбора данных, что облегчает сбор больших объемов данных о пациенте, по-

звояля разрабатывать персонализированные и точные подходы к лечению, соответствующие индивидуальным потребностям пациента.

Роботы-хирурги и медицинские помощники (зарубежные роботы-хирурги Da Vinci, Dixon Revo-i, Senhance, MAKO и российские AST, LevshAI) — ключевые элементы современной инструментальной медицины, повышающие точность операций и качество ухода за пациентами, облегчающие также работу персонала. Несмотря на дороговизну такого оборудования и операций, необходимость специального обучения хирургов, они обеспечивают повышенную точность и малоинвазивность операций, возможность работы в труднодоступных зонах, снижение времени госпитализации. Медицинские помощники выполняют разнообразные задачи, улучшая уход за пациентами — таковы роботы-медсестры, роботы-ассистенты и консультанты, роботы-компаньоны, роботы дезинфекции и реабилитации. Роботы в медицине не заменяют врачей, а становятся их незаменимыми помощниками, повышая качество лечения и ухода. Однако их массовое внедрение требует решения проблем, связанных с их стоимостью, обучением и этикой.

Биотелеметрия (биомедицинская или медицинская телеметрия) обеспечивает мониторинг и передачу физиологических данных от пациента в удаленное место для анализа, интерпретации и диагностики. Эта технология позволяет осуществлять мониторинг физиологических параметров (частоты сердечных сокращений, артериального давления, температуры и другие жизненно важных показателей), с использованием беспроводных или удаленных систем связи. Например, биотелеметрия широко используется в кардиологии для удаленного мониторинга сердечной деятельности и при лечении сердечных заболеваний, что улучшает уход за пациентами, позволяя раннее выявление отклонений, облегчая своевременное вмешательство и улучшая общее лечение хронических заболеваний.

Имплантируемые биомедицинские устройства, которые хирургическим путем вживляются в организм для мониторинга, диагностики или лечения болезней, предназначены для взаимодействия с биологическими системами и могут варьироваться от элементарных датчиков до изолированных электронных систем. Их обычно используют в долгосрочном мониторинге и лечении хронических болезней. Кардиостимуляторы и дефибрилляторы используют для регулирования аномальных сердечных ритмов и подачи электрических импульсов в сердце для поддержания его ритма. Имплантируемые кардиомониторы применяются при мониторинге электрической активности сердца с целью выявления аритмии или других отклонений. Имплантируемые нейростимуляторы применяют при электрической стимуляции нервных волокон или областей мозга для лечения хронической боли, двигательных расстройств или других неврологических заболеваний. Имплантируемые глюкометры непрерывно контролируют уровень глюкозы у пациентов с диабе-

том, поставляя данные для помощи в управлении уровнем сахара в крови. Имплантируемые системы доставки предназначены для доставки лекарств непосредственно в участки тела, обеспечивая целенаправленное лечение таких состояний, как хроническая боль или рак.

Цифровые средства визуализации и диагностики, такие как цифровая рентгенография, PACS (система архивации и передачи изображений) и диагностические инструменты на базе ИИ, позволяют быстро и точно ставить диагноз, а также бесперебойно обмениваться медицинскими изображениями и отчетами. Цифровые лекарства повышают вовлеченность пациентов в лечебный процесс и их приверженность плану лечения. Мобильные приложения напоминают пациентам о приеме лекарств, отслеживать симптомы. При этом должны быть соблюдены стандарты безопасности цифровой медицины, защищенность данных пациентов и их конфиденциальность в соответствии с целям и потребностями лечебного учреждения.

Одним из самых передовых направлений цифровизации является применение нейротехнологий (нейропротезирование) и их внедрение в систему здравоохранения, наиболее перспективным трендом которого является протезирование сенсорных систем (слуха, зрения и др.), а также протезов конечностей.

2. Формирование цифрового здравоохранения в России

Проблемы глобального характера: рост численности народонаселения, его демографическое старение, распространенность хронических неинфекционных заболеваний, постоянный рост затрат на здравоохранение с одновременным увеличением дефицита ресурсов, включая кадры [Малеина М., 2023: 5]; [Пугачев П., 2021: 12]; [Шереметьева Н., 2024: 43], могут быть преодолены активным использованием широкого спектра ИТ и цифровых технологий.

В связи с этим растет роль правового регулирования применения передовых технологий, включая ИИ, необходимости баланса и взаимосвязи между методами правового регулирования, их взаимодействия в целях создания условий для развития современных технологий, включая искусственный интеллект [Bogdanovskaya I. et al., 2025: 124–147].

Цифровая трансформация здравоохранения при использовании таких современных технологий, как Интернет вещей, удаленный мониторинг и телемедицина, ИИ, блокчейн, интеллектуальные носимые устройства, цифровые информационные платформы, а также инструменты, позволяющие осуществлять удаленный сбор и обмен данными и релевантной информацией по всей экосистеме, обеспечивающие непрерывность медицинской помощи, доказали свой большой потенци-

ал. Такие показатели достигаются в том числе за счет улучшения медицинской диагностики, принятия решений о лечении на основе данных, цифровой терапии, клинических испытаний, автономного управления медицинской помощью и уходом, ориентированных на человека, а также создания массива основанного на фактических данных о знаниях, навыках и компетентности медицинских учреждений и персонала .

Цифровые технологии не только модернизируют традиционные методы лечения, но коренным образом изменяют способы получения медицинской помощи, существенно влияя на пути развития здравоохранения. Переход к цифровому здравоохранению — не только вопрос модернизации, а необходимость улучшения результатов лечения, оптимизации медицинских операций и персонализированной помощи. Получение доступа к полным данным о пациентах в режиме реального времени в процессе оцифровки клинической информации позволяет принимать обоснованные решения, сокращать количество ошибок и оптимизировать координацию медицинской помощи, а аналитика данных, основанная на цифровых системах, помогает выявлять ранние признаки заболеваний, определять пробелы в медицинской помощи и оптимизировать процесс лечения. Объем и разнообразие медицинской информации в сфере здравоохранения: от историй болезни и результатов лабораторных исследований, повсеместное внедрение электронных медицинских карт, применение носимых устройств и устройств с интернет-поддержкой, выросли в геометрической прогрессии, добавив к этому непрерывный поток данных в режиме реального времени.

Наиболее широко в российской практике цифровая медицина нашла применение в Москве, где замена аналогового оборудования цифровой техникой позволила создать единый цифровой контур московского здравоохранения. Запись к врачам, карты пациентов, плановые и экстренные госпитализации, назначения и рецепты, прививки, результаты исследований и анализов и другая медицинская информация аккумулируются ЕМИАС и доступны в режиме онлайн. Технологии ИИ, «компьютерное зрение», анализ и интерпретация лучевых снимков, электронная медкарта, система диагностики, управление медсервисами, «цифровая реанимация» и другие медицинские сервисы показали высокую эффективность [Сизов Г., 2024: 41–52].

Уровень цифровизации здравоохранения наиболее полно оценивается посредством определения «цифровой зрелости», т.е. использования цифровых систем и технологий в оказании медицинской помощи, управлении здравоохранением и взаимодействия с пациентами, который отражает уровень интеграции информационных технологий в бизнес-процессы медицинских организаций, качество их использования и соответствие требованиям законодательства.

В соответствии с Указом Президента Российской Федерации от 28.11.2024 № 1014 «Об оценке эффективности деятельности высших

должностных лиц субъектов Российской Федерации и деятельности исполнительных органов субъектов Российской Федерации» критерий «цифровой зрелости» применяется для оценки государственного управления, в том числе в здравоохранении⁶. Достижение «цифровой зрелости» в рассматриваемой сфере определено Указом Президента России от 7.05.2024 №309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»⁷, названо одной из главных целей национального развития и предполагает в том числе автоматизацию большей части транзакций в рамках единых отраслевых цифровых платформ и модели управления на основе данных в русле ускоренного внедрения технологий обработки больших объемов данных, машинного обучения и ИИ.

Компонентами цифровой зрелости являются медицинские информационные системы, дистанционные формы взаимодействия и медпомощи (телемедицина), цифровые инструменты управления медицинскими данными и услугами и т.д. В частности, ст. 9.1 Федерального закона от 21.11.2011 № 323-ФЗ⁸ предусматривает формирование Единой государственной информационной системы в сфере здравоохранения (далее—ЕГИСЗ), которая действует в соответствии с обновленным Положением, утвержденным Постановлением Правительства Российской Федерации от 09.02.2022 № 140⁹. ЕГИСЗ —комплекс, включающий федеральные интеграционные системы: реестры медицинских и фармацевтических работников и организаций, электронных медицинских документов и нормативно-справочной информации в сфере здравоохранения; электронную регистратуру; интегрированную электронную медицинскую карту. Он содержит ряд подсистем, в том числе реестров лекарственных препаратов для медицинского применения; автоматизированного сбора информации о показателях здравоохранения из различных источников и отчетности; обезличивания персональных данных; геоинформационную подсистему; подсистему защиты информации. ЕГИСЗ реализует ряд функций: идентификации и систематизации сведений о лицах, содержащихся в подсистемах единой системы, управления базами данных, формирования единого хранилища данных, защиты информации, информационно-технологического взаимодействия подсистем единой системы между собой и с иными информационными системами, а также выполняет функции общесистемных технологических сервисов.

Цифровая зрелость определяется также как расчетный показатель, устанавливаемый по методике, утвержденной приказом Минцифры от

⁶ Собрание законодательства РФ. 2024. № 49 (Часть V). Ст. 7576.

⁷ Собрание законодательства РФ. 2024. № 20. Ст. 2584.

⁸ Собрание законодательства РФ. 2011. № 48. Ст. 6724.

⁹ Available at: URL: <http://pravo.gov.ru> (дата обращения: 27.12.2025)

28.12.2024 № 1210. Федеральный закон от 28.11.2025 № 426-ФЗ «О федеральном бюджете на 2026 год и на плановый период 2027 и 2028 годов» (таблица 165)¹⁰ предусматривает создание единого цифрового контура в общественном здравоохранении, внедрение медицинских информационных систем и государственных информационных систем в сфере здравоохранения, обеспечивающих взаимодействие с ЕГИСЗ и в медицинских организациях государственной системы здравоохранения. Цифровая зрелость определяет степень использования цифровых систем и технологий в процессах оказания медицинской помощи, управления здравоохранением и взаимодействия с пациентами, а также отражает уровень интеграции ИТ в бизнес-процессы медицинских организаций, качество их использования и соответствие требованиям законодательства.

Основная цель достижения цифровой зрелости — повышение качества и доступности медицинской помощи. Цифровая зрелость отражает уровень использования цифровых технологий, платформенных решений и компьютерных приложений при оказании медицинской помощи, уровень управления здравоохранением и взаимодействия с пациентами. Она показывает степень интеграции цифровых ИТ в бизнес-процессы медицинских организаций, качество их использования и соответствие требованиям законодательства для достижения основной цели — повышение качества и доступности медицинской помощи.

Особенности цифровой трансформации здравоохранения требуют современных инструментов оценки цифровой зрелости медицинских организаций. Критерии оценки цифровой зрелости могут зависеть от методологии применяемой модели. Практика показывает большое количество примеров применения таких моделей [Вошев В., 2023: 615—627]. Действует Electronic Medical Record Adoption Model — модель, разработанная международной организацией Healthcare Information and Management Systems Society, которая оценивает по шкале от 0 до 7 степень интеграции электронных медицинских записей и цифровых решений в деятельности медицинских организаций.

В России опыт Минздрава позволил создать методику объективной и системной оценки уровня цифровой зрелости, которая фиксирует особенности структуры и деятельности организаций, адаптивность к различным уровням здравоохранения, способствует стандартизации цифровой трансформации, обеспечивает идентификацию и анализ проблемных зон и разработку рекомендаций для повышения цифровой зрелости организаций. Методика содержит алгоритм расчета уровня цифровой зрелости, позволяет определить уровень их готовности к цифровой трансформации, охватывает основные аспекты цифровизации, обеспечивая комплексный подход к анализу и выявлению затруд-

¹⁰ Собрание законодательства РФ. 2025. № 48 (Часть I–III). Ст. 7237.

няющих цифровую трансформацию проблем и позволяет формировать рекомендации к их устранению.

Применение телемедицинских технологий распространяется как в России, так и за рубежом. Так, по ст. 36.2 Федерального закона от 21.11.2011 № 323-ФЗ медицинская помощь с применением телемедицины организуется и оказывается в установленном Минздравом порядке на основе клинических рекомендаций и в соответствии со стандартами. С применением телемедицинских технологий допускаются консультации лечащего врача, а также дистанционное наблюдение за состоянием пациента на основании данных о нем, зарегистрированных с применением медицинских изделий, предназначенных для мониторинга состояния организма человека, и (или) на основании данных, внесенных в ЕГИСЗ или государственную информационную систему субъекта федерации. Применение телемедицинских технологий допускается клиниками частной системы здравоохранения — участников экспериментального правового режима в сфере цифровых инноваций в соответствии с программой такого режима в сфере цифровых инноваций, утверждаемой в соответствии с Федеральным законом от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации»¹¹. Порядок организации и оказания медицинской помощи с применением телемедицинских технологий утвержден приказом Минздрава России от 11.04.2025 № 193н.

В ст. 34 Федерального закона от 21.11.2011 № 323-ФЗ выделен самостоятельный вид медицинской помощи — специализированная помощь, включающая профилактику, диагностику и лечение болезней и состояний (в том числе в период беременности, родов и послеродовой период), требующих использования специальных методов и медицинских технологий, а также реабилитацию. Специализированная, в том числе высокотехнологичная помощь оказывается в медицинских и иных организациях государственной, муниципальной и частной систем здравоохранения, имеющих лицензии.

Высокотехнологичная медицинская помощь, являющаяся частью специализированной медицинской помощи, означает применение новых сложных и (или) уникальных методов, а также ресурсоемких методов лечения с научно доказанной полезностью, в том числе клеточных технологий, роботизированной техники, информационных технологий и методов геномной инженерии, разработанных на основе достижений медицинской науки и смежных отраслей науки и техники. Такая помощь оказывается в соответствии с Приказом Минздрава России от 11.04.2025 № 186н по перечню видов высокотехнологичной медицинской помощи. Приказ содержит методы лечения и источники ее финансирования,

¹¹ Собрание законодательства РФ. 2021. № 27 (часть I). Ст. 5159.

установленные в рамках программы государственных гарантий бесплатной медицинской помощи, которые включают в том числе перечень видов высокотехнологичной медицинской помощи с использованием уникальных методов лечения. Помощь оказывают медицинские организации, включенные в единый реестр.

Перспективы цифрового здравоохранения связаны прежде всего с комплексным развитием этого направления. В соответствии с поручением Президента Российской Федерации распоряжением Правительства от 17.04.2024 №959р утверждено Стратегическое направление в области цифровой трансформации здравоохранения¹², которое во многом определило перспективы развития отечественного цифрового здравоохранения, поставило цель достижения высокого уровня показателя «цифровой зрелости» и ускоренного перехода здравоохранения на новые управленческие и технологические уровни с полным переходом к «цифровым двойникам» и других «сквозным» технологиям, тем самым обеспечив создание платформенной экосистемы на основе целостных и однородных первичных данных.

Стратегически цифровое преобразование выполняет более широкую задачу — оно способствует достижению технологического суверенитета и обеспечивает условия развития здравоохранения и долгосрочного устойчивого социально-экономического развития страны в условиях динамизма внешних и внутренних факторов. Цифровая трансформация здравоохранения осуществляется на основе отечественных ИКТ, обеспечивающих технологический суверенитет, в том числе отечественных «сквозных» цифровых технологий, а также на базе платформизации, т.е. формирования отраслевой технической политики в области ИКТ, единых подходов к построению архитектуры информационных систем здравоохранения, в том числе формирования компонентов отраслевой архитектуры информационных систем на базе общих инструментов их моделирования и описания. Процесс цифровой трансформации здравоохранения строится на общих информационных моделях, на унификации стандартов обмена информацией и на регламентации взаимодействия различных систем и субъектов, а также на создании инфраструктурной платформы для решения задач на всех уровнях управления, что обеспечит высокий уровень информационной безопасности. Особое внимание уделяется формированию цифровой экосистемы сбора, обработки и использования данных в целях повышения качества медицинской помощи, развитию биомедицинских исследований, внедрению индивидуальных электронных медицинских устройств, а также технологиям динамического наблюдения с использованием платформ централизованных диагностических сервисов.

¹² Собрание законодательства РФ. 2024. № 17. Ст. 2388.

Реализация перспективных целей и задач цифровизации осуществляется в рамках политики цифровой трансформации Минздравом и другими участниками домена «Здравоохранение» посредством применения платформы «ГосТех» и с соблюдением принципов клиентоцентричности.

Определены основные технологии реализации этой политики. В частности, ИИ будет применен при автоматизации процессов, оптимизации ресурсов, обнаружении аномалий и для аналитической информации для поддержки решений в сфере здравоохранения. Технологии работы с большими данными помогут предиктивному моделированию при разработке лекарств и совершенствовании лечения. Анализ больших данных позволит повысить точность планирования клинических исследований. Технологии беспроводной связи в контексте платформ технологического управления будут использоваться для связи между различными устройствами и системами. Отраслевые цифровые технологии будут применяться в рамках домена «Здравоохранение» во всех необходимых в соответствии с законодательством объектах и процессах.

При этом важна сертификация носимых устройств и других медицинских изделий (предусмотрено в ст. 38 Федерального закона № 323-ФЗ, чтобы считать их цифровыми медицинско-диагностическими изделиями — устройствами, приборами, а не инструментами поддержания здоровья (каковы часы-трекеры, «умные» браслеты и т.п.).

Оперативность регулирования цифровых технологий осуществляется посредством правового механизма режимов, вводимых в соответствии с Федеральным законом от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций» (ред. от 31.07.2025)¹³. Отработка правового регулирования в экспериментальном режиме правового регулирования (режим «песочницы») позволяет оперативно опробовать особенности правового регулирования цифровых технологий одновременно с выработкой правовых средств и механизмов их применения в здравоохранении.

В медицине за последние годы такой механизм применяется широко. К примеру, постановлением Правительства Российской Федерации от 09.12.2022 № 2276 установлен экспериментальный правовой режим в сфере цифровых инноваций медицинской деятельности с применением технологий сбора и обработки сведений о состоянии и диагнозах граждан в отношении реализации инициативы социально-экономического развития «Персональные медицинские помощники» (ПМП). С помощью средств такого правового механизма осуществляются прием, обработка, хранение и передача в информационные системы медицинских организаций показателей измерений медицинских изделий, зарегистри-

¹³ Собрание законодательства РФ. 2020. № 31 (часть I). Ст. 5017.

рованных по Правилам государственной регистрации медицинских изделий (утверждены постановлением Правительства от 27.12. 2012 № 1416).

Пилотное дистанционное наблюдение за состоянием пациента с использованием информационной системы (платформы) ПМП подтвердило пользу применения технологии дистанционного мониторинга состояния пациентов с использованием дистанционных устройств, отработаны механизмы безопасного информационного взаимодействия информационных систем. В 2024 году создана информационная система ПМП, интегрированная с ЕГИСЗ. Платформа ПМП контролирует соответствие движения данных национальному стандарту ПНСТ 995-2024 «Системы киберфизические. ПМП. Форматы обмена данными. Общие требования». Сделан вывод о допустимости придания специальному регулированию свойства общего регулирования¹⁴.

Постановлением Правительства Москвы от 31.10.2025 №1706 на ее территории на три года установлен экспериментальный правовой режим цифровых и технологических инноваций по подписанию информированного добровольного согласия на медицинское вмешательство или отказа от него с использованием электронной графической подписи.

Биометрические персональные данные, к которым относятся характеризующие физиологические и биологические особенности человека сведения, на основании которых можно установить его личность, имеют особый правовой режим и порядок обработки и использования в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ (ред. от 24.06.2025) «О персональных данных»¹⁵, Федеральным законом от 29.12.2022 № 572-ФЗ (ред. от 28.12.2024) «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации»¹⁶. К биометрическим данным относятся фото- и видеоизображения человека, его дактилоскопические данные, анализ ДНК, данные о голосе и радужной оболочке глаз.

Особая сфера регулирования медицины — биобанки, в которых хранятся биологические материалы человека, биомедицинские клеточные продукты на условиях и в порядке, указанные в ст. 37 Федерального закона от 23.06.2016 № 180-ФЗ (ред. от 04.08.2023) «О биомедицинских кле-

¹⁴ Сводный аналитический отчет Минэкономразвития от 05.12.2025. Available at: URL: https://www.economy.gov.ru/material/file/download/3ffe5db176a775124b76812453fdf362/svodniy_analiticheskiy_otchet_122025.pdf (дата обращения: 13.11.2025)

¹⁵ Собрание законодательства РФ. 2006. № 31 (часть I). Ст. 3451.

¹⁶ Там же. 2023. № 1 (часть I). Ст. 19.

точных продуктах»¹⁷ при сохранении их биологических свойств и предотвращении их инфицирования и загрязнения. Биобанки пока являются новой для российского права категорией [Останина Е., 2023: 66–67]; [Мохов А., 2021: 343], связанной с хранением большого количества биоматериала пациентов, аналогично биобанку Международного сообщества биологических и экологических репозиториям. Один из немногих отечественных примеров — Биобанк наследственной патологии. Это коллекция биологических образцов (ДНК, крови, тканей, клеток и др.), собранных на базе НИИ медицинской генетики Томского НИМЦ¹⁸.

Практика показывает, что цифровая трансформация здравоохранения может порождать и негативные последствия. Она не гарантирует исключения врачебных ошибок, низкокачественных медицинских услуг, утечки данных, что обуславливает применение более совершенных технологий и соблюдение всех действующих нормативных актов каждой национальной юрисдикции [Osadchuk M., 2020: 148–155]. К примеру, внедрение синтетических данных при использовании ИИ в исследованиях и диагностике порождает и проблемы «синтетического доверия» — необоснованной уверенности в моделях, обученных на искусственно сгенерированных наборах данных, которые не соответствуют клинической достоверности или демографическим реалиям. Необходимы действенные меры предосторожности при использовании медицинского ИИ, в том числе стандарты обучающих данных, тестирование на уязвимость в процессе разработки и раскрытия информации о происхождении синтетических данных для обеспечения полной подотчетности. Эти меры обеспечивают целостность и справедливость данных в клинических приложениях, предлагают новые стандарты ответственного и справедливого использования синтетических данных в здравоохранении [Koul A., Duran D., 2025: 2–5].

Цифровые технологии допускают риски неблагоприятных последствий: нежелательных лекарственных реакций или ошибок в приеме лекарств. Небезопасные методы лечения могут возникать на разных этапах процесса, включая ошибочные назначения лекарств (их несоответствие возрасту и состоянию, неправильная дозировка, противопоказания и невнимательность к лекарственным взаимодействиям), ошибки при выдаче и назначении, а также неправильный мониторинг лечения [Insani W. et al., 2025: 27]. Применение биотехнологий тоже связано с рисками, включая негативное влияние на здоровье; это обратная сторона лечения и профилактики болезней¹⁹.

¹⁷ Там же. 2016. № 26 (часть I). Ст. 3849.

¹⁸ Available at: URL: <https://www.medgenetics.ru/institut/bank/> (дата обращения: 13.11.2025)

¹⁹ WEF. Global Risks Report. January 2025. P. 53–55. Available at: URL: <https://www.weforum.org/publications/global-risks-report-2025> (дата обращения: 13.11.2025)

Помимо указанных рисков перед здравоохранением стоят и этические проблемы, например, относительно технологии ИИ, которые определены в Кодексе этики применения искусственного интеллекта в сфере охраны здоровья²⁰. К ним, в частности, относятся: повышенный риск причинения вреда здоровью в силу потенциальных ошибок обработки данных и знаний, а также заключений (рекомендаций), формируемых ИИ; проблемы кибербезопасности, включая несанкционированное вмешательство в алгоритмы работы ИИ или доступ к персональным данным пациентов и др.

Обостряется проблема ответственности за врачебную ошибку в условиях применения ИИ, хотя судебная и правоприменительная практика только формируется. Врач несет уголовную, а медицинское учреждение — гражданско-правовую ответственность за некачественные медицинские услуги. Применение деликтной ответственности, как отмечают специалисты [Гришин С., Одинцов С., 2024: 43–50], для определения вины врача, который использовал технологии ИИ, не однозначно. Нейросети показывают более высокие показатели точности, чем врачи. Однако итоговое заключение делает врач, а не ИИ.

В соответствии с доктриной «responsible infinitor» [Kamensky S., 2020: 9], предусматривающей ответственность работодателя за неосторожное причинение вреда работником при выполнении трудовой функции, медицинская организация отвечает за то, что ее руководители не полностью обучали и контролировали работников при применении технологий ИИ. Однако возложение ответственности на ИИ будет означать признание его правосубъектности, что противоречит законодательству. Вместе с тем широкое применение ИИ, по мнению ряда ученых [Magrani E., 2019: 7–8]; [Иванова А., 2021: 155], может повлечь профессиональную деградацию врачей и утрату ими навыков диагностирования. Невозможно забывать и о «галлюцинациях» ИИ при вынесении решения или постановке диагноза, что тоже приводит к врачебным ошибкам. В цифровой медицине проблема ответственности — одна из самых жгучих, а в условиях применения ИИ и других цифровых технологий появляются дополнительные риски и угрозы, что усложняет структуры правоотношений и, соответственно, структуры ответственности участников таких правоотношений.

Вместе с тем достижения цифровой медицины означают формирование направлений, вызванных прогрессом биомедицины и биотехнологий, что в свою очередь способствует становлению новых направле-

²⁰ Утв. Межведомственной рабочей группой при Минздраве по вопросам создания, развития и внедрения в клиническую практику медицинских изделий и сервисов с использованием технологий искусственного интеллекта, протокол от 14.02.2025 № 90/18-0/117. Available at: URL: <https://portal.egisz.rosminzdrav.ru/default/06/kodeks-etiki-primenenia-iskusstvennogo-intellekta-v-sfere-ohrany-zdorov-a-1.pdf> (дата обращения: 13.11.2025)

ний правового регулирования — концепций нейроправа, биоправа и др. [Кравец И., 2022: 130].

Развитие правовой базы цифрового здравоохранения означает прежде всего разработку нормативных актов, регулирующих порядок применения технологий в цифровизации медицинской деятельности и медпомощи, в том числе посредством оптимального механизма экспериментальных правовых режимов в отдельных видах медицинской деятельности с целью последующего применения результатов в правовом регулировании. Примеры: внедрение электронной графической подписи при оформлении информированного добровольного согласия на медицинское вмешательство или отказа от него; применение технологий сбора и обработки сведений о состоянии здоровья и о диагнозах граждан.

Цифровизация затрагивает и документооборот. Новации применимы также при его внедрении, установлении взаимодействия медучреждений и регуляторов в электронном формате. Так, внесенные в Федеральный закон от 12.04.2010 № 61-ФЗ (ред. от 29.12.2025) «Об обращении лекарственных средств»²¹ изменения предусматривают перевод большинства процедур регистрации и оборота лекарственных средств в электронный формат с использованием ФГИС «Госуслуги» и ЕГИСЗ. Закон разрешает оформлять информационный листок пациента о согласии на участие в клинических испытаниях как в электронном виде, так и в бумажном. Кроме того, разработка и применение высокотехнологичных медицинских препаратов потребовала внесения в Закон нового понятия «высокотехнологичного лекарственного препарата». Это генотерапевтический лекарственный препарат, или лекарственный препарат на основе соматических клеток, или продукт тканевой инженерии.

Заключение

Цифровое здравоохранение формирует уникальные перспективы развития цифрового здравоохранения и правового регулирования. Цифровые технологии являются важным компонентом и движущей силой формирования устойчивых систем здравоохранения. Для создания экосистемы цифрового здравоохранения необходимо развивать отечественную стратегию цифровизации данной сферы. Экосистема позволит объединить финансовые, организационные, человеческие и технологические ресурсы, а также обеспечит координацию между многочисленными заинтересованными участниками системы цифрового здравоохранения в целях установления приоритетов, стандартов и системной цифровой IT- архитектуры, реализуя необходимую их интеграцию.

²¹ Собрание законодательства РФ. 2010. № 16. Ст. 1815.

Цифровое здравоохранение приносит пользу как пациенту, так и обществу. Концепция цифрового здравоохранения реализуется в ракурсе требований, связанных с цифровыми решениями, которые включают: подход к медицинской помощи, основанный на биологических данных; использование цифровых инструментов отслеживания результатов лечения и улучшения доступа к медицинской помощи; расширение возможностей телемедицины и прочих дистанционных медицинских услуг, а также совершенствование методов финансирования для снижения затрат. Биометрические данные особенно важны, так как они дают четкое понятие о проблемах с доступом к медицинской помощи и позволяют целенаправленно помогать пациентам. Распространение телемедицины и робототехнических устройств (роботов-хирургов, роботов-помощников) позволяет улучшать взаимодействие пациентов и врачей независимо от их местонахождения, а ряд мобильных инструментов повышает уровень профилактики. Становится очевидным, что на стыке технологий и здравоохранения возникла быстро развивающаяся правовая сфера — цифровое здравоохранение. По мере того, как инновации в сфере медицинских технологий преобразуют отрасль, потребность в комплексной системе нормативных актов, регулирующих правоотношения в сфере цифровой медицины становится животрепещущей. В связи с этим есть смысл создать специальный раздел, посвященный вопросам цифрового здравоохранения, в Федеральном законе от 21.11.2011 №323-ФЗ, включив в его текст нормы о целях и задачах цифровой медицины, стратегии ее развития, ее направлениях и принципах.



Список источников

1. Вошев Д.В. Обзор методологий и моделей оценки цифровой зрелости в медицинских организациях, оказывающих первичную медико-санитарную помощь // Наука молодых. 2023. № 4. С. 615–627.
2. Гришин С.М., Одинцов С.В. Тенденции электронного здравоохранения и особенности практики рассмотрения споров по оказанию медицинских услуг с применением цифровых технологий // Проблемы экономики и юридической практики. 2024. № 5. С. 43–50.
3. Иванова А.П. Правовые проблемы использования искусственного интеллекта в сфере здравоохранения // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Государство и право. Реферативный журнал. 2021. № 1. С. 151–159.
4. Кравец И.А. Бионейроконституционализм и достоинство: теоретические основы, диалог этических и юридических требований и перспективы взаимодействия // Журнал российского права. 2022. № 6. С. 5–31. DOI: 10.12737/jrl.2022.059.
5. Малеина М.Н. Правовой статус биобанка (банка биологических материалов человека) // Право. Журнал Высшей школы экономики. 2020. № 1. С. 99–100.

6. Малеина М.Н. Правовое регулирование применения медицинских роботов-хирургов в комплексе цифровых технологий // Медицинское право. 2023. № 1. С. 2–5.
7. Мохов А.А. Биобанкам и биобанковской деятельности — надлежащее правовое обеспечение. Биозкономика: доктрина, законодательство, практика. М.: Проспект, 2021. С. 339–349.
8. Останина Е.А. Биобанк как правовая категория // Юридический вестник Самарского университета. 2023. № 2. С. 66–67.
9. Пугачев П.С., Гусев А.В. и др. Мировые тренды цифровой трансформации отрасли здравоохранения // Национальное здравоохранение. 2021. № 2. С. 5–12.
10. Сизов Г.Г. Цифровая трансформация первичной медико-санитарной помощи в Москве // Национальное здравоохранение. 2024. № 3. С. 41–52.
11. Тарасенко Т.Д. и др. Методика оценки цифровой зрелости медицинских организаций // Врач и информационные технологии. 2025. № 3. С. 76–89.
12. Шереметьева Н.В. Правовое регулирование и охрана применения робототехники и искусственного интеллекта в медицинской деятельности // Медицинское право. 2024. № 3. С. 40–43.
13. Azarfar G. et al. Responsible adoption of multimodal artificial intelligence in health care: promises and challenges. *The Lancet Digital Health*, 2025, vol. 7, iss. 12, p. 100917. DOI: 10.1016/j.landig.2025.100917
14. Backman J. et al. Exome sequencing and analysis of 454,787 UK Biobank participants. *Nature*, 2021, vol. 599, pp. 628–634. doi:10.1038/s41586-021-04103-z
15. Bogdanovskaya I. et al. Artificial Intelligence and Law: From Theory to Practice. *Legal Issues in the Digital Age*, 2025, vol. 6, no. 1, pp. 124–147. DOI: 10.17323/2713-2749.2025.1.124.148
16. Bontempi D. et al. Face Age, a deep learning system to estimate biological age from face photographs to improve prognostication: a model development and validation study. *The Lancet Digital Health*, 2025, vol. 7, iss. 6, p. 100870.
17. Cao X., Liu T. et al. Recent advances in nanozyme-based sensing technology for antioxidant detection. *Sensors*, 2024, vol. 24(20), p. 6616.
18. Cortes A., Johnston I. et al. The UK Biobank Whole-Genome Sequencing Consortium. Whole-genome sequencing of 490,640 UK Biobank participants. *Nature*, 2025, vol. 645, pp. 670–692. <https://doi.org/10.1038/s41586-025-09272-9>
19. Florea L., Diamond D. Sensors and “The internet of biochemical things”. *Frontiers in Sensors*, 2022, vol. 3, pp. 1–7. <https://doi.org/10.3389/fsens.2022.1010212>
20. Garg M., Karpinski M. et al. Disease prediction with multi-omics and biomarkers empowers case-control genetic discoveries in the UK Biobank. *Nature Genetics*, 2024, vol. 56, pp. 1821–1831. <https://doi.org/10.1038/s41588-024-01898-1>
21. Insani W. et al. Digital Health Technology Interventions for Improving Medication Safety: Systematic Review of Economic Evaluations. *Journal of Medical Internet Research*, 2025, pp. 1–16. DOI: 10.2196/65546
22. Kamensky S. Artificial Intelligence and Technology in Health Care: Overview and Possible Legal Implications. *De Pual Journal of Health Care Law*, 2020, vol. 21, no. 3, pp. 4–12.

23. Koul A., Duran D. et al. Synthetic data, synthetic trust: navigating data challenges in the digital revolution. *Lancet Digital Health*, 2025, vol. 7, iss. 11, pp. 1–7. DOI: 10.1016/j.landig.2025.100924
24. Lee B., Ghovanloo M. An overview of data telemetry in inductively powered implantable biomedical devices. *IEEE Communications Magazine*, 2019, vol. 57, no. 2, pp. 74–80. DOI:10.1109/MCOM.2018.1800052
25. Lino C., Barrias S. et al. Biosensors as diagnostic tools in clinical applications. *Biochimica et Biophysica Acta. Reviews on Cancer*, 2022, vol. 1877(3), p. 188726.
26. Magrani E. New perspectives on ethics and the laws of artificial intelligence. *Internet policy review*, 2019, vol. 8, no 3, pp. 4–10. DOI: 10.14763/2019.3.1420
27. Maity D., Guha P., Buchmann P., Mansouri M., Fussenegger M. Blood-Glucose-Powered Metabolic Fuel Cell for Self-Sufficient Bioelectronics. *Advanced Materials*, 2023, vol. 35, iss. 21, pp. 1–14. DOI:10.1002/adma.202300890
28. Nusinovici S. et al. Retinal photograph-based deep learning predicts biological age, and stratifies morbidity and mortality risk. *Age and Ageing*, 2022, no. 4, pp. 1–9.
29. Osadchuk M.A. et al. Legal Regulation in Digital Medicine. *Journal of Advanced Research in Law and Economics*, 2020, vol. 11, no. 1, pp. 148–155.
30. Raghu V., Weiss J. et al. Deep Learning to Estimate Biological Age From Chest Radiographs. *Journal of American College Cardiol Img.*, 2021, vol. 14, pp. 2226–2236.
31. Ringeve M., Armel F. et al. Advancing Health Care With Digital Twins: Meta-Review of Applications and Implementation Challenges. *Journal of Medical Internet Research*, 2025, vol. 27, p. 44. <https://www.jmir.org/2025/1/e69544>
32. Sen A., Oswalia J. et al. Recent trends in nanozyme research and their potential therapeutic applications. *Current Research in Biotechnology*, 2024, vol. 7, p. 100205. <https://doi.org/10.1016/j.crbiot.2024.100205>
33. Schroer D., Simon S., Trommer G. Medtech's Generative AI Opportunity. Available at: URL: <https://www.bcg.com/publications/2023/generative-ai-in-medtech>
34. Thirumala M., Monika S. Transforming Healthcare: The power and potential of digital medicine. *Future Science OA*, 2024, vol. 10, no. 1, p. 2430357. DOI: 10.1080/20565623.2024.2430357
35. Zalatan J., Petrini L. et al. Engineering bacteria for cancer immunotherapy. *Current Opinion in Biotechnology*, 2024, vol. 85, pp. 1–13. DOI: 10.1016/j.copbio.2023.103061
36. Zargartalebi H., Mirzaie S. et al. Active-reset protein sensors enable continuous in vivo monitoring of inflammation. *Science*, 2024, vol. 386, pp. 1146–1153.
37. Zhou H., Baptista-Hon D. et al. Concepts and applications of digital twins in healthcare and medicine. *International Consortium of Digital Twins in Medicine*, 2024, vol. 5, iss. 9, p. 101028. <https://doi.org/10.1016/j.patter.2024.101028>

Информация об авторе:

А.А. Карцхия — доктор юридических наук, доцент.

Статья поступила в редакцию 22.11.2025; одобрена после рецензирования 22.12.2025; принята к публикации 19.01.2026.

Научная статья

JEL: K00

УДК 004:34(063)

DOI:10.17323/2713-2749.2026.1.121.140

Правовые особенности практики внедрения IoT-систем в организациях (учреждениях) Республики Татарстан



**Кирилл Радикович Кирушин¹,
Данил Ильдарович Сафин²**

^{1,2} Набережночелнинский государственный педагогический университет,
Россия 423806, Республика Татарстан, Набережные Челны, ул. Р.М. Низа-
метдинова, 28,

¹ k.kirushin@mail.ru, <https://orcid.org/0000-0002-8958-3673>

² danil-safin-2018@mail.ru, <https://orcid.org/0000-0002-2375-5225>



Аннотация

Внедрение технологий Интернета вещей (IoT) в ключевые секторы экономики регионов России, включая промышленность, жилищно-коммунальное хозяйство, логистику и здравоохранение, создает значительные правовые вызовы, связанные с безопасностью обрабатываемых данных. Настоящая статья посвящена комплексному анализу правовых особенностей практики внедрения IoT-систем в организациях и учреждениях Республики Татарстан, выступающей одним из лидеров цифровой трансформации в Российской Федерации. Целью исследования является выявление правовых проблем, возникающих при обработке данных с использованием умных устройств, а также разработка научно обоснованных предложений по совершенствованию соответствующих механизмов регионального правового регулирования и правоприменения. Методологическую основу работы составили анализ федерального и регионального нормативно-правового регулирования в сфере защиты информации и персональных данных, обобщение и систематизация региональной судебной

практики за период 2020-2024 годов, а также эмпирическое исследование локальных актов организаций, включая типовые согласия на обработку данных и практику правового просвещения сотрудников. В результате исследования установлено, что цифровизация отраслей экономики республики сопровождается формированием существенных правовых пробелов, включая неопределенность правового режима данных, генерируемых IoT-устройствами, отсутствие норм, регулирующих оборот такой информации, и разрозненность технических стандартов защиты. Авторами предложен комплекс мер, включающий разработку концепции правового режима для IoT-данных, основанного на дифференциации по степени риска и принципе контекстуальной анонимизации, а также дополнение регионального законодательства типовыми требованиями к обработке данных. Особое внимание уделено обоснованию модели дифференциации административной ответственности за нарушения в исследуемой сфере. Практическая значимость работы заключается в формировании конкретных правовых механизмов, направленных на минимизацию юридических рисков операторов и обеспечение баланса между технологическим развитием и защитой прав субъектов данных. Предложенные авторами решения могут быть применены как в Республике Татарстан, так и в других субъектах Российской Федерации, сталкивающихся с аналогичными правовыми проблемами в условиях цифровой трансформации экономики.



Ключевые слова

Интернет вещей; персональные данные; Республика Татарстан; региональное законодательство; IoT-системы; умные устройства; защита данных; административная ответственность.

Благодарности: статья опубликована в рамках проекта по поддержке публикаций авторов российских образовательных и научных организаций в научных изданиях НИУ ВШЭ.

Для цитирования: Кирушин К.Р., Сафин Д.И. Правовые особенности практики внедрения IoT-систем в организациях (учреждениях) Республики Татарстан // Вопросы права в цифровую эпоху. 2026. Том 7. № 1. С. 121–140. DOI:10.17323/2713-2749.2026.1.121.140

Введение

В Республике Татарстан процессы цифровой трансформации экономики приобретают все более выраженный системный характер, особенно для регионального хозяйства. Данная тенденция требует тщательного анализа, поскольку сопряжена с необходимостью соблюдения целого комплекса нормативных требований, регулирующих обработку и защиту данных, функционирование критической информационной инфраструктуры, а также обеспечение информационной безопасности в условиях растущей цифровизации. Базовое правовое регулирование в сфере обработки и защиты персональных

данных осуществляется на федеральном уровне, в частности — Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»¹. Однако на федеральном уровне устанавливаются общие принципы, в то время как вопросы конкретизации и детализации этих норм, особенно в отраслевом и региональном разрезе, требуют участия субъектов Российской Федерации.

Исследование правового регулирования защиты персональных данных, получаемых IoT-устройствами на примере Республики Татарстан, показывает, что сегменты промышленности, ЖКХ, логистики и здравоохранения республики демонстрируют высокую степень внедрения IoT-технологий. Поэтому изучение регионального правоприменения и возможностей совершенствования таких правовых механизмов (в рамках полномочий субъектов федерации) на примере указанных сегментов позволит выработать предложения, значимые как для Татарстана, так и для других регионов России.

1. Анализ практики внедрения IoT и правовых вызовов в ключевых отраслях Республики Татарстан

Рассматривая промышленную сферу как один из приоритетных сегментов внедрения IoT, нетрудно заметить, что предприятия машиностроительного и нефтегазохимического комплексов республики демонстрируют внедрение наиболее продвинутых практик интеграции «умных» технологий. На производственных площадках КАМАЗа и Завода имени Серго развернуты комплексные платформы промышленной IoT-системы, обеспечивающей непрерывный сбор и анализ данных с технологического оборудования². Внедрение датчиков вибрации, температурных сенсоров и приборов учета энергопотребления не только позволяет оптимизировать производственные процессы, но и приводит к возникновению новых правовых вызовов, связанных с классификацией и защитой собираемой информации. Суть этих вызовов заключается в правовой неопределенности: телеметрические данные, собираемые с оборудования, могут одновременно содержать признаки персональных данных (например, при привязке станка к конкретному оператору), коммерческой тайны (параметры качества производства) и технической информации, не охраняемой специальными режимами.

Отсутствие четких критериев разграничения этих режимов в федеральном законодательстве затрудняет предприятиям выбор надлежащих мер защиты и создает риски привлечения к ответственности за их неприменение. По зако-

¹ Федеральный закон от 27.07.2006 № 152-ФЗ (последняя редакция) «О персональных данных» // СЗ РФ. 2006. № 31. Ст. 3451.

² КАМАЗ планирует на 20% поднять загрузку оборудования при помощи искусственного интеллекта. Available at: URL: https://vestikamaza.ru/posts/kamaz_planiruet_na_20_podnyat_zagruzku_oborudovaniya_pri_pomoshhi_iskusstvennogo_intellekta/ (дата обращения: 20.11.2025)

нодательству РФ и Республики Татарстан часть таких данных подпадает под определение коммерческой тайны либо относится к сведениям ограниченного доступа, что требует разработки предприятиями локальных нормативных актов, регламентирующих порядок их обработки, хранения и передачи³.

Особого внимания заслуживает правовое регулирование телеметрических данных, генерируемых на объектах нефтегазохимического комплекса республики. Как показывает практика ведущих предприятий отрасли (например, Татнефти и Нижнекамскнефтехима⁴), внедрение удаленного мониторинга скважин и трубопроводов, фиксирующих параметры давления, состав флюидов и коррозионных процессов, формируют массив информации, который одновременно обладает экономической ценностью и потенциальной уязвимостью с точки зрения информационной безопасности. Правовая проблема в таком случае носит не индивидуальный, а отраслевой характер.

Поскольку нефтегазовый сектор отнесен к критической информационной инфраструктуре, операторы обязаны соблюдать требования Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»⁵, которые налагают дополнительные обязанности по защите данных, но при этом не всегда учитывают специфику их автоматического сбора IoT-устройствами. В связи с этим предприятия вынуждены выстраивать многоуровневые механизмы защиты, сочетающие технические средства шифрования с правовыми инструментами — договорами о неразглашении, соглашениями о конфиденциальности с контрагентами, а также с внутренними регламентами по управлению доступом к данным.

В сфере ЖКХ Татарстана внедрение IoT-технологий осуществляется преимущественно в рамках концепции «умного города», что предполагает масштабную цифровизацию систем учета и управления ресурсами. В Казани, Набережных Челнах и Альметьевске активно разворачиваются автоматизированные системы коммерческого учета энергоресурсов (далее — АСКУЭ), включающие «умные» счетчики электроэнергии, воды и тепла, передающие

³ Приказ Министерства промышленности и торговли Республики Татарстан от 15.03.2023 № 44-ОД «Об утверждении Политики безопасности обработки персональных данных Министерства промышленности и торговли Республики Татарстан» // СПС КонсультантПлюс.

⁴ Татнефть формирует IT-кластер. Available at: URL: <https://rg.ru/2018/12/11/reg-pfo/tatneft-formiruet-it-klaster.html> (дата обращения: 20.11.2025); СИБУР получил экономический эффект 6,5 млрд рублей от внедрения цифровых технологий в 2024 году. Available at: URL: https://op-ex.ru/post_news/sibur-poluchil-ekonomicheskij-effekt-65-mlrd-rublej-ot-vnedreniya-czifrovyh-tehnologij-v-2024-godu/ (дата обращения: 24.11.2025)

⁵ Федеральный закон от 26.07.2017 № 187-ФЗ (последняя редакция) «О безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ. 2017. № 31. Ст. 4724.

данные по беспроводным сетям связи⁶. С юридической точки зрения эксплуатация таких систем порождает ряд существенных вопросов, связанных с правовой природой собираемых сведений⁷. В частности, показания приборов учета, привязанные к конкретным жилым помещениям, могут рассматриваться как персональные данные. Такая ситуация обязывает операторов систем АСКУЭ соблюдать требования о получении согласия субъектов данных, об обеспечении их права на доступ и исправление информации, а также о реализации технических мер защиты. Обозначенные меры предусмотрены такими законодательными актами, как Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»⁸ и Приказ ФСБ России от 24.10.2022 № 524 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств»⁹. В юридической литературе подчеркивается, что выполнение указанных технических мер, включая сертификацию средств защиты, является необходимым условием обеспечения безопасности персональных данных [Мельников П.А., 2018: 182].

Логистический сектор Татарстана демонстрирует высокую степень готовности к внедрению IoT-решений, что обусловлено стратегическим положением республики как ключевого транспортного узла Поволжского региона. На объектах Казанского мультимодального логистического центра и порта Свияжск активно используются GPS/ГЛОНАСС-трекеры для мониторинга грузопотоков, RFID-метки автоматизации складского учета, а также датчики контроля микроклимата в рефрижераторных контейнерах¹⁰. Экс-

⁶ «Умные счетчики»: Татарстан опередит Россию по установке приборов учета. Available at: URL: <https://rt.plus.rbc.ru/pressrelease/5c4182797a8aa9770cf87bef> (дата обращения: 20.11.2025)

⁷ Приказ Министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Татарстан от 12.03.2018 №35/о «Об утверждении Положения об обработке персональных данных работников Министерства строительства, архитектуры и жилищно-коммунального хозяйства Республики Татарстан» // СПС КонсультантПлюс.

⁸ Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // СПС КонсультантПлюс.

⁹ Приказ ФСБ России от 24.10.2022 № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств» // СПС КонсультантПлюс.

¹⁰ Тихий триумф Ирека Салихова: как оживает свияжский логистический центр. Available at: URL: <https://www.business-gazeta.ru/article/553001> (дата обращения: 16.11.2025)

плуатация этих систем сопряжена с необходимостью соблюдения требований к трансграничной передаче данных, особенно при перевозке грузов в страны Евразийского экономического союза. В соответствии с положениями ст. 12 Закона № 152-ФЗ от 27.07.2006, трансграничная передача персональных данных допускается только при адекватных гарантиях защиты¹¹.

В системе здравоохранения Республики внедрение IoT-технологий осуществляется в рамках регионального проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы здравоохранения», предполагающего создание интегрированных систем удаленного мониторинга пациентов и автоматизации фармацевтического учета¹². В республиканских медицинских учреждениях развернуты платформы, позволяющие передавать данные с носимых устройств (глюкометров, тонометров, пульсметров) в электронные медицинские карты пациентов¹³. Обработка такой информации сопряжена с повышенными требованиями к защите, поскольку медицинские данные относятся к специальной категории персональных данных в соответствии со ст. 10 Закона № 152-ФЗ от 27.07.2006. При этом использование приложений Интернета вещей поднимает ряд вопросов, связанных с согласием субъекта на обработку данных и формированием профилей пользователей на основе собираемой информации, что требует более строгого правового регулирования [Линьков В.В., Семенов Е.Ю., 2020: 193].

Складывающаяся практика указывает, что медицинские организации (учреждения) обязаны получать письменное согласие пациентов на обработку сведений о состоянии здоровья; применять сертифицированные средства криптографической защиты при передаче данных; ограничивать доступ к информации только уполномоченными сотрудниками; вести журналы учета обращений к персональным данным. Особую трудность могут вызывать вопросы отзыва пациентом согласия на обработку данных, а также пределы обработки персональных данных без согласия в случаях, предусмотренных законом для оказания медицинской помощи [Людско В.В., Свередюк М.Г., Ступак В.С., 2021: 506–508].

При анализе нормативной базы внедрения IoT в Татарстане виден ее многоуровневый характер: на федеральном уровне ключевыми регулято-

¹¹ Приказ МЭ РТ от 15.03.2023 № 64 «О внесении изменения в Политику безопасности обработки персональных данных Министерства экономики Республики Татарстан» // СПС КонсультантПлюс.

¹² Постановление Кабинета Министров от 11.05.2022 № 431 «Об утверждении Положения о государственной информационной системе Республики Татарстан “Электронное здравоохранение Республики Татарстан”» // СПС КонсультантПлюс.

¹³ Число участников телемедицинского мониторинга в Татарстане достигло 1 тыс. человек. Available at: URL: <https://tass.ru/v-strane/17890215> (дата обращения: 20.11.2025)

рами выступают законы № 152-ФЗ от 27.07.2006, № 187-ФЗ от 26.07.2017, № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; на региональном уровне — Стратегия социально-экономического развития Республики Татарстан до 2030 года, Постановление Кабинета Министров Республики Татарстан от 18.08.2021 № 748 «Об утверждении Стратегии в области цифровой трансформации отраслей экономики, социальной сферы и государственного управления Республики Татарстан», Программа «Умный город», утвержденная Кабинетом Министров Республики; ведомственные акты Министерства цифрового развития государственного управления, информационных технологий и связи Республики и др. При этом наблюдается существенный дефицит специализированных норм, регулирующих специфические аспекты функционирования IoT. Отсутствует ясное определение правового статуса данных, генерируемых IoT-устройствами, не урегулирован порядок распределения ответственности между оператором системы, поставщиком оборудования и пользователем, а также не установлены единые требования к трансграничной передаче телеметрической информации.

Эмпирическое исследование позволяет выявить ряд проблем правового характера: неопределенность правового режима данных приводит к тому, что одна и та же информация может одновременно квалифицироваться как персональные данные, коммерческая тайна или сведения, составляющие государственную тайну (разное толкование квалификации информации может создавать риски неправомерного ее раскрытия и повлечь административную и уголовную ответственность); отсутствие унифицированных технических стандартов в области шифрования и аутентификации повышает уязвимость IoT-систем, что подтверждается взломами «умных» счетчиков в секторе ЖКХ; разрозненность регуляторных требований затрудняет разработку единой корпоративной политики информационной безопасности, вынуждая предприятия создавать собственные локальные акты.

Технические ограничения устройств Интернета вещей (низкое энергопотребление, малый форм-фактор, ограниченные вычислительные ресурсы) требуют существенной адаптации традиционных методов защиты, таких как шифрование и аутентификация, что осложняет создание унифицированных систем безопасности [Полегенько А.М., 2018: 42].

Татарстан демонстрирует прогрессивные подходы к минимизации правовых рисков, связанных с внедрением IoT. В 2024 году на базе ИТ-парка Казани создан Центр компетенций кибербезопасности IoT, осуществляющий разработку типовых договоров для операторов IoT-систем с учетом соответствующих правовых норм, проведение аудитов соответствия информационных систем законодательству о персональных данных, организацию образовательных программ по правовым аспектам кибербезопасности. В особой экономической зоне «Алабуга» внедряются экспериментальные правовые режимы, упрощающие сертификацию IoT-устройств при сохра-

нении требований к защите данных, что позволяет ускорить масштабирование инновационных решений и минимизировать юридические барьеры¹⁴.

Таким образом, внедрение IoT в Республике характеризуется высокой технологической зрелостью и активной государственной поддержкой, но сопровождается возникновением существенных правовых вызовов. Для дальнейшего развития необходимо принятие подзаконных актов, конкретизирующих требования к обработке IoT-данных; гармонизация отраслевых стандартов с федеральным законодательством; разработка механизмов трансграничной передачи информации в рамках ЕАЭС; усиление кадрового потенциала в области правового регулирования кибербезопасности. Без решения этих задач масштабное внедрение IoT-технологий может привести к росту правовых рисков, связанных с нарушением конфиденциальности, целостности и доступности данных, что потребует от предприятий более ответственного подхода к соблюдению нормативно-правовых требований.

2. Судебная практика защиты персональных данных, собираемых IoT-устройствами (2020–2024 гг.)

Судебная практика Татарстана за указанный период демонстрирует постепенное формирование устойчивых подходов к разрешению споров, связанных с обработкой персональных данных IoT-устройствами. Характерно, что большинство дел возникает по инициативе граждан, чьи права были нарушены в результате несанкционированного сбора, хранения или передачи данных, генерируемых умными устройствами (к примеру, бытовыми сенсорами, корпоративными системами мониторинга).

Типичной категорией споров являются дела о неправомерной передаче данных IoT-устройств третьим лицам. В одном из арбитражных дел истец доказал, что компания-оператор умной системы домофона передавала видеоданные с камер наблюдения маркетинговым агентствам без согласия жильцов. Суд, руководствуясь ст. 7 и 9 Закона № 152-ФЗ, признал действия оператора незаконными, обязал прекратить передачу данных и взыскал компенсацию морального вреда в размере 50 тыс. руб. Важным правовым выводом стало признание видеоизображений, фиксируемых IoT-камерами, персональными данными, требующими особой защиты¹⁵.

Другой пример из судебной практики связан с нарушениями при обработке биометрических данных. Так, в уголовном деле рассматривался иск к сети фитнес-клубов, использовавших умные браслеты для сбора данных о сердечном ритме и физической активности клиентов. Суд установил, что согласие на об-

¹⁴ Завод СОЛЛЕРС в ОЭЗ «Алабуга» внедрил технологии IoT и Big Data для оптимизации производства. Available at: URL: <https://dzen.ru/a/aFFfn38a1G6hKUve> (дата обращения: 20.11.2025)

¹⁵ Решение Верховного Суда Республики Татарстан от 4.10.2022 № А33-12456/2022 // СПС Консультант Плюс.

работку биометрии было получено в общей форме, без конкретизации целей и сроков, что противоречит требованиям ч. 4 ст. 9 Закона № 152-ФЗ. Решение суда включало предписание об уничтожении незаконно собранных данных и штраф в размере 30 тыс. руб. за нарушение порядка получения согласия¹⁶.

Другой вопрос, затрагиваемый в судебной практике, касается оценки технической защиты персональных данных. Приведем пример арбитражного дела, в котором рассматривался иск к производителю умных колонок, чьи устройства передавали аудиозаписи на серверы без уведомления пользователей. Суд указал на необходимость соблюдения требований Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»¹⁷, требующего внедрения средств защиты от несанкционированного доступа. Решение включало предписание о доработке программного обеспечения и о компенсации в размере 70 тыс. руб.¹⁸.

Ключевыми проблемами, выявляемыми судебной практикой, остаются недостаточная информированность граждан о характере собираемых IoT-данными; пробелы в регламентации трансграничной передачи данных, генерируемых устройствами; отсутствие единых стандартов шифрования для маломощных IoT-сенсоров; трудности доказывания причинно-следственной связи между действиями оператора и ущербом. Общероссийская судебная практика также демонстрирует типичные категории нарушений, включая передачу персональных данных третьим лицам без согласия, отказ в предоставлении информации и неправомерный доступ к данным, что подтверждает системный характер выявленных проблем [Миллер И.П., 2017: 387–388]. При этом региональный опыт создает новые меры защиты персональных данных, генерируемых IoT-устройствами (например, повышение роли экспертиз в области кибербезопасности при рассмотрении гражданских и административных дел, формирование прецедентов по коллективной защите прав).

Анализ судебной практики Татарстана выявляет тенденцию к ужесточению правовой защиты субъектов персональных данных в условиях цифровизации быта и производства. Суды, рассматривая споры, связанные с IoT-устройствами, квалифицируют данные умных устройств (включая аудио- и видеопотоки) как объекты, подпадающие под режим персональных данных. Примечательно, что основным драйвером формирования этой прак-

¹⁶ Материалы уголовного дела № 2-345/2023 // Архив Вахитовского районного суда Казани Республики Татарстан, 2023.

¹⁷ Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // СПС КонсультантПлюс.

¹⁸ Решение Верховного Суда Республики Татарстан от 12.11. 2024 № А33-2345/2024 // СПС Консультант Плюс.

тики выступают граждане. Это свидетельствует о росте правосознания в области цифровой приватности, однако пробелы в правовом регулировании и стандартах безопасности усложняют процесс доказывания. Региональные суды демонстрируют готовность применять не только отраслевое законодательство, но и технические регламенты, оценивая адекватность мер защиты, что указывает на движение от формального подхода к сущностной оценке нарушений. Это позволяет заключить, что региональная судебная практика не только оперативно реагирует на технологические вызовы, но и вносит вклад в выявление новых возможностей для совершенствования защиты прав субъектов персональных данных.

3. Проблемы правового просвещения работников и модель его организации в условиях распространения IoT

В условиях активной цифровой трансформации экономики Республики внедрение IoT-технологий приобретает системный и масштабный характер. Умные датчики последовательно интегрируются в производственные процессы промышленных предприятий, системы видеонаблюдения с функцией распознавания лиц развертываются в государственных организациях (учреждениях) и бизнес-центрах, носимые устройства активно используются в корпоративных программах здоровья. Данная технологическая динамика порождает острую и постоянно нарастающую потребность в правовом просвещении работников относительно защиты персональных данных, которые собираются посредством IoT-устройств.

Рассматривая контекст внедрения IoT в Республике, следует обратиться к данным Министерства цифрового развития государственного управления, информационных технологий и связи региона. В 2023–2024 годах в Республике реализован целый ряд значимых проектов с активным использованием технологий IoT¹⁹. В их число входят цифровизация коммунальных сетей с установкой умных счетчиков в жилых домах Казани и Набережных Челнов, внедрение систем видеоаналитики на предприятиях нефтехимического комплекса, развертывание «умных офисов» в структурах исполнительной власти, а также использование носимых устройств в программах корпоративного здоровья на крупных предприятиях.

Как свидетельствует практика, наиболее частой причиной утечек персональных данных является человеческий фактор, что подтверждает необходимость системного повышения квалификации сотрудников, допущенных к обработке данных, и разработки внутрикорпоративных регламентов [Вепрев С.Б., Нестерович С.А., 2021: 154–155]. Указанные инициативы

¹⁹ Мониторинг регионального законодательства в сфере развития цифровой экономики в регионах АИРР. Available at: URL: https://cesi.tatarstan.ru/file/pub/pub_1613527.pdf (дата обращения: 10.11.2025)

неизбежно сопровождаются массовым сбором разнообразных персональных данных — биометрических (отпечатки пальцев, распознавание лиц), геолокационных (фиксация перемещений по территории предприятия), поведенческих (анализ активности за рабочим местом), физиологических (частота сердечных сокращений и иные показатели). При этом в соответствии со ст. 3 Закона № 152-ФЗ любая информация, позволяющая идентифицировать физическое лицо, подлежит обязательной правовой защите. Это накладывает на организации серьезные обязательства по обеспечению конфиденциальности и безопасности собираемых сведений.

Региональный опыт нормотворчества, в частности, например, в Алтайском крае, демонстрирует, что детализация требований к содержанию типовых согласий на обработку персональных данных на уровне субъекта РФ позволяет восполнить пробелы федерального законодательства и усилить защиту прав субъектов персональных данных [Коваленко К.Е., Коваленко Н.Е., 2020: 128]. Прежде всего, обращает на себя внимание нечеткость формулировок целей обработки данных. В документах повсеместно встречаются обобщенные, размытые формулировки (например, «для обеспечения безопасности объекта», «в целях оптимизации рабочих процессов»), при полном отсутствии конкретизации относительно сценариев использования информации. Например, не разъясняется, каким образом данные могут применяться для анализа продуктивности персонала на таких крупных предприятиях, как КамАЗ или ТАНЕКО; не указываются точные сроки хранения информации, в том числе в региональных центрах обработки данных; не определяется четкий круг лиц, имеющих право доступа к собранным сведениям, включая подрядчиков из числа татарстанских IT-компаний²⁰.

Особую озабоченность вызывает недостаточная информированность работников о технических аспектах функционирования региональных IoT-платформ. В большинстве случаев сотрудники не получают развернутых сведений о принципах работы интегрированных систем (например, взаимодействующих с городской платформой «Умный город»), о методах анонимизации данных, применяемых локальными IT-провайдерами, а также о конкретных механизмах защиты от утечек в условиях кросс-регионального обмена информацией. Такая информационная асимметрия существенно ограничивает возможность осознанного принятия решений относительно предоставления согласия на обработку персональных данных.

Правовое просвещение работников в Татарстане в сфере защиты персональных данных, собираемых IoT-устройствами, должно учитывать ряд факторов, обусловленных региональными особенностями. Прежде всего необходимо принимать во внимание отраслевую специфику: для работников нефтехимических предприятий (к примеру, ТАНЕКО, Нижнекамскнефтехим) акцент в обучении следует делать на защите данных, собираемых си-

²⁰ Политика ПАО «КамАЗ» в отношении обработки персональных данных. Available at: URL: <https://kamaz.ru/about/policy/politika-personalnykh-dannyh/> (дата обращения: 20.11.2025)

стемами промышленной безопасности; для сотрудников государственных организаций (учреждений), на соблюдении требований к обработке информации в рамках проектов «Умный город». Важным аспектом является языковой фактор: образовательные материалы должны быть доступны как на русском, так и на татарском языке, что обусловлено многонациональным составом трудовых коллективов. Кроме того, необходимо включать в программы просвещения разъяснения положений региональных нормативных актов (к примеру, постановлений Кабинета Министров Республики, регулирующих использование IoT-систем в муниципальных структурах). Существенное значение имеет также ознакомление с практикой регионального Управления Роскомнадзора: работникам важно знать о типичных нарушениях, выявляемых в ходе проверок татарстанских организаций, например, об отсутствии локальных актов о защите данных в малых предприятиях.

При построении системы правового просвещения целесообразно опираться на ряд ключевых принципов. Их допустимо классифицировать следующим образом: принцип контекстуальности предполагает детальное разъяснение того, какие именно данные собирает система (например, система контроля доступа в зданиях Кабинета Министров, датчики в «умных» автобусах Казани или носимые устройства на предприятиях особой экономической зоны); принцип визуализации рисков подразумевает использование наглядных материалов: инфографики на двух языках, а также разбор реальных кейсов из региональной практики, включая инциденты с утечкой данных, например, в медицинских учреждениях Татарстана; принцип интерактивности требует внедрения тренингов с имитацией типовых ситуаций (к примеру, отработки алгоритмов действий при получении запроса на доступ к данным от региональных органов власти или при обнаружении подозрительной активности IoT-устройств на объектах компании ПАО «Татнефть»); принцип регулярности предполагает проведение ежегодных обучающих семинаров с учетом последних изменений в законодательстве, в том числе требований Министерства цифрового развития Республики, а также в свете внедрения новых IoT-решений.

Для системной организации правового просвещения в татарстанских организациях (учреждениях) предлагается последовательная модель, включающая четыре взаимосвязанных этапа. По нашему мнению, к таким этапам следует отнести: диагностический этап, этап обработки контента, этап реализации и оценки полезности проведенных мероприятий.

На диагностическом этапе должен быть осуществлен всесторонний аудит используемых IoT-устройств с обязательным изучением реестра региональных IT-решений, а также проведен анализ действующих соглашений на обработку данных на предмет их соответствия требованиям Закона № 152-ФЗ и постановления Кабинета Министров Республики. Важной составляющей диагностики является выявление «слепых зон» в осведомленности работников посредством опросов на русском и татарском языках.

На этапе разработки образовательного контента создаются двуязычные памятки с детальным разъяснением ключевых технических терминов, таких

как «анонимизация» и «токенизация». Могут быть подготовлены видеонструкции, демонстрирующие порядок управления настройками приватности на IoT-устройствах, наиболее распространенных в Республике (например, на датчиках системы «Умный дом», предоставляемых местными провайдерами). Особое внимание должно быть уделено разработке кейсов на основе зафиксированных в республике инцидентов, что позволяет сделать обучение максимально прикладным и ориентированным на практику.

Этап реализации образовательных программ предусматривает проведение вводных курсов для новых сотрудников в русле отраслевой специфики организации (учреждения). В этом ключе должны быть организованы тематические вебинары для руководителей подразделений, в рамках которых детально разбираются требования Министерства цифрового развития Республики и последние изменения в нормативной базе. Вместе с тем могут внедряться симуляционные игры, направленные на отработку навыков реагирования на типичные инциденты (к примеру, утечка данных с датчиков жилищно-коммунального хозяйства). Многоуровневый подход позволит обеспечить охват всех категорий работников и отражает специфику их взаимодействия с IoT-устройствами в рамках функциональных обязанностей, возложенных согласно трудовым договорам.

Заключительный этап — оценка пользы просветительских мероприятий. Данный этап может быть осуществлен посредством комплексного тестирования уровня знаний работников на русском и татарском языках, мониторинга динамики обращений в службу защиты данных организации, а также анализа изменений в количестве и характере нарушений, выявляемых региональным Управлением Роскомнадзора. Регулярный сбор и анализ этих показателей позволят своевременно корректировать содержание и методы правового просвещения в свете выявленных дефицитов знаний и актуальных потребностей соответствующих работников.

Таким образом, правовое просвещение работников в сфере защиты персональных данных, собираемых IoT-устройствами в Татарстане, требует комплексного подхода, учитывающего отраслевую специфику региона (нефтехимическая промышленность, государственные услуги, жилищно-коммунальное хозяйство), необходимость двуязычного представления материалов и включения региональных кейсов, важность взаимодействия с местными органами власти (Министерство цифрового развития Республики, Управление Роскомнадзора по РТ), а также потребность в регулярном обновлении программ в рамках динамичного развития региональной цифровой инфраструктуры.

4. Совершенствование юридических механизмов защиты данных, генерируемых IoT-устройствами

В условиях активного развития цифровых технологий и повсеместного внедрения IoT-устройств повышенную актуальность приобретает вопрос

совершенствования законодательной базы в сфере защиты персональных данных. Татарстан, демонстрируя передовые позиции в области цифровизации, сталкивается с правовыми вызовами, характерными для всей страны. Поэтому возникает объективная потребность в совершенствовании региональных правовых механизмов. Во многих странах уже разработаны и применяются регуляторные меры, направленные на обеспечение безопасности и защиты персональных данных в сфере Интернета вещей, включая специальные законы и стандарты, что подтверждает необходимость развития аналогичных подходов в России [Кучковская Н.В., 2023: 353–354].

Субъекты РФ вправе в пределах своих полномочий принимать нормативные акты, детализирующие федеральные требования. Опираясь на ст. 4 Закона № 152-ФЗ, допускающую принятие ведомственных и региональных актов по отдельным вопросам, Татарстан может и должен развивать собственную нормативную базу. Такая база призвана не дублировать или подменять федеральный закон, а конкретизировать его применительно к специфике обработки данных, формируемых в результате работы IoT-инфраструктуры, и в ракурсе отраслевых особенностей региональной экономики (промышленность, ЖКХ, здравоохранение). Современные реалии характеризуются тем, что персональные данные все чаще генерируются автоматически, без непосредственного участия человека. Такие данные обладают уникальными характеристиками: они формируются в массовом порядке и могут содержать информацию о поведенческих паттернах пользователей. В связи с этим встает необходимость в создании специального правового механизма, регулирующего их обработку и защиту.

Создание мониторинга безопасности персональных данных в IoT-инфраструктуре критически важно. Такая система должна включать механизмы регулярного аудита защищенности систем, оценки рисков нарушения безопасности, анализа инцидентов и выработки превентивных мер, а также формирования статистических отчетов о состоянии защиты данных. В контексте развития цифровой экономики большое значение приобретает вопрос государственного контроля за обработкой персональных данных в IoT-среде. Необходимо создать специализированные подразделения по контролю, разработать методики оценки защищенности систем [Дриленко Д.В., Федяев С.М., 2025: 133–134].

В условиях цифровизации экономики и активного внедрения IoT-технологий повышенную значимость приобретает вопрос о создании системы регламентации процессов обработки, хранения и передачи персональных данных, собираемых с помощью IoT-систем. Республика Татарстан, являясь одним из передовых в сфере цифровизации регионов, нуждается в разработке специализированного регионального регламента, отражающего специфику обработки данных в условиях массового внедрения умных систем.

В виду развития цифровых технологий и активного внедрения IoT-систем в Татарстане актуальным становится совершенствования механизмов административной ответственности за нарушения в сфере защиты персональ-

ных данных. Существующая система правовых норм требует адаптации к специфике IoT-инфраструктуры и новым видам правонарушений. Анализ законодательства показывает, что в РФ отсутствует нормативная база, устанавливающая квалификацию административных правонарушений при обработке персональных данных с использованием IoT-устройств. Необходимость учета специфики IoT-технологий при установлении ответственности обосновывается и в современных исследованиях, посвященных правовой характеристике Интернета вещей [Забайкин Ю.В., Лунькин Д.А., 2023: 331–332]. Действующие нормы КоАП РФ (например, ст. 13.11 «Нарушение законодательства Российской Федерации в области персональных данных») носят общий характер и не учитывают технической специфики автоматизированного сбора данных. Последние изменения законодательства, в частности, введение ст. 272.1 УК РФ и новых составов в ст. 13.11 КоАП РФ, предусматривающих оборотные штрафы, свидетельствуют о тенденции усиления ответственности операторов за утечки данных. Однако специфика IoT по-прежнему остается вне поля зрения законодателя [Ковалев С.Д., 2024: 272–273].

Поэтому назрела дифференциация административной ответственности в области нарушений в сфере защиты персональных данных. Под дифференцированной системой административной ответственности в контексте IoT мы понимаем установление квалифицирующих признаков составов правонарушений, которые позволяют разграничивать ответственность в зависимости от: объема обрабатываемых данных (массовый сбор); типа данных (биометрия, геолокация); последствий (причинение вреда критической инфраструктуре); субъекта ответственности (оператор, производитель оборудования). Любое расширение оснований для обработки данных без согласия субъекта, включая ссылки на законные интересы оператора, должно сопровождаться четкими критериями и ограничительным толкованием, чтобы не допустить необоснованного вторжения в частную жизнь [Давымока С.В., 2025: 448–449].

Принципиально важен вопрос об уровне правового регулирования такой системы. В соответствии с п. «к» ч. 1 ст. 72 Конституции Российской Федерации, административное и административно-процессуальное право находится в совместном ведении РФ и ее субъектов. Однако установление составов правонарушений (диспозиций и санкций) является прерогативой федерального законодателя (КоАП РФ). В связи с этим деятельность Республики Татарстан должна быть направлена не на создание региональных составов правонарушений в сфере IoT (что было бы выходом за пределы компетенции), а на реализацию права законодательной инициативы и разработку предложений по изменению федерального законодательства, а также на детализацию процедур привлечения к ответственности в региональных подзаконных актах в рамках полномочий субъекта. В целях реализации мысли мы предлагаем следующий комплекс мер на примере Республики Татарстан: разработка типовых регламентов взаимодействия операторов IoT-систем с контрольными

органами, включая порядок расследования инцидентов и фиксации доказательственной базы; утверждение региональных методических рекомендаций для судей и должностных лиц Роскомнадзора по квалификации правонарушений в сфере IoT, учитывающих отраслевую специфику (например, несанкционированный сбор биометрических данных в системах «умный город»); предложения о дифференциации составов административных правонарушений путем дополнения КоАП квалифицирующими признаками, учитывающими особенности IoT-систем (в частности, предлагается дополнить ст. 13.11 КоАП такимиотягчающими обстоятельствами (составами), как «обработка персональных данных, автоматически генерируемых техническими устройствами (телеметрических данных), без уведомления субъекта о таком сборе»; «несанкционированная трансграничная передача данных, собранных с использованием IoT-устройств на объектах критической информационной инфраструктуры»; «непринятие оператором мер по своевременному уведомлению об инцидентах, приведших к утечке биометрических персональных данных из IoT-систем»); использование региональных механизмов административного воздействия (предостережения, предписания) в рамках существующих полномочий для оперативного реагирования на выявленные уязвимости в IoT-системах организаций ЖКХ и здравоохранения.

Кроме того, важным направлением является совершенствование правового просвещения и локального нормотворчества, чтобы сами операторы данных могли минимизировать риски нарушений еще на стадии проектирования IoT-решений.

Таким образом, предлагаемая система административной ответственности является двухуровневой: федеральный (установление дифференцированных составов правонарушений в КоАП) и региональный уровни (разработка методических рекомендаций для правоприменителей, регламентов взаимодействия и профилактических мер). Реализация предложенных мер, разработанных под углом разграничения предметов ведения, позволит создать действенный механизм административного преследования за нарушения в сфере защиты персональных данных IoT-системами, отражающий специфику их функционирования, и будет способствовать повышению уровня защиты прав субъектов персональных данных.

5. Концепция специального правового режима обработки данных в IoT-среде

Анализ правоприменительной практики и пробелов в регулировании приводит к выводу о необходимости формирования комплексного подхода к защите данных. Такой подход, по мнению авторов, должен включать совершенствование механизмов ответственности и создание принципиально новой концепции регулирования самих данных.

В отличие от общего режима персональных данных, регулируемого Федеральным законом «О персональных данных», предлагаемый режим призван учитывать особенности функционирования технологий Интернета вещей. К числу таких особенностей относятся массовость и непрерывность сбора данных, их тесная связь с объектами критической информационной инфраструктуры, а также высокая степень автоматизации процессов обработки, протекающих без непосредственного участия человека. В рамках настоящего исследования предлагаются базовые элементы такого режима, адаптированные для регионального уровня на примере Республики Татарстан. Включение принципов защиты данных в международно-правовую базу и установление четких правил этического использования искусственного интеллекта, таких как прозрачность, подотчетность, справедливость и недискриминация, имеют решающее значение для создания глобального стандарта ответственного использования новых технологий [Абрамова А.Г., 2024: 48–50].

Так, первым элементом предлагаемого режима может выступить принцип «контекстуальной анонимизации». В отличие от тотального обезличивания, которое способно нивелировать полезность данных для решения задач промышленности или ЖКХ, предлагается внедрить правило, согласно которому данные, собираемые с устройств (телеметрия, показания приборов учета), могут обрабатываться в обезличенном виде для статистических целей и оптимизации процессов. При этом указанные данные должны быть «обратимо деанонимизированы» с применением криптографических средств и строгой аудируемой процедуры исключительно в случаях, прямо предусмотренных законом, например, при расследовании аварий на объектах критической информационной инфраструктуры или по мотивированному запросу правоохранительных органов. Реализация этого принципа позволяет снять коллизию, при которой одна и та же информация одновременно может рассматриваться и как коммерческая тайна, и как потенциально персональные данные.

В качестве второго элемента может являться дифференциация правового статуса данных. Предлагается ввести в региональные подзаконные акты либо инициировать на федеральном уровне классификацию данных, генерируемых IoT-устройствами, по степени риска для прав субъектов. К данным низкого риска предлагается относить показания общедомовых приборов учета и агрегированную статистику загруженности оборудования без привязки к конкретному оператору, что предполагает применение базовых требований к защите. Данные среднего риска включают геолокацию служебного транспорта, сведения из систем контроля доступа и телеметрию, привязанную к рабочему месту оператора, что требует усиленной аутентификации и шифрования. Данные высокого риска охватывают биометрическую информацию, включая распознавание лиц и отпечатки пальцев, а также медицинские показатели, получаемые с носимых устройств, что обуславливает необходимость соблюдения самых строгих мер защиты, включая криптографию, лицензирование деятельности и изолированное хранение. Использование биометрических данных сопряжено с рядом серьезных

угроз, включая возможность манипуляции данными, скрытого наблюдения за индивидами и внедрения систем социального рейтинга, что требует особого внимания законодателя [Жирнова Н.А., Ковалева Н.Н., 2024: 112–115].

Наконец, третьим элементом предлагаемой концепции может стать разработка и внедрение регионального стандарта ответственного внедрения технологий Интернета вещей. Основываясь на полномочиях субъекта федерации, предусмотренных ст. 4 Федерального закона «О персональных данных», а также на успешном опыте функционирования особой экономической зоны «Алабуга», целесообразно утверждение Постановлением Кабинета Министров Республики Татарстан документа «Типовые требования к организации обработки данных в ведомственных и муниципальных IoT-системах». Данный документ мог бы содержать обязательные формулировки для согласий на обработку данных, уточняющие цели такой обработки и устраняющие размытые формулировки, выявленные в ходе анализа локальных актов организаций. Кроме того, в нем можно закрепить минимальные технические стандарты шифрования для различных типов IoT-устройств с учетом их энергопотребления, а также регламент взаимодействия оператора IoT-системы с региональным Управлением Роскомнадзора и Министерством цифрового развития Республики Татарстан при возникновении инцидентов, включая сроки уведомления и состав комиссии по расследованию.

Реализация указанных элементов на региональном уровне позволит, не дожидаясь изменений в федеральном законодательстве, принятие которых может быть длительным процессом, создать действенную правовую среду, минимизирующую риски, выявленные анализом судебной практики.

Заключение

Республика Татарстан демонстрирует высокий уровень цифровизации различных секторов экономики, что подтверждается активным внедрением IoT-технологий в промышленности, жилищно-коммунальном хозяйстве, логистике и здравоохранении. Предприятия региона — ПАО «КАМАЗ», АО «Производственное объединение „Завод имени Серго“», ПАО «Татнефть» и другие, активно интегрируют умные системы в свои производственные и управленческие процессы. Анализ правового регулирования показал, что федеральная нормативная база (прежде всего ФЗ № 152-ФЗ) является фундаментом защиты персональных данных, который однако требует адаптации к специфике их обработки в IoT-среде. Существенные пробелы в законодательстве (неопределенность правового режима данных, отсутствие унифицированных стандартов) носят федеральный характер. В этих условиях роль регионального законодательства заключается в оперативной конкретизации федеральных норм в отраслевых регламентах, разработке типовых документов (согласий, политики) и усилении правового просвещения. Предложенные в исследовании меры, разработанные на основе анализа практики Республики Татарстан и учитывающие федеральное

регулирование, могут быть масштабированы при условии их соответствия федеральному законодательству и под углом необходимости последующей имплементации наиболее успешных региональных практик в федеральные подзаконные акты и отраслевые стандарты и использованы в других субъектах Российской Федерации для минимизации правовых рисков при внедрении технологий Интернета вещей.

Исследование внедрения IoT-систем в ключевых отраслях экономики региона позволило выявить ряд системных проблем. В частности, установлено, что локальные нормативные акты организаций (учреждений) не в полной мере соответствуют требованиям законодательства в области защиты персональных данных, что создает дополнительные риски нарушения прав субъектов данных. Особенно остро эта проблема проявляется в секторе ЖКХ и на малых предприятиях логистического сектора. Судебная практика Республики показывает тенденцию к формированию устойчивых подходов к разрешению споров в сфере защиты персональных данных, однако правовые механизмы требуют совершенствования. Анализ судебных решений показывает необходимость усиления ответственности за нарушения в сфере защиты персональных данных и разработки более действенных механизмов превентивной защиты. В результате исследования разработаны предложения по совершенствованию правового регулирования: обоснована двухуровневая модель дифференциации административной ответственности за нарушения в сфере защиты персональных данных; предложена и содержательно раскрыта концепция специализированного правового режима для данных, генерируемых IoT-устройствами. Важно отметить, что предложенные в исследовании решения могут быть использованы не только в Татарстане, но и в других регионах Российской Федерации, сталкивающихся с аналогичными проблемами в сфере защиты персональных данных в условиях цифровизации экономики.



Список источников

1. Абрамова А.Г. Новые технологии и их значение в защите персональных данных (Интернет Вещей, Искусственный интеллект) // Вестник Российско-Армянского (Славянского) университета: гуманитарные и общественные науки. 2024. № 2. С. 44–52.
2. Вепрев С.Б., Нестерович С.А. Меры по совершенствованию защищенности персональных данных в сети Интернет / Информационная безопасность: вчера, сегодня, завтра. Материалы международной научно-практической конференции. М.: Российский государственный гуманитарный университет, 2021. С. 153–158.
3. Давымока С.В. Права и законные интересы оператора персональных данных // Современный ученый. 2025. № 7. С. 446–450.
4. Дриленко Д.В., Федяев С.М. Правовое регулирование контекстно-зависимых IoT-датчиков и технологий машинного зрения: коллизия ФЗ № 152-ФЗ и ФЗ № 572-ФЗ при обработке биометрии (нормативно-правовой анализ и эмпирическое исследование судебной практики 2018-2025 гг.) // Научные

труды Кубанского государственного технологического университета. 2025. № 5. С. 123–139.

5. Жирнова Н.А., Ковалева Н.Н. Проблемы обеспечения конфиденциальности персональных данных при использовании систем искусственного интеллекта // Журнал российского права. 2024. № 7. С. 109–121.

6. Забайкин Ю.В., Лунькин Д.А. Правовая характеристика использования Интернета вещей // Вопросы российского и международного права. 2023. Т. 13. № 4-1. С. 329–335.

7. Зиновьева Е.А. К вопросу о реализации прав и свобод личности в условиях цифровизации // Проблемы экономики и юридической практики. 2022. Т. 18. № 4. С. 94–99.

8. Ковалев С.Д. Обзор последних изменений в Федеральном Законе «О персональных данных» // Аграрное и земельное право. 2024. № 12(240). С. 272–274.

9. Коваленко К.Е., Коваленко Н.Е. Соотношение федерального и регионального законодательства в области защиты персональных данных / Эволюция российского права. Материалы заочной международной конференции молодых ученых и студентов. Екатеринбург: Уральский государственный юридический университет, 2020. С. 127–128.

10. Кучковская Н.В. Развитие права в области IoT // Вопросы российского и международного права. 2023. Т. 13. № 4-1. С. 350–356.

11. Линьков В.В., Семенов Е.Ю. Правовые проблемы защиты персональных данных при интеграции Интернета вещей в повседневную жизнь // Закон и право. 2020. № 10. С. 193–195.

12. Люцко В.В. и др. Отзыв согласия пациента на обработку персональных данных из медицинской организации: правомерность и возможности правового регулирования // Современные проблемы здравоохранения и медицинской статистики. 2021. № 4. С. 502–514.

13. Мельников П.А. Анализ законодательной базы РФ, обеспечивающей защиту персональных данных / Инновационный потенциал молодежи: социальная, экологическая и экономическая устойчивость. Материалы международной молодежной конференции. Екатеринбург: Уральский федеральный университет, 2018. С. 179–183.

14. Миллер И.П. Правовые аспекты использования персональных данных при использовании электронными услугами / Безопасность городской среды. Материалы научно-практической конференции. Омск: Омский государственный технический университет, 2018. С. 385–389.

15. Полегенько А.М. Особенности защиты информации в Интернете вещей // International Journal of Open Information Technologies. 2018. Т. 6. № 10. С. 41–45.

Информация об авторах:

К.Р. Кирушин — кандидат юридических наук, старший преподаватель.

Д.И. Сафин — ассистент.

Статья поступила в редакцию 24.12.2025; одобрена после рецензирования 28.01.2026; принята к публикации 28.01.2026.

Научная статья

JEL: K14

УДК: 343.71

DOI:10.17323/2713-2749.2026.1.141.163

Уголовно-правовой комплаенс тестирования информационных систем на киберустойчивость



Евгений Александрович Русскевич

Московский государственный юридический университет им. О.Е. Кутафина (МГЮА), Россия 123342, Москва, Садовая-Кудринская ул., 9/2,
rusскеvich@mail.ru, <https://orcid.org/0000-0003-4587-8258>



Аннотация

Увеличивающаяся с годами зависимость человека, общества и государства от цифровых технологий обуславливает возрастающий запрос на услуги в области защиты компьютерных систем. Формирование в России самостоятельного рынка кибербезопасности уже состоялось и оценивается многомиллиардным оборотом. Одним из значимых сегментов отрасли является оказание услуг, связанных с комплексной и всесторонней проверкой информационной системы на устойчивость к компьютерным атакам. Одновременно с этим активно развивается практика краудсорсингового анализа защищенности информационных систем, когда любой желающий может участвовать в тестировании информационной системы и при обнаружении уязвимости получить вознаграждение. Цель исследования состоит в разработке теоретических рекомендаций и предложений по митигации уголовно-правовых рисков, возникающих при тестировании информационных систем на киберустойчивость. Исследование основано на применении общенаучных и специальных методов (анализ, синтез, индукция, формально-юридический, абстрактно-логический и др.). В отсутствие специального правового регулирования «этичный хакер», ищущий уязвимости в информационных системах, несомненно, подвергает себя риску уголовного преследования. Соответственно решение данной проблемы требует определения правового режима тестирования информационных систем на киберустойчивость. В работе делается вывод, что специалист, проверяющий защищенность компьютерной системы, обладая необходимыми знаниями, опираясь на опробованные методы и инструментарий, стремится к

достижению общественно полезного результата, но всегда допускает (хотя бы в самой малой степени) угрозу выхода из строя системы с возможными негативными последствиями в виде аварийного отключения автоматизированных систем управления технологическими процессами, поломки оборудования, уничтожения или блокирования данных и т.п. Подобное поведение специалиста, равно как и наступление соответствующих последствий, в полной мере отвечает положениям уголовного закона об обоснованном риске (ст. 41 Уголовного кодекса России). В статье предлагается ряд рекомендаций по митигации уголовно-правовых рисков тестирования информационных систем на киберустойчивость.



Ключевые слова

уголовное право; компьютерные преступления; уголовно-правовой комплаенс; кибербезопасность; «белые хакеры»; уголовно-правовой риск.

Для цитирования: Русскевич Е.А. Уголовно-правовой комплаенс тестирования информационных систем на киберустойчивость // Вопросы права в цифровую эпоху. 2026. Том 7. № 1. С. 141–163. DOI: 10.17323/2713-2749.2026.1.141.163

Введение

Тестирование на проникновение является практикой обеспечения защищенности объектов цифровой инфраструктуры от компьютерных атак. В самом обобщенном виде под пентестом понимается практика оценки безопасности системы путем выявления и эксплуатации уязвимостей с использованием хакерских приемов [Reddy P., Pelletier J., 2022: 1117–1125].

Со временем эта деятельность выделилась в один из сегментов рынка информационной безопасности. По данным Marketsand Markets, размер мирового рынка тестирования на проникновение в 2024 г. оценивался в 1,7 млрд. долл. США и по прогнозам достигнет 3,9 млрд. долл. к 2029 г. По мере того как киберпреступность становится все более изощренной и высокотехнологичной организациям понадобятся передовые инструменты тестирования на проникновение, чтобы опережать стремительно развивающиеся цифровые угрозы. Высокие стандарты защиты конфиденциальных данных будут стимулировать спрос на надежные решения пентестинга. Ожидается, что рынок тестирования на проникновение продолжит рост, поддерживаемый ростом киберпреступности, усложнением и ужесточением регулятивного законодательства в сфере информационной безопасности¹.

¹ Penetration Testing Market Size, Size, Growth & Latest Trends. Available at: URL: <https://www.marketsandmarkets.com/Market-Reports/penetration-testing-market-13422019.html> (дата обращения: 05.09.2025)

Механизм пентеста предполагает оценку объекта информационной инфраструктуры на его защищенность от угроз путем анализа его архитектуры и обнаружения уязвимостей. Это может быть реализовано только посредством «тестовых атак», когда проверяемый ресурс должен в реальных условиях показать готовность противостоять вредоносному воздействию. В негативном сценарии развития атаки специалист получает сведения, что объект информационной инфраструктуры не прошел проверку и был скомпрометирован (взломан). В отчете приводится соответствующее объяснение в виде обнаруженных уязвимостей².

В доктрине отмечается ключевое различие между неправомерным доступом (взломом) и пентестом: хакеры взламывают систему, чтобы завладеть чувствительной информацией и нанести ущерб, тогда как специалисты в области тестирования в ответ на проникновение предупреждают об уязвимостях безопасности, которые можно эксплуатировать, и помогают их устранить [Tudosí A.-D. et al., 2023].

Пентест важен не только в процессе оценки защищенности объекта информационной инфраструктуры, который уже долго используется и, возможно, устарел в свете новейших угроз. Он крайне востребован и в ситуации, когда заказчик и будущий владелец цифрового сервиса намерен проверить, насколько защищенный продукт ему подготовили разработчики.

Идея Bug Bounty в том, что даже высший уровень защиты может быть преодолен нетрадиционными решениями талантливого хакера-одиночки. Компания может вкладывать немалые средства в информационную безопасность, содержать внушительный штат специалистов, обладающих самыми высокими компетенциями, но это не дает полной гарантии защищенности от проникновения. Следовательно, необходимо действовать на опережение. Открытый конкурс на обнаружение уязвимостей с объявленным заранее вознаграждением направлен именно на это [Laszka A. et al., 2018: 138–159].

Очевидное преимущество Bug Bounty в сравнении с пентестом — в привлечении к тестированию неограниченного числа специалистов в сфере информационной безопасности [Kuehn A., Mueller M., 2014: 1–16]. Кроме того, оплата производится не за тестирование, а как награда за выявленную уязвимость. Следовательно, в финансовом отношении Bug Bounty — весомый инструмент проверки системы на киберустойчивость. Привлекая к тестированию сотни и даже тысячи специалистов самой разной квалификации, организатор платит только за результат. Не стоит упускать из виду и то, что Bug Bounty позволяет компаниям

² Available at: URL: <https://www.ptsecurity.com/ru-ru/research/analytics/results-of-pentests-2023/#id1> (дата обращения: 02.09. 2025)

рекрутировать талантливых профессионалов в сфере информационной безопасности.

Изучение источников показывает, что в России Bug Bounty становится востребованным: «За 2024 г. портрет клиента багбаунти-платформ изменился: если год назад это были только крупные технологические компании, банки, ритейл или ИТ-компании, то сейчас к ним добавились организации из других сфер. Теперь программы багбаунти запускают страховые компании и компании в сфере ИБ, разработчики программного обеспечения (в том числе отечественных продуктов, создаваемых по программам импортозамещения), логистические организации, службы доставки, букмекеры, органы субъектов федерации. Кроме того, интерес к баг баунти-программам увеличился и у небольших компаний, у которых вопросы ИБ не самые приоритетные. Именно такие организации выбирают баг баунти как наиболее оптимальный и удобный механизм работы над защищенностью»³.

Специалисты отмечают, что наиболее значимым барьером для полноценного развития отрасли тестирования на проникновение является угроза привлечения к уголовной ответственности за посягательства на защищенные компьютерные данные и информационные системы [Fiorinelli G., Zucca V., 2024]. В зарубежной литературе есть исследования, посвященные митигации правовых рисков данной деятельности [Park S., Albert K., 2020].

В отечественной доктрине правовые риски организации и проведения пентеста и Bug Bounty практически не разработаны. В публикациях справедливо отмечается, что отсутствие четких правовых оснований и правил кибериспытаний создает значительные риски как для организаторов, так и для участников [Смородина Е.П., Бурцев Р.Д., 2023: 116–122].

1. Уголовно-правовые риски пентеста (penetration testing)

В России прохождение регулярных тестирований на проникновение является обязанностью отдельных субъектов. В соответствии с Положением Банка России от 17.08.2023 № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг

³ Российский рынок ИБ и его роль в мировой индустрии, итоги 2024 года и прогнозы на 2025. Available at: URL: <https://www.ptsecurity.com/ru-ru/research/analytics/rossijskij-rynok-ib-i-ego-rol-v-mirovoj-industrii-itogi-2024-goda-i-prognozy-na-2025/#id22> (дата обращения: 03.09.2025)

информационного обмена, операторы услуг платежной инфраструктуры и операторы электронных платформ обязаны проводить ежегодное тестирование на предмет проникновения в информационную инфраструктуру и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры⁴.

В соответствии с Распоряжением Правительства Российской Федерации от 28.08.2019 № 1911-р «Об утверждении Концепции создания государственной единой облачной платформы» система защиты информации такой платформы должна проходить ежегодный независимый внутренний и внешний аудит, выполняемый лицензированными Федеральной службой по техническому и экспортному контролю организациями, мер информационной безопасности, защиты информации, включая исследование уязвимостей и тестирование на проникновение⁵.

В стандартах информационной безопасности подчеркивается: использование специалиста по тестированию на проникновение (как правило, подрядчика) для оценки действенности безопасности системы посредством попытки проникновения в систему с ведома и при согласии соответствующего должностного лица организации является одной из предпосылок доверия к программе безопасности. По мере усложнения компьютерных систем поддержание безопасности становится все более затруднительным. Использование групп тестирования на проникновение может содействовать обнаружению слабых мест в системе организации⁶.

Несмотря на будничность тестирования на проникновение в сфере мониторинга киберустойчивости, следует напомнить, что она не свободна от уголовно-правовых рисков, которые в теории раскрываются как «опасность быть подвергнутым уголовному преследованию без законных материально-правовых оснований для этого либо претерпеть различного рода ограничения, связанные с предварительной или окончательной, вступившей в силу или отмененной оценкой деяния как преступления» [Жалинский А.Э., 2009: 242].

Аспекты нормативного обеспечения и правовых рисков пентеста в отечественной доктрине нередко разрабатываются в рамках «аудита информационной безопасности». Такая постановка проблемы не лишена оснований, если под аудитом в самом широком смысле понимать только независимую проверку какой-либо деятельности. Специалисты отмечают, что нормативная база пока не полностью обосновывает це-

⁴ См.: Вестник Банка России. 2023. № 76.

⁵ См.: Собрание законодательства РФ. 2019. № 36. Ст. 5066.

⁶ См.: ГОСТ Р ИСО/ТО 13569-2007. Национальный стандарт Российской Федерации. Финансовые услуги. Рекомендации по информационной безопасности (утв. Приказом Ростехрегулирования от 27.12.2007 № 514-ст).

левые установки, методики проверки, права и обязанности субъектов и объектов контроля, процедуры фиксации и направления результатов контроля информационных систем руководству и собственникам. Внешение изменений в Федеральный закон «Об аудиторской деятельности» в отношении введения в прочих услуг проверки информационной безопасности хозяйствующего субъекта, а также разработка стандартов государственного аудита позволят унифицировать данный вид деятельности» [Сафонова М.Ф., Кривошей Д.Н., 2024: 644–664].

Применительно к пентесту уголовно-правовые риски обусловлены разными обстоятельствами, среди которых отсутствие в теории и практике единой трактовки признаков составов преступлений в сфере компьютерной информации. Более предметно вероятность необоснованного уголовного преследования при пентесте выражается следующими факторами:

- пентест предполагает преодоление средств программно-технической защиты цифрового ресурса, что внешне соответствует признакам неправомерного доступа к охраняемой законом компьютерной информации (ст. 272 Уголовного кодекса Российской Федерации; далее — УК РФ);

- используемый специалистами инструментарий тестовых компьютерных атак может обладать признаками вредоносности по смыслу ст. 273 УК РФ;

- при тестировании специалист может получить доступ к конфиденциальной информации, затрагивающей права и свободы разных лиц. Это может служить основанием для уголовного преследования за нарушение неприкосновенности частной жизни, нарушение тайны переписки или переговоров, неправомерные действия с компьютерной информацией, содержащей персональные данные (ст. 137, 138 и 272¹ УК РФ);

- как и любая другая профессиональная деятельность, пентест может быть связан с наступлением неблагоприятных последствий (например, с производственным травматизмом, повреждением дорогостоящего оборудования и т.п.). Это может быть обусловлено как некомпетентностью, так и заурядным недобросовестным отношением лица к его обязанностям;

- инцидент информационной безопасности может обусловить постановку вопроса о привлечении к уголовной ответственности специалиста в соответствии со ст. 274 УК РФ или ч. 3 ст. 274¹ УК РФ за недобросовестное исполнение обязанностей, связанных с аудитом состояния защищенности объекта информационно-коммуникационной инфраструктуры.

Уголовно-правовой риск обвинения в неправомерном доступе к компьютерной информации в целом устраняется согласием правообладате-

ля цифрового ресурса на тестирование на проникновение. Поскольку ст. 272 УК РФ устанавливает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, такое согласие указывает, что доступ был санкционированным, т.е. правомерным. При этом важно, что согласие касается конкретного (по своему содержанию и методике) тестирования в отношении строго определенного ресурса или ресурсов и в течение ограниченного периода времени. Игнорирование специалистом любого из этих условий не позволит сослаться на правомерность доступа к компьютерной информации.

Согласие должно быть выражено уполномоченным субъектом в надлежащей форме. Дело здесь даже не в том, что отсутствие документально оформленных отношений между сторонами не позволит доказать специалисту в области информационной безопасности, что он действовал по поручению и в интересах владельца ресурса. Правомерный доступ может быть обеспечен только владельцем информационной системы либо иными лицами в пределах их полномочий. Так, например, руководитель филиала не вправе санкционировать такой доступ к единой информационной сети всей компании [Pupillo A., Ferreira A., Varisco G., 2018].

В связи с этим можно допустить вероятность добросовестного заблуждения специалиста в правомерности его действий, когда согласие было дано не уполномоченным субъектом. Так как IT-специалист, как правило, не обладает юридическим образованием и не может знать всех нюансов корпоративного управления, такое заблуждение является основанием квалифицировать содеянное как невинное причинение вреда (ст. 28 УК РФ).

Согласие на тестирование на проникновение должно предельно четко определить его границы. Под границами тестирования и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры понимается перечень объектов данной инфраструктуры, для которых должны проводиться такие тестирования и анализ⁷. Нарушение специалистом по кибербезопасности условий тестирования в этой части также позволяет сделать вывод об общей неправомерности его действий с квалификацией содеянного по ст. 272 УК РФ или ст. 274¹ УК РФ.

Не меньшую трудность создает уголовно-правовой риск пентеста в части возможного уголовного преследования за совершение действий с вредоносными компьютерными программами или вредоносной ком-

⁷ См.: Методические рекомендации Банка России по проведению тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры организаций финансового рынка (утв. Банком России 22.01.2025 № 2-МР) // СПС Консультант Плюс.

пьютерной информацией. В доктрине отмечается, что при анализе законности происхождения программных средств совершения высокотехнологичных преступлений нужно также устанавливать легитимность программного обеспечения, изначально пригодного к решению преступных задач. В эту группу средств входят, например, программы, объединенные назначением «тестирование на проникновение». Особенностью работы таких программ является моделирование несанкционированного доступа к компьютерной системе. В силу уголовно-правовой неурегулированности статуса подобного программного обеспечения его создание и применение могут быть признаны незаконными, хотя оно фактически служит целям информационной безопасности [Поляков В.В., 2024: 435–453].

Пленум Верховного Суда Российской Федерации (далее — ВС РФ) в абз. 2 п. 8 постановления от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая Интернет» сформулировал разъяснение вредоносности программы или иной компьютерной информации, основанное на критерии предназначенности для несанкционированного (скрытого от пользователя) воздействия на данные и нейтрализации средств их защиты⁸.

Подобный подход, определяющий вредоносность программы ее функциональным предназначением оказывать неправомерное (несанкционированное) воздействие на компьютерные данные и системы, следует из буквального толкования ст. 273 УК РФ, является наиболее подерживаемым в доктрине и распространенным в практике.

Вредоносность программы — категория юридическая и находится в компетенции судебно-следственных органов. Компьютерно-техническая экспертиза решает задачу описания общего алгоритма действия программы. Выводы эксперта всегда имеют хотя и определяющий, но не окончательный характер в разрешении вопроса о вредоносности программы. Признаками вредоносного программного обеспечения, которые могут быть установлены судебной компьютерно-технической экспертизой, являются: 1) обладание функционалом уничтожения, блокирования, модификации или копирования пользовательской информации или нейтрализации средств ее защиты; 2) инсталляция без согласия пользователя; 3) функционирование в скрытом от пользователя режиме; 4) операции с компьютерной информацией без согласия пользователя.

Анализ судебной практики показывает, что вопрос о вредоносности компьютерной программы является дискуссионным и характеризуется

⁸ См.: Бюллетень Верховного Суда РФ. 2023. № 3.

состоянием правовой неопределенности. Так, по одному делу суд отмечает: «Утверждения защитника: созданные Ж. программы «Beacon DNS», «beacon_dns_admin», «dns-bot-js» не вредоносны, а являют собой аналог легальных программ тестирования на проникновение, они созданы по заданию работодателя, оказывающего услуги разработки программного обеспечения по защите информации, а потому эти программы не могут нейтрализовать средства защиты, несанкционированно копировать информацию с удаленного компьютера, не могут быть установлены на нем без ведома пользователя, так как для этого требуется создание дополнительной программы, чего не делал Ж., проверены в ходе судебного следствия и не нашли подтверждения»⁹.

В пособиях специалистам по направлению «Информационная безопасность» указывается: «Поиск уязвимостей можно осуществлять вручную, используя полученную информацию и базы данных уязвимостей. Однако это очень долгий и трудоемкий процесс. А можно воспользоваться сканерами уязвимостей... Они позволяют не только находить открытые уязвимости в установленном программном обеспечении и операционных системах, но и определять устаревшие протоколы шифрования» [Бегаев А.Н., Бегаев С.Н., Федотов В.А., 2018: 45].

В то же время изучение судебной практики показывает, что использование специальных продуктов для сканирования объектов информационной инфраструктуры с целью обнаружения уязвимостей может быть квалифицировано по ст. 273 УК РФ: «С. с вышеназванного ноутбука, используя интернет-соединение, предоставленное интернет-провайдером... запустил программу... и приискал удаленный интернет-ресурс правительства... для последующего сканирования на предмет обнаружения уязвимостей программой... Согласия на данное действие со стороны правообладателя ресурса... у С. не имелось»¹⁰.

Аналогичное решение об определении программы как вредоносной, но уже с квалификацией по ч. 1 ст. 274¹ УК РФ, суд принял в следующей ситуации: «Установлено, что М., находясь у себя дома... действуя умышленно, с целью проверки своих навыков по использованию программного обеспечения, достоверно зная, что ресурс... имеющий доменное имя... входит в информационно-телекоммуникационную сеть Университета, то есть относится к объектам критической информационной инфраструктуры, на мобильном телефоне марки... открыл цифровое

⁹ Приговор Фрунзенского районного суда Владимира от 29.10.2021 по делу № 1-23/2021 // СПС Консультант Плюс. Кассационным постановлением Второго кассационного суда общей юрисдикции от 13.01.2023 № 77-4/2023 данный приговор оставлен без изменения.

¹⁰ Постановление Коминтерновского районного суда Воронежа от 27.09.2022 по делу № 1- 751/2022.

окно свободно распространяемого в сети программного обеспечения, предназначенного для сетевого аудита безопасности информационных ресурсов, в том числе в открытых телекоммуникационных сетях, ранее установленного на указанный мобильный телефон, и внес в него данные электронного адреса Университета... После чего М. запустил указанное программное обеспечение с применением дополнительных скриптов... осуществив использование данного программного обеспечения с целью проверки наличия на сайте... уязвимостей»¹¹.

Подобные факты уголовного преследования за использование программ-сканеров не единичны¹². Во всех ситуациях принципиальным аргументом обвинения было, что такие действия — использование программы-сканера для обнаружения уязвимостей объекта информационной инфраструктуры — были совершены без согласия владельца (администратора) цифрового ресурса (отсутствовали договорные отношения на проведение тестирования).

Изучение судебной практики показывает, что ссылки лица на двойное предназначение компьютерной программы не исключает уголовно-правового риска по ст. 273 УК РФ¹³.

В упомянутом ранее постановлении Пленума ВС РФ 15.12.2022 № 37 уже сформулирована позиция, согласно которой не образует преступления использование вредоносной программы с согласия собственника компьютерного устройства и не преследующее цели неправомерного доступа к охраняемой законом компьютерной информации. Данная правовая позиция Верховного Суда внесла некоторую определенность в вопрос о квалификации действий IT-специалистов с компьютерными программами, обладающими функционалом преодоления средств программно-технической защиты. Однако в указанном разъяснении отсутствует указание на распространение. Последнее заключается в сознательном предоставлении лицу либо неограниченному кругу лиц доступа к таким объектам в любой форме. Согласие лица на получение вредоносной программы само по себе не исключает уголовной ответственности за распространение по смыслу ст. 273 УК РФ. Принимая во внимание, что, согласно позиции ВС, исключается преступность не

¹¹ Постановление о прекращении уголовного дела в связи с назначением судебного штрафа Куйбышевского районного суда Омска от 19.01.2024 по делу № 1-21/2024(1-398/2023).

¹² См.: Апелляционное постановление Омского областного суда от 20.02.2023 по делу № 22-491/2023; Приговор Рязского районного суда Рязанской области от 29.12.2020 по делу № 1-163/2020; Приговор Каргапольского районного суда Курганской области от 26.11.2020 по делу № 1-91/2020.

¹³ Приговор Магаданского городского суда Магаданской области от 06.07.2022 по делу № 1-195/2022 // СПС Консультант Плюс.

только санкционированного использования, но и создания вредоносных программ для тестирования системы на состояние защищенности, логично сделать вывод, что применение данного разъяснения возможно и в отношении распространения.

Вместе с тем данный вопрос не нашел окончательного решения как в теории, так и в судебной практике. Показателен следующий пример из практики: «Подсудимый С. в судебном заседании вину в предъявленном ему обвинении в совершении указанного преступления признал частично, пояснив, что он реализовывал компьютерную программу... однако данная программа не является вредоносной программой, а является программой тестирования сайтов, с помощью которой можно выявить уязвимость сайтов».

Суд, принимая решение по делу, оценивая доказательства в совокупности, указал следующее: «К показаниям подсудимого С. в части не признания вины в инкриминируемом преступлении, суд относится с недоверием, поскольку они опровергаются представленными стороной обвинения доказательствами и установленными обстоятельствами, в связи с чем признаются судом недостоверными, расцениваются как выбранная линия защиты с целью избегания уголовной ответственности за содеянное, в связи с чем не могут повлиять на выводы суда о виновности С. в инкриминируемом ему деянии»¹⁴.

Вероятно, при принятии судом данного решения ключевую роль сыграло то, что подсудимый на момент совершения деяния распространил компьютерную программу, обладающую признаками вредоносности, не осуществляя деятельности по тестированию. Программа была реализована через специализированную платформу и лишь с оговоркой, что ее можно использовать для аудита информационной безопасности.

В целом же риск привлечения к уголовной ответственности за использование и распространение тех же программ-сканеров, совершенные с согласия собственника информационной системы и в ходе ее тестирования для проверки уязвимости средств защиты компьютерной информации, следует оценить как низкий. В подтверждение следует указать, что Конвенция Организации Объединенных Наций против киберпреступности (2024) в ст. 11 «Неправомерное использование устройств» напрямую определяет, что не является преступлением получение, производство, продажа, приобретение для использования, ввоз, распространение или иная форма предоставления или владение компьютерными программами, информацией либо устройствами без цели совершения какого-либо из преступлений, признанных таковыми

¹⁴ Приговор Ахтубинского районного суда Астраханской области от 19.09.2022 № 1-207/2022; Постановлением Четвертого кассационного суда общей юрисдикции от 13.06.2023 № 77-2043/2023 данный приговор оставлен без изменения.

в соответствии со ст. 7–10 Конвенции (незаконный доступ; незаконный перехват; воздействие на электронные данные; воздействие на информационно-коммуникационную систему), в рамках разрешенного испытания или защиты информационно-коммуникационной системы¹⁵.

Методика пентеста предполагает, что после доступа к уязвимым сервисам и повышения привилегий до самого высокого уровня, специалист должен собрать доказательства проникновения, которые будут отражены в окончательном отчете для компании-заказчика [Ерышов В.Г., Ларионец К.А., 2022: 209–210]. В этой части, когда лицо соприкасается с чувствительной информацией самого различного рода, возникает риск ответственности по российскому уголовному законодательству за совершение неправомерных действий с конфиденциальной информацией.

Рядом документов в среде тестирования не рекомендуется использование данных, полученных в результате реализации актуальных технологических процессов. Если для тестирования необходимы данные, максимально приближенные к реальным, рекомендуется формирование тестовых массивов данных путем необратимого обезличивания, маскирования и (или) искажения сведений, полученных в результате реализации банковских технологических процессов. Не рекомендуется использование в тестировании данных, в отношении которых на основании законодательства Российской Федерации, внутренних документов организации и (или) договоров с клиентами и контрагентами, распространяется требование конфиденциальности¹⁶.

С точки зрения устранения уголовно-правового риска ответственности специалиста, осуществляющего тестирование на проникновение, за совершение действий с информацией ограниченного доступа, данная рекомендация выглядит наиболее предпочтительной. В ином случае, когда предполагается доступ к реальным данным, соответствующие права и обязанности специалиста необходимо регламентировать в договоре на услугу аудита информационной безопасности.

При тестировании на проникновение в отношении объекта информационной инфраструктуры специалист отвечает за наступление негативных последствий, находящихся в причинно-следственной связи с

¹⁵ См.: Конвенция принята Резолюцией 79/243 Генеральной Ассамблеи ООН от 24.12 2024 и открыта для подписания в октябре 2025 г.). Available at: URL: <https://docs.un.org/ru/A/RES/79/243> (дата обращения: 04.11.2025)

¹⁶ См.: Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем» РС БР ИББС-2.6-2014» (приняты и введены в действие Распоряжением Банка России от 10.07.2014 № Р-556) // СПС Консультант Плюс.

воздействием на компьютерную систему в рамках выполняемых работ. Результаты исследований показывают, что следующим после ограниченного бюджета фактором, препятствующим регулярному тестированию на проникновение, является угроза нарушения непрерывности бизнес-процессов. Перед службой информационной безопасности организации прежде всего стоит задача бесперебойности данных процессов. Поэтому руководители таких служб настороженно относятся к пентестам, поскольку многие из них сталкивались с простоями в работе¹⁷.

Пентест изначально предполагает возможность негативных последствий для тестируемого объекта информационной инфраструктуры. Так, ГОСТ Р 58143-2018 регламентирует: «Варианты тестирования, основанные на неправильном умышленном или неумышленном использовании внешних объектов или зависимых от объекта оценки компонентов, должны моделировать сбои программного обеспечения для выявления ошибок безопасности и потенциальных уязвимостей. Оценщик должен также моделировать нетипичные действия, которые направлены на разрушение предположений, созданных при разработке программного обеспечения относительно собственного состояния и состояния среды функционирования. Результат ошибки может быть неочевидным, последствия ошибки может быть сложно обнаружить вне объекта оценки. Результат может быть представлен в виде сообщения об ошибке или полного нарушения функционирования объекта оценки»¹⁸.

Соответствующие положения национальных стандартов, изначально предполагающие вероятность непредвиденных негативных последствий пентеста, позволяют утверждать: если специалист осуществлял тестирование с соблюдением известных условий эксплуатации объекта оценки, на основе шаблонов атак, разработанных по общепринятым национальным и (или) зарубежным источникам, ответственность за наступление таких последствий должна быть исключена.

В известной мере наступление таких последствий соответствует положениям об обоснованном риске (ст. 41 УК РФ). При исследовании защищенности компьютерной системы специалист, обладая необходимыми знаниями и навыками, опираясь на испытанные методы и

¹⁷ Есть ли необходимость в автоматизации тестирования на проникновение? Available at: URL: <https://www.ptsecurity.com/ru-ru/research/analytics/est-li-neobhodimost-v-avtomatizacii-testirovaniya-na-proniknovenie/#id19> (дата обращения: 03.09.2025)

¹⁸ См.: ГОСТ Р 58143-2018. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения (утв. и введен в действие Приказом Росстандарта от 24.05.2018 № 274-ст).

инструментарий, стремится к достижению общественно полезного результата, но всегда допускает (хотя бы и в самой малой степени) угрозу выхода из строя системы с последующими возможными негативными последствиями.

Другое дело, если такое тестирование проводилось с угрозой для жизни и здоровья многих лиц либо с очевидными нарушениями базовых правил и методик тестирования на проникновение. Здесь ответственность специалиста может быть реализована за проявление преступной неосторожности согласно положениям ст. 274 УК РФ или ч. 3 ст. 274¹ УК РФ.

Специалист, отвечающий за аудит информационной безопасности в организации, может в отдельных случаях нести ответственность и за преступное бездействие. Как правило, это применимо к ситуациям квалификации действий работников, на которых возложены обязанности внутреннего аудита информационной безопасности. Данный подход уже нашел подтверждение в материалах судебной практики. Так, по одному из дел по обвинению в совершении преступления, предусмотренного ч. 3 ст. 274¹ УК РФ, суд указывает, что обвиняемый, «...заведомо зная о том, что на него возложены обязанности по выявлению, анализу и мониторингу уязвимостей систем безопасности информационной системы... а также реагированию на компьютерные инциденты... не исполнил свои обязанности по мониторингу (просмотру и анализу) записей регистрации (аудита) в журнале регистрации событий информационной панели...»¹⁹.

Есть смысл полагать, что ответственность специалиста по информационной безопасности компании за преступное бездействие при наступлении компьютерного инцидента должна выступать реакцией на исключительные (как в приведенном выше примере) проявления профессиональной недобросовестности. В каждом таком случае должно быть неоспоримо установлено, что у IT-специалиста была не гипотетическая (она всегда имеется), а фактическая возможность предотвратить наступление негативных последствий для объектов информационной инфраструктуры организации.

Добровольное предоставление результатов несанкционированного тестирования на проникновение может быть учтено судом при решении вопроса о заглаживании причиненного преступлением вреда и принятии решения об освобождении от уголовной ответственности. Примером служит следующее решение: «Судом установлено, что С. обвиняется в совершении преступления средней тяжести, ранее не судим, полностью признает вину в совершении инкриминируемого ему преступления, имеет довольно молодой возраст, активно способствовал раскрытию и расследованию преступления, каких-либо негативных последствий, в том

¹⁹ Приговор Кызылского городского суда Республики Тыва от 23.08.2024 по делу № 1-1309/2024.

числе реального ущерба, включая вред для деловой репутации потерпевшего в результате противоправной деятельности С. не наступило, им были принесены извинения потерпевшему путем направления соответствующего письма и отчета в электронном виде сканирования о выявленных рисках и уязвимостях системы для укрепления информационной защищенности ресурса. Указанные извинения С. Департаментом были приняты и каких-либо претензий к подсудимому не имеется»²⁰.

Следует поддержать данное решение суда. Сообщение лицом всех сведений, полученных в результате компьютерной атаки, позволяет владельцу информационного ресурса в итоге существенно повысить уровень информационной безопасности. В этом отношении изначально противоправное поведение приводит к положительному результату — устранению уязвимостей системы от актуальных киберугроз.

2. Уголовно-правовые риски Bug Bounty

Риски краудсорсингового метода проверки киберустойчивости объекта информационной инфраструктуры во многом совпадают с уже проанализированными применительно к тестированию на проникновение. Это позволяет сконцентрировать внимание на проблемной тематике, характерной именно для этого (набирающего с каждым годом популярность) метода обнаружения уязвимостей в компьютерных системах.

В России отсутствует специальное регулирование организации и проведения программ (соревнований) неограниченного круга участников (исследователей) по тестированию информационных продуктов и (или) систем на защищенность от несанкционированного проникновения. В 2023 г. законодательная инициатива Минцифры РФ завершилась неудачей.

Обращение к зарубежному законодательству позволяет найти примеры регулирования механизма получения информации об уязвимостях компьютерных систем программой Bug Bounty. Закон Евросоюза «О киберустойчивости» предписывает: «Производители должны иметь соответствующие политики и процедуры, включая скоординированное раскрытие уязвимостей, упомянутых в пункте (5) Части II Приложения I, для обработки и устранения потенциальных уязвимостей в продукте с использованием цифровых элементов, о которых сообщается из внутренних или внешних источников»²¹. В приложении оговаривается,

²⁰ Постановление о прекращении уголовного дела в связи с деятельным раскаянием Коминтерновского районного суда Воронежа от 27.09.2022 по делу № 1-751/2022.

²¹ Cyber Resilience Act. Available at: URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2847> (дата обращения: 09.09.2025)

что производители обязаны не только применять регулярные тесты безопасности продукта с цифровыми элементами, но и обеспечивать соблюдение политики скоординированного раскрытия информации об уязвимостях.

С 15.02.2023 в Бельгии действуют правила участников программ Bug Bounty (Belgian Act on the Protection of Whistleblowers of November 28, 2022). По данному Закону лица, сообщающие информацию об уязвимостях в Центр кибербезопасности Бельгии, не будут считаться правонарушителями в связи с их действиями, необходимыми для сообщения об уязвимости, при соблюдении условий: 1) физическое или юридическое лицо должно доказать, что оно незамедлительно направило письменный отчет об уязвимости в Центр кибербезопасности и в соответствующую организацию (владельцу системы) в соответствии с процедурой на веб-сайте Центра. Подача таких отчетов невозможна после начала уголовного судопроизводства; 2) исследователь должен действовать без преступного умысла; 3) сообщивший не должен выходить за рамки необходимых и соразмерных действий для подтверждения потенциальной уязвимости. Инструкции указаны на веб-сайте Центра; 4) исследователь не должен публично раскрывать информацию об уязвимости без согласия Центра.

Важно, что эти положения применяются ко всем организациям Бельгии, в том числе и к тем, у которых нет собственной программы Bug Bounty. Комментируя значимость принятого Закона, специалисты отметили: «До сих пор этичный хакинг, даже совершенный с самыми благими намерениями, подлежал наказанию в соответствии с бельгийским уголовным законодательством. Как следствие, этичный хакер, сообщавший организации об уязвимости безопасности в ее системах, рисковал быть привлеченным к уголовной ответственности. Новое законодательство устраняет этот риск и, как мы надеемся, приведет к увеличению обнаружения уязвимостей, сообщаемых организациям, что позволит им повысить безопасность их систем»²².

С положительной стороны следует отметить то обстоятельство, что в российской судебной практике отсутствуют примеры осуждения участника (испытателя) или организатора программы Bug Bounty. Это, однако, не позволяет быть уверенным, что риски уголовного преследования в этой сфере отсутствуют вовсе. По данным исследователей, уголовно-правовые риски занимают лидирующее место (35%) в ряду остальных, которые препятствуют развитию данной практики информационной безопасности [Kadam R., Roy B., 2025: 3219–3229].

²² New Belgian legal framework gives safe harbor to ethical hackers and bug bounty hunters. Available at: URL: <https://www.intigriti.com/blog/news/new-belgian-legal-framework-gives-safe-harbor-to-ethical-hackers-and-bug-bounty-hunters> (дата обращения: 15.08.2025)

Традиционный Bug Bounty характеризуется правовой неопределенностью оценки действий испытателя как правомерных при преодолении средств программно-технической защиты информационного продукта и (или) системы. В отличие от пентеста, здесь соглашение не заключается с участником программы (испытателем). Присоединение исследователя к программе путем акцепта условий ее проведения, пожалуй, нельзя признать таким соглашением. Вопрос является дискуссионным.

В зарубежной доктрине также отмечается, что риск привлечения к уголовной ответственности за неправомерный доступ к компьютерной информации является наиболее высоким для участников Bug Bounty. Однако если такой доступ был реализован строго в соответствии с правилами кибериспытаний, его предлагается оценивать как правомерный [Vostoupal J., Stupka V., 2024: 5]. Применительно к случаям, в которых из-за неправильного толкования правил Bug Bounty участник неправомерно преодолел средства программно-технической защиты, содеянное рассматривается как неосторожная форма неправомерного доступа к защищенной компьютерной системе (negligent data or system interference)²³.

По российскому законодательству такие действия участника кибериспытаний подпадают под признаки нарушения правил доступа по смыслу ст. 274 УК РФ. Ответственность наступает только если это деяние повлекло уничтожение, блокирование, модификацию или копирование компьютерной информации и причинение крупного ущерба (свыше 1 млн. руб.).

В условиях отсутствия ясного правового регулирования нельзя согласиться с тем, что программа Bug Bounty предстает как своего рода призыв к осуществлению компьютерных атак на ту или иную информационную систему с согласия ее владельца при очевидном игнорировании интересов пользователей. Такая система может содержать чувствительную (конфиденциальную) информацию третьих лиц. Подобное решение владельца ресурса создает угрозу причинения существенного вреда правам и законным интересам других лиц (в том числе в части неприкосновенности частной жизни, тайны переписки, коммерческой тайны и т.п.). Нельзя игнорировать то, что сам механизм Bug Bounty не позволяет его организатору контролировать поведение всех испытателей. Последние,

²³ Пример — положения ст. 232 Уголовного кодекса Чехии, где предусмотрена ответственность за вмешательство в работу компьютерного оборудования по неосторожности. Но ответственность наступает только при условии причинения существенного ущерба имуществу другого лица. Само по себе деструктивное воздействие на данные, аппаратное или программное обеспечение еще не позволяет говорить о признаках состава преступления. Available at: URL: <https://rm.coe.int/czech-criminal-code-in-english-as-amended-in-2023/1680b5e324> (дата обращения: 12.09.2025)

получив доступ в рамках программы, могут совершить неправомерные действия (передавать чувствительную информацию третьим лицам, использовать в личных целях и др.) [Kinis U., 2018: 508–522].

Именно поэтому в действующих программах Bug Bounty организаторы справедливо оговаривают, что исследователям запрещено получать доступ к данным другого пользователя, изменять и уничтожать их, а также раскрывать любую конфиденциальную информацию, случайным образом полученную в ходе поиска уязвимостей; воздействовать на учетные записи других пользователей; использовать обнаруженную уязвимость в личных целях; пытаться получать доступ к учетным записям, данным пользователей информационных систем или к любым другим конфиденциальным данным, выходящим за пределы действий, минимально необходимых для демонстрации найденной уязвимости; целенаправленно выгружать персональные данные пользователей из внутренних систем веб-сервисов и приложений, иных информационных ресурсов, не указанных в техническом задании. В целом организаторы Bug Bounty обоснованно исходят из того, что изменение, модификация, удаление, замена и любые другие действия с информацией в тестируемой системе возможны лишь в отношении данных, которые ассоциированы с учетной записью самого участника (своего рода специально созданный тестовый аккаунт), либо другого пользователя, который дал согласие на совершение таких действий²⁴.

Таким образом, недопустимо определение условием подтверждения выявленной уязвимости действия участника по копированию конфиденциальной информации (например, персональных данных пользователей). Это создает прямую угрозу уголовного преследования в соответствии со ст. 272¹ УК РФ за незаконные действия (использование, передача, сбор и хранение) с компьютерной информацией, содержащей персональные данные. При этом действия самих организаторов могут быть квалифицированы по ч. 6 той же статьи как создание и обеспечение функционирования ресурса в Интернете, заведомо предназначенного для совершения незаконных действий в отношении компьютерной информации, содержащей персональные данные. В такой форме допускается организация Bug Bounty строго с использованием специально привлеченных для этого аккаунтов клиентов (в согласии на обработку персональных данных должна оговариваться возможность доступа к таким данным в процессе кибериспытаний на проникновение).

Неприемлемо и условие о переводах денежных средств без согласия клиента, что создает угрозу уголовного преследования в соответствии

²⁴ См., напр.: программа Bug Bounty «Информационные ресурсы Нижегородской области». Available at: URL: <https://bugbounty.standoff365.com/programs/ppov> (дата обращения: 09.09.2025)

с п. «г» ч. 3 ст. 158 УК РФ. Несмотря на возможную незначительность размера изымаемого имущества (до 2500 руб.), содеянное подпадает под признаки квалифицированного состава кражи — с банковского счета потерпевшего. В данном случае целесообразно реализовать иное решение, которое явно бы указывало либо на отсутствие безвозмездности изъятия (испытатель пополняет счет участника и потом уже переводит средства со счета), либо на ничтожность ущерба и отсутствие корыстной цели (испытатель совершает символическую транзакцию в размере 1 руб.).

Обращаясь к вопросу уголовно-правовых рисков Bug Bounty, нельзя не рассмотреть дело Дж. Салливана. Бывший директор службы безопасности «Юбер» Салливан принял решение о выплате двум хакерам, взломавшим инфраструктуру компании в 2016 г., требуемого ими вознаграждения. Салливан скрыл данный инцидент и утечку данных более 50 млн. пассажиров и 600 000 водителей «Юбер» от контролирующих органов. При этом он санкционировал выплату 100 тыс. долл. в рамках программы Bug Bounty «Юбер», хотя по данной программе максимальный размер выплаты составлял лишь 10 тыс. долл. (Хакеры угрожали в случае отказа от передачи требуемой суммы распространить похищенные у компании конфиденциальные данные пользователей). Салливана признали виновным в воспрепятствовании правосудию и в сокрытии тяжкого преступления²⁵.

Решение по делу Салливана было воспринято весьма критически специалистами в сфере информационной безопасности: «Это решение лишает частные организации возможности управлять своими компьютерными системами, поскольку трактует Закон о компьютерном мошенничестве и злоупотреблениях так, что он запрещает им ретроспективно разрешать доступ к своим системам. Согласно этому толкованию исследователи безопасности, действующие добросовестно, выявляющие уязвимости и ответственно сообщающие о них компаниям, по-прежнему могут быть привлечены к уголовной ответственности, если они получили доступ к системе ранее официального разрешения. Толкование совершенно не соответствует современным практикам кибербезопасности и подвергает организации, руководителей служб информационной безопасности и национальную безопасность повышенному риску»²⁶.

По российскому законодательству такие действия лица, наделенного управленческими полномочиями в коммерческой организации, подпа-

²⁵ Former Uber Security Chief Found Guilty of Hiding Hack from Authorities. Available at: URL: <https://www.nytimes.com/2022/10/05/technology/uber-security-chief-joe-sullivan-verdict.html> (дата обращения: 09.08.2025)

²⁶ См.: A Court Ruling on Bug Bounties Just Made the Internet Less Safe. Available at: URL: <https://www.infosecurity-magazine.com/opinions/court-ruling-bug-bounties-internet/> (дата обращения: 25.08.2025)

дают под признаки злоупотребления полномочиями (ст. 201 УК РФ). Не исключена и вероятность ответственности за хищение имущества организации в форме растраты (ст. 160 УК РФ).

Обязанность информирования об инцидентах информационной безопасности касается только субъектов критической информационной инфраструктуры РФ. Положения Закона предписывают субъектам критической информационной инфраструктуры: 1) незамедлительно информировать о компьютерных атаках и компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ; 2) оказывать содействие должностным лицам федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов; 3) реагировать на компьютерные инциденты в порядке, утвержденном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ²⁷.

Указанные положения Закона в целом направлены на достижение транспарентности и кооперации. Замалчивание компьютерных инцидентов дает преимущество преступникам, позволяет им предпринимать новые компьютерные атаки. Практика сокрытия проблем в сфере информационной безопасности известна. Компании неохотно сообщают об инцидентах, связанных с утечкой пользовательской информации. Это порождает репутационные и финансовые потери. Неисполнение указанных выше обязанностей соответствующими субъектами объективно создает угрозу причинения существенного вреда не только защищенности критической информационной инфраструктуры РФ, но также правам и свободам отдельных граждан и организаций.

Из приведенного выше следует, что сокрытие информации об инцидентах информационной безопасности с объектами, не относящимися к критической информационной инфраструктуре РФ, не может служить основанием для привлечения к уголовной ответственности за злоупотребление полномочиями (ст. 201 УК РФ).

²⁷ Статья 9 Федерального закона от 26.07.2017 № 187-ФЗ (ред. от 07.04.2025) «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС Консультант Плюс.

Наконец, следует указать на вполне очевидный риск привлечения к уголовной ответственности в случае, когда участник программы кибериспытаний вводит в заблуждение ее организатора. Правила проведения Bug Bounty предполагают, что получение информации об уязвимостях компьютерной системы надлежит осуществлять без использования инсайдерской информации либо иной помощи сотрудников компании-организатора кибериспытаний²⁸. Если информация была получена именно так, что позволило участнику сфальсифицировать отчет и получить незаслуженное вознаграждение, содеянное может быть квалифицировано как мошенничество (ст. 159 УК РФ).

Заключение

Современная практика кибербезопасности активно использует методы внешнего тестирования и программы стимулирования выявления уязвимостей. Эти подходы позволяют организациям заранее обнаруживать уязвимости, а специалистам-исследователям — зарабатывать и развивать свои профессиональные навыки.

В отсутствие специального правового регулирования «этичный хакер», ищущий уязвимости в информационных системах, несомненно, подвергает себя риску уголовного преследования. Для полного решения проблемы соответствующих рисков требуется внятное определение правового режима тестирования информационных систем на киберустойчивость. Такое регулирование должно охватывать как целевое тестирование на проникновение в рамках отдельных договорных отношений и публичных конкурсов, так и процедуры разглашения выявленных уязвимостей, информация о которых была получена лицом по собственной инициативе.

В настоящее время митигация уголовно-правовых рисков специалистами в области информационной безопасности обеспечивается отдельными разъяснениями Верховного Суда Российской Федерации и доктринальным толкованием.

²⁸ Правила одной из программ содержат следующие запреты: 1) устраиваться на работу в компанию для получения легитимного доступа к системам компании и реализации недопустимых событий; 2) подкупать сотрудников компании или осуществлять с ними сговор; пользоваться иной добровольной помощью действующих сотрудников компании (прикрытие действий исследователя, облегчение доступа или реализации недопустимого события, добровольное предоставление оборудования); 3) использовать любые способы воздействия на работников компании; 4) подкупать, иным образом воздействовать на поставщиков услуг или контрагентов компании, вступать с ними в сговор. См.: Программа Bug Bounty «Tom Tailor». Available at: URL: <https://bugbounty.standoff365.com/programs/tom-tailor> (дата обращения: 12.09.2025)

В целом политика государства в исследуемой области должна быть направлена к одной общей цели — максимально возможной популяризации практики выявления и надлежащего раскрытия информации об уязвимостях в целях защиты объектов информационной инфраструктуры, в том числе реализацией образовательных и иных просветительских кампаний, введения систем премирования и общественного признания социально полезного хакинга. Необходимо не только создавать правовые основания для деятельности «этичных хакеров», но и вести за них борьбу в идеологическом поле.



Список источников

1. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение. СПб.: Университет ИТМО, 2018. 45 с.
2. Ерышов В.Г., Ларионец К.А. Основные этапы, методики и средства проведения тестирования на проникновение. Сборник докладов научной конференции «Обработка, передача и защита информации в компьютерных системах» 2022 г. СПб.: Санкт-Петербургский университет аэрокосмического приборостроения, 2022. С. 209–210.
3. Жалинский А.Э. Уголовное право в ожидании перемен: теоретико-инструментальный анализ. М.: Проспект, 2009. 400 с.
4. Поляков В.В. Криминалистическая классификация средств высокотехнологических преступлений // Вестник Санкт-Петербургского государственного университета. Право. 2024. № 2. С. 435–453.
5. Сафонова М.Ф., Кривошей Д.Н. Аудит информационной и кибербезопасности: нормативное регулирование и проблемы функционирования // Международный бухгалтерский учет. 2024. №6. С. 644–664.
6. Смородина Е.П., Бурцев Р.Д. и др. Экономико-правовые основы этичного хакинга в Российской Федерации // Цифровая и отраслевая экономика. 2023. № 2. С. 116–122.
7. Fiorinelli G., Zucca V. Is Road to Hell Paved with Good Intentions? A Criminological and Criminal Law Analysis of Prospective Regulation for Ethical Hacking in Italy and the EU. In: Papers of 8th Italian Conference on Cyber Security. 2024. <https://ceur-ws.org/Vol-3731/paper45.pdf>
8. Kadam R., Roy B. Bug Bounty Programs: A Comprehensive Meta-Analytical Review of Strategies, Challenges, and Future Directions. International Research Journal on Advanced Engineering Hub, 2025, vol. 3, pp. 3219–3229. <https://doi.org/10.47392/IRJAEH.2025.0473>
9. Kinis U. From Responsible Disclosure Policy towards State Regulated Responsible Vulnerability Disclosure Procedure: Latvian approach. Computer Law & Security Review, 2018, vol. 34, no. 3, pp. 508–522. <https://doi.org/10.1016/j.clsr.2017.11.003>
10. Kuehn A., Mueller M. Analyzing bug bounty programs: an institutional perspective on the economics of software vulnerabilities. In: 2014 TPRC Conference Paper, 2014, pp. 1–16. <http://dx.doi.org/10.2139/ssrn.2418812>
11. Laszka A. et al. Rules of Engagement for Bug Bounty Programs. In: Financial Cryptography and Data Security. International Conference. Berlin: Springer, 2018, pp. 138–159. <https://doi.org/10.1007/978-3-662-58387-68>

12. Park S., Albert K. Researcher's Guide to Some Legal Risks of Security Research. The Cyberlaw Clinic at Harvard Law School, 2020. 31 p. <https://clinic.cyber.harvard.edu/wp-content/uploads/2024/08/Security-Researchers-Guide-8-2-24.pdf>
13. Pupillo A., Ferreira A., Varisco G. Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges. In: Report of a CEPS Task Force, 2018. <https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/>
14. Reddy P., Pelletier J. The Pentest Method for Business Intelligence. In: Papers of the Jubilee International Convention on Information, Communication and Electronic Technology. 2022, pp. 1117–1125. <https://doi.org/10.23919/MIPRO55190.2022.9803788>
15. Tudosi A.-D. et al. Research on Security Weakness Using Penetration Testing in a Distributed Firewall. Sensors, 2023, vol. 23, no. 5, pp. 1–18. <https://doi.org/10.3390/s23052683>
16. Vostoupal J., Stupka V. et al. The Legal Aspects of Cybersecurity Vulnerability Disclosure: to the NIS 2 and beyond. Computer Law & Security Review, 2024, vol. 53, pp. 1–18. <https://doi.org/10.1016/j.clsr.2024.105988>

Информация об авторе:

Е.А. Русскевич — доктор юридических наук, доцент.

Статья поступила в редакцию 31.10.2025; одобрена после рецензирования 24.12.2025; принята к публикации 15.01.2026.

Legal Issues in the **DIGITAL AGE**

ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ТЕКСТА СТАТЕЙ

Представленные статьи должны быть оригинальными, не опубликованными ранее в других печатных изданиях. Статьи должны быть актуальными, обладать новизной, содержать выводы исследования, а также соответствовать указанным ниже правилам оформления. В случае ненадлежащего оформления статьи она направляется автору на доработку.

Статья представляется в электронном виде в формате Microsoft Word по адресу: lawjournal@hse.ru

Адрес редакции: 109028, Москва, Б. Трехсвятительский пер, 3, оф. 113

Рукописи не возвращаются.

Объем статьи

Объем статей до 1,5 усл. п.л., рецензий — до 0,5 усл. п.л.

При наборе текста необходимо использовать шрифт «Times New Roman». Размер шрифта для основного текста статей — 14, сноска 11; нумерация сносок сплошная, постраничная. Текст печатается через 1,5 интервала.

Название статьи

Название статьи приводится на русском и английском языке. Заглавие должно быть кратким и информативным.

Сведения об авторах

Сведения об авторах приводятся на русском и английском языках:

- фамилия, имя, отчество всех авторов полностью
- полное название организации места работы каждого автора в именительном падеже, ее полный почтовый адрес.
- должность, звание, ученая степень каждого автора
- адрес электронной почты для каждого автора

Аннотация

Аннотация предоставляется на русском и английском языках объемом 250–300 слов. Аннотация к статье должна быть логичной (следовать логике описания результатов в статье), отражать основное содержание

(предмет, цель, методологию, выводы исследования).

Сведения, содержащиеся в заглавии статьи, не должны повторяться в тексте аннотации. Следует избегать лишних вводных фраз (например, «автор статьи рассматривает...»).

Исторические справки, если они не составляют основное содержание документа, описание ранее опубликованных работ и общеизвестные положения, в аннотации не приводятся.

Ключевые слова

Ключевые слова приводятся на русском и английском языках. Необходимое количество ключевых слов (словосочетаний) — 6–10. Ключевые слова или словосочетания отделяются друг от друга точкой с запятой.

Сноски

Сноски постраничные.

Сноски оформляются согласно ГОСТ Р 7.0.5-2008 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления», утвержденному Федеральным агентством по техническому регулированию и метрологии. Подробная информация на сайте <http://law-journal.hse.ru>.

Тематическая рубрика

Обязательно код международной классификации УДК.

Список литературы

В конце статьи приводится список литературы. Список следует оформлять по ГОСТ 7.0.5-2008.

Статьи рецензируются. Авторам предоставляется возможность ознакомиться с содержанием рецензий. При отрицательном отзыве рецензента автору предоставляется мотивированный отказ в опубликовании материала.

Плата с аспирантов за публикацию рукописей не взимается.