DOI: 10.24412/2075-7913-2025-2(98)-68-73

УДК 342.41 + 342.511.5

Евлоев Т. Я.

ПРАВОВОЕ ОПРЕДЕЛЕНИЕ И РЕГУЛИРОВАНИЕ ЦИФРОВОЙ ИНФОРМАЦИИ, ЦИФРОВЫХ СИСТЕМ И КИБЕРДЕЯТЕЛЬНОСТИ В КОНТЕКСТЕ КИБЕРУГРОЗ

Аннотация. *В статье рассматриваются проблемы правового определения понятий цифровой информации, цифровых систем и кибердеятельности. Основным направлением исследования является попытка систематизировать и обобщить текущие правовые определения перечисленных понятий, выделить основные проблемы, освещаемые в литературе. В процессе анализа выявляется неточность и отсутствие единого подхода к цифровой информации и кидбердеятельности и системности в правовом поле, российское законодательство и правоприменение при этом характеризуется фрагментарностью и непоследовательностью, но, вместе с тем, и положительным стремлением к уточнению и адаптации к современным технологическим вызовам. Отдельное внимание уделяется анализу правовой регламентации кибердеятельности в контексте киберугроз. В этом ключе российское право демонстрирует большую последовательность и адаптивность, однако выявляются дисбаланс в регуляции технических и социально-психологических кибердействий, фрагментарное и неэффективное правоприменение.*

Ключевые слова: *киберугрозы, цифровое право, концептуальный анализ, цифровые активы, цифровизация, кибердеятельность*

Для цитирования: Евлоев Т. Я. Правовое определение и регулирование цифровой информации, цифровых систем и кибердеятельности в контексте киберугроз // Проблемы права. 2025. Т. 2 (98). С. 68–73.

Yevloev T. Ya.

LEGAL DEFINITION AND REGULATION OF DIGITAL INFORMATION, DIGITAL SYSTEMS AND CYBER ACTIVITIES IN THE CONTEXT OF CYBER THREATS

Abstract. *In the article are considered the problems of legal definition of the concepts of digital information, digital systems and cyber activities. The main focus of the study is an attempt to systematize and summarize the current legal definitions of the listed concepts, to highlight the main problems covered in the literature. The analysis reveals the imprecision and lack of a unified approach to digital information and cyber activities and systematicity in the legal field, Russian legislation and law enforcement is characterized by fragmentation and inconsistency, but, at the same time, a positive desire for clarification and adaptation to modern technological challenges. Special attention is paid to analyzing the legal regulation of cyber activities in the context of cyber threats. In this regard, Russian law demonstrates greater consistency and adaptability, but it reveals an imbalance in the regulation of technical and socio-psychological cyber activities, fragmented and ineffective law enforcement.*

Keywords: *cyber threats, digital law, conceptual analysis, digital assets, digitalization, cyber activities.*

Правовой ландшафт, связанный с цифровой информацией и системами в Российской Федерации, претерпевает значительные изменения, обусловленные стремительным развитием цифровых технологий и необходимостью соответствующей адаптации правовой базы. Во-первых, правовой статус цифровой информации и систем в России характеризуется динамичным взаимодействием между существующими правовыми нормами и возникающими реалиями цифровой эпохи. Однако, в то же время, на настоящий момент единое правовое определение цифровой информации и цифровых систем с учетом всех доступных в настоящий момент технических возможностей до конца не выработано. Так, Сидоренко [1] в нескольких своих работах, посвященных адаптивности права, подчеркивает структурную инертность российских правовых механизмов перед лицом цифровой трансформации. Она обращает внимание на двойную проблему концептуальных инноваций и системной гибкости, указывая, что хотя правовая система формально интегрирует цифровые понятия, она часто не отражает их реальную сложность и динамику. Эту точку зрения поддерживает Кузьмин [2], который рассматривает социологические последствия дигитализации права, отмечая, что право остается нормативно жестким, в то время как цифровые практики по своей природе изменчивы. Рузанова [3] развивает этот аргумент и приходит к выводу, что в российском законодательстве отсутствует интегрированная структура, в которой цифровые нормы могли бы систематически присутствовать. Она предполагает, что этот структурный недостаток препятствует как согласованности законодательства, так и эффективности правоприменения.

Цельность правового подхода и его интегрированность в существующее правовое поле, на наш взгляд, является наиболее серьезным вопросом. Так, например, в ряде работ в этом ключе утверждается, что цифровая информация должна рассматриваться не просто как производная от традиционных имущественных или информационных категорий, а как объект sui generis, обладающий особыми свойствами, требующими особого правового режима [4]. Подчеркивается, что в существующей в России правовой базе отсутствует единое операциональное определение цифровых прав, что подрывает как возможность их реализации, так и доктринальную ясность. Так, одним из основополагающих законодательных актов в данной области является Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Данный закон устанавливает общие принципы регулирования отношений в сфере информации и информационных технологий, а также определяет права и обязанности участников информационного пространства. Однако, широкие и порой расплывчатые формулировки закона затрудняют его толкование. Так, статья 2 определяет информацию как «сведения (сообщения, данные) независимо от формы их представления», что не позволяет точно определить понятие информации в контексте быстро развивающихся цифровых технологий. Кроме того, статья 12 описывает государственное регулирование в сфере информационных технологий, но не содержит подробных механизмов его реализации, что приводит к неопределённости в правоприменительной практике.

В целях решения проблемы растущего значения цифровых активов 18 марта 2019 года Федеральным законом № 34-ФЗ в Гражданский кодекс Российской Федерации были внесены поправки. Этот закон ввел статью 141.1, определяющую цифровые права как обязательства и другие права, предусмотренные законом, содержание и условия которых определяются правилами информационной системы, отвечающей критериям, установленным законом. Хотя это представляет собой позитивный шаг на пути к признанию цифровых прав в рамках гражданского права, использование правил информационной системы для определения содержания этих прав вызывает обеспокоенность в отношении правовой определенности и возможности произвольного толкования. Закон не проводит четкого разграничения между цифровыми и традиционными правами собственности, что приводит к неопределенности в юридических сделках с цифровыми активами. Кроме того, в сфере гражданского и коммерческого права выявляются несоответствия между теоретической квалификацией и практическим применением, особенно в области обмена цифровыми активами, формирования договоров и цифровых доказательств [5]. В работах [6] и [7] подчеркивается, что правовая инфраструктура цифровой экономики остается недостаточно развитой, а правовой статус цифровых платформ, баз данных

и алгоритмов до сих пор является предметом дискуссий. Примечательно, что российское гражданское и коммерческое право также начало признавать цифровые угрозы в качестве правовых явлений, влияющих на договорные отношения, распределение ответственности и процедуры доказывания. Лаптев отмечает, что цифровая информация, которая исторически рассматривалась как второстепенный объект гражданского оборота, сегодня выступает в качестве основного вектора риска в коммерческих сделках и должна быть юридически определена в терминах, отражающих ее уязвимость к киберугрозам. Это касается не только потери данных и манипуляций с ними, но и неправильного толкования алгоритмов, кампаний по дезинформации и зависящих от платформы асимметрий, которые подрывают справедливость договора или целостность рынка, усугубляют риск монополизации в определенных областях.

В то же время, вместо системности, существующий законодательный подход часто прибегает к фрагментарным отраслевым нормам, которые либо дублируют друг друга, либо оставляют юридически неопределенными существенные аспекты кибердеятельности. Более того, Пинкевич (2019)[8] выявляет несоответствие между способностью уголовного законодательства реагировать на цифровые правонарушения и реальной практикой поведения киберпреступников, подчеркивая, что латентность, интернационализация и анонимность цифровых преступлений требуют нового поколения правовых определений и процессуальных инструментов. Неоднозначность правового статуса цифровых технологий распространяется и на сферу государственного управления. Бондарев [9] исследует, как цифровые системы интегрируются в государственное управление и публично-правовые процессы, и показывает, что, хотя эти системы функционально необходимы, их правовая основа остается непоследовательной, особенно в части административной ответственности и цифрового суверенитета. Романовская [10] утверждает, что концептуальные категории права, информационного общества и цифрового суверенитета пересекаются таким образом, что еще не получили адекватного теоретического осмысления в российской правовой доктрине, что приводит к нормативной фрагментации и стратегической неопределенности.

Основным законом, который регулирует вопросы кибербезопасности в России, является Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критически важной информационной инфраструктуры Российской Федерации». Этот закон устанавливает правовые и организационные основы защиты критически важной информационной инфраструктуры (КИИ). Согласно данному закону, организации, эксплуатирующие КИИ, обязаны применять меры безопасности, сообщать о любых инцидентах и сотрудничать с государственными органами. Однако в сфере правоприменения остаются некоторые неясности, особенно в определении понятия «критически важная информационная инфраструктура» и конкретных обязательств, которые накладываются на операторов. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» определяет основные принципы обеспечения информационной безопасности. Киберугрозы характеризуются как незаконное проникновение или угроза проникновения внутренних или внешних субъектов в описанную выше инфраструктуру для достижения политических, социальных или иных целей. Несмотря на то, что этот закон служит основой для регулирования в данной сфере, он не содержит конкретных положений, касающихся новых технологий и киберугроз, что может затруднить его практическое применение.

В Уголовном кодексе Российской Федерации киберпреступления рассматриваются в главе 28, которая включает статьи 272–274.1. Статья 272 устанавливает уголовную ответственность за несанкционированный доступ к компьютерной информации. Статья 273 определяет наказание за создание и распространение вредоносного программного обеспечения. А статья 274 регулирует вопросы нарушения правил эксплуатации информационных систем. Важно в этом контексте отметить, что ключевым аспектом концептуализации киберугроз в российской правовой мысли является понятие адаптивного регулирования. Сидоренко [1] полагает, что цифровая трансформация заставила российское право стать более рефлексивным и контекстно-чувствительным, признавая, что киберугрозы не статичны, а развиваются вместе с технологическим прогрессом. Это особенно заметно в попытках формализовать адаптивные правовые модели, которые опираются на гибкие право-

вые категории, упреждающее регулирование и итеративную обратную связь с технологическими системами. В настоящее время такие модели оказывают все большее влияние на разработку нормативных актов, особенно в таких областях, как безопасность данных, облачная инфраструктура и системы цифровой идентификации [2, 8]. Тем не менее, финальная реализация этих идей и тенденций на настоящий момент часто оказывается все так же не системна. Например, статья 274.1, введённая Федеральным законом от 26 июля 2017 года № 194-ФЗ, направлена на защиту критически важных информационных инфраструктур от незаконного вмешательства. Несмотря на наличие соответствующих положений в законодательстве, практика их применения остаётся неоднозначной. Количество обвинительных приговоров по делам о киберпреступлениях остаётся небольшим, что вызывает сомнения в эффективности правовых норм в этой сфере. Кроме того, этот закон опирается на понятие «критически важных инфраструктур», размытость которого для правоприменения уже обсуждалась выше.

Таким образом, как мы видим, системная классификация и интеграция киберугроз в правовую доктрину остаются актуальной проблемой. Как отмечает Полякова [11], систематизация российского права под влиянием цифровых технологий осложняется отсутствием четкой метаправовой архитектуры. Нормы кибербезопасности, кроме обсужденных выше, разбросаны по федеральным законам, указам президента, отраслевым нормативным актам и неформальным руководствам, что создает фрагментарный правовой ландшафт и дополнительные сложности для правоприменения. Такая разрозненность препятствует последовательной правовой оценке, особенно в случаях, связанных с анонимными кибератаками или инцидентами, а также с теми инцидентами, которые происходят на пересечении территориальной, ведомственной и иных юрисдикций. В этом ключе Беликова [12], обсуждая проект Цифрового кодекса России, говорит как о перспективах, так и об ограничениях кодификации цифровых норм в единый правовой акт.

Важно также обратить внимание, что в Доктрине информационной безопасности Российской Федерации также сформулирован взгляд государства на киберугрозы, которые подразделяются на информационно-психологические и информационно-технические. Особое внимание в доктрине уделяется защите информационной инфраструктуры, под которой понимается совокупность информационных систем, веб-сайтов и сетей связи, расположенных на территории России или используемых в соответствии с международными договорами. Таким образом, на текущий момент с концептуальной точки зрения российское право более регламентировано в сфере технической безопасности информации, должным образом не учитывая информационно-психологические угрозы. Тем временем, с развитием продвинутого мошенничества, распространения фейковой информации эта сфера кажется не менее, если в каком-то смысле не более важной для четкого и эффективного регламентирования. В этом ключе при анализе трансформации юридической науки в России, рядом авторов отмечается, что юридическое образование и теория еще не полностью интегрировали эпистемологические последствия цифровизации [11, 13].

Одной из наиболее актуальных проблем, выявленных в литературе, является сложность разработки компетентной и учитывающей контекст правовой оценки цифровых правонарушений. Поскольку цифровое поведение часто связано с новыми формами агентов и субъектов, децентрализацией и трансграничным взаимодействием, традиционные категории вины, причинно-следственной связи и ответственности становятся проблематичными. Это особенно очевидно при правовом регулировании автоматизированных систем и искусственного интеллекта, где остается неясным, как возлагать ответственность в случае причинения вреда или неисправности. В свою очередь, Гиреев [14], исследуя нормативно-правовое обеспечение цифровизации, утверждает, что институциональный аппарат регулирования цифровой трансформации характеризуется диффузностью регулирования, дублированием юрисдикций и нечеткостью мандатов. Отсутствие нормативных критериев оценки преднамеренности действий, совершенных в цифровой среде, приводит к доктринальной неопределенности и судебной непоследовательности [15, 16]. Во всех областях цифрового права в России — гражданской, административной, уголовной и публичной — общим является необходимость более глубокой интеграции технических знаний в правовые процессы [17]. Таким образом, на текущий момент

можно выявить следующие основные особенности и проблемы правового определения и регулирования цифровой информации и цифровых систем в контексте киберугроз:

1. Российское право активно предпринимает попытки адаптироваться к развитию технологий и способов обработки и использования информации;

2. При защите от киберугроз закон в большей степени регламентирует техническую, а не информационно-психологическую и социальную сторону вопроса. С одной стороны, это делает правоприменение более быстрым и эффективным в вопросах защиты критической инфраструктуры, суверенитета, технической части телекоммуникационной сети, но, с другой стороны, существующих законов и постановлений часто оказывается недостаточно, чтобы дать полную правовую оценку новым видам мошенничества, распространения ложной информации, использованию авторских и иных прав;

3. Недостаток точности в определениях цифровой информации, критической инфраструктуры, кибердеятельности усложняет правовую оценку действий любых субъектов в цифровом информационном пространстве. К этому прибавляется отсутствие отдельных определений для простых и сложных нейросетевых алгоритмов, оценки деятельности с помощью нейросетей и принципов распределения ответственности при использовании таких сложных систем;

4. Недостаток цельности и системности делает правоприменение неэффективным, во многих случаях остается не до конца ясным механизм взаимодействия между государственными структурами для предотвращения и пресечения киберугроз.

Все эти особенности и проблемы определения и регулирования цифровой информации и кибердеятельности обуславливают необходимость в рамках российского права рассматривать цифровую сферу и кибердеятельность как отдельную область права, человеческой деятельности и культуры, вплоть до пересмотра и дополнения в этой области определений как «информации», так и способов ее обработки, видов субъектов и т. д. Однако в то же время важно не терять связь с основополагающими правовыми принципами, традициями и ценностями, интегрируя эту новую область права в общую правовую и судебную систему.

Литература

1. Sidorenko E. Transformation of law in the context of digitalization: defining the correct priorities // Digital Law Journal. 2020
2. Kuzmin A. Digital technologies in the legal sphere // The Sociology of Law; 2022
3. Рузанова В. Природа нормативного массива в сфере информационных технологий и его место в системах российского права и законодательства (в аспекте процесса «цифровизации» права) // Studia Sieci Uniwersytetów Pogranicza; 2021
4. Talapina E. Digital law and digital rights in Russia: polemical notes // Legal Issues in the digital Age. 2021. № 1.
5. Laptev V. Digital information as an object of civil and commercial turnover at the present stage. // Государство и право. 2022.
6. Gavrilova Y. Legal Problems of Digital Technology Development in the Russian Federation // Legal Concept, 2022.
7. Kolontaevskaya I. Organizational and Legal Enforcement of Digital Economy in the Russian Federation at the Present Stage. 2021.
8. Pinkevich T. Security of digital technologies in the criminal legislation of the Russian Federation. // Vestnik of Kostroma State University. 2019
9. Bondarev A. V. The legal nature of digital technologies in public administration. // The rule-of-law state: theory and practice. 2023.
10. Романовская О. В. Право, информационное общество, цифровой суверенитет // Изв. Сарат. ун-та Нов. сер. Сер. Экономика. Управление. Право. 2024. № 2.
11. Polyakova T. A. Transformation of the science of Information Law and information legislation: a new stage in the conditions of scientific and technological development of Russia. // Государство и право. 2024.
12. Belikova K. M. The digital code of Russia: current state and prospects. // Economic problems and legal practice, 2024.
13. Polyakova T. Conceptual approaches to the legal regulation of information security in the conditions of digitalization and transformation of law. // Journal of the Ural Federal district Information security. 2019.
14. Гиреев. Д. Т. Теория государства и права. 2021.
15. Khasimova L. N. Digital Rights in Russia: Legal Regulation and Development Prospects. // Proceedings of the 2nd International Scientific and Practical Conference “Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth”, 2020.

16. Sidorenko, E. & Arzumanova, L. & Amvrosova, O. Adaptability and Flexibility of Law in the Context of Digitalization. 2021. 10.1007/978–3–030–53277–2_62.;
17. Полякова Т. А., Троян Н. А. Актуальные проблемы систематизации законодательства России под влиянием цифровых технологий в период цифровой трансформации // Вестник Университета имени О. Е. Кутафина. 2023. № 2 (102).

References

1. Sidorenko E. Transformation of law in the context of digitalization: defining the correct priorities. // Digital Law Journal. 2020.
2. Kuzmin A. Digital technologies in the legal sphere. // The Sociology of Law; 2022.
3. Ruzanova V. Priroda normativnogo massiva v sfere informacionnyh tehnologij i ego mesto v sistemah rossijskogo prava i zakonodatel'stva (v aspekte processa «cifrovizacii» prava). // Studia Sieci Uniwersytetów Pogranicza; 2021.
4. Talapina E. Digital law and digital rights in Russia: polemical notes // Legal Issues in the digital Age. 2021. № 1.
5. Laptev V. Digital information as an object of civil and commercial turnover at the present stage. // Государство и право. 2022.
6. Gavrilova Y. Legal Problems of Digital Technology Development in the Russian Federation. // Legal Concept, 2022.
7. Kolontaevskaya I. Organizational and Legal Enforcement of Digital Economy in the Russian Federation at the Present Stage. 2021.
8. Pinkevich T. Security of digital technologies in the criminal legislation of the Russian Federation. // Vestnik of Kostroma State University. 2019
9. Bondarev A. V. The legal nature of digital technologies in public administration. // The rule-of-law state: theory and practice. 2023.
10. Romanovskaja O. V. Pravo, informacionnoe obshhestvo, cifrovoj suverenitet // Izv. Sarat. un-ta Nov. ser. Ser. Jekonomika. Upravlenie. Pravo. 2024. № 2.
11. Polyakova T. A. Transformation of the science of Information Law and information legislation: a new stage in the conditions of scientific and technological development of Russia. // Государство и право. 2024.
12. Belikova K. M. The digital code of Russia: current state and prospects. // Economic problems and legal practice, 2024.
13. Polyakova T. Conceptual approaches to the legal regulation of information security in the conditions of digitalization and transformation of law. // Journal of the Ural Federal district Information security. 2019.
14. Gireev. D. T. Teorija gosudarstva i prava. 2021.
15. Khasimova L. N. Digital Rights in Russia: Legal Regulation and Development Prospects. // Proceedings of the 2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth", 2020.
16. Sidorenko, E. & Arzumanova, L. & Amvrosova, O. Adaptability and Flexibility of Law in the Context of Digitalization. 2021. 10.1007/978–3–030–53277–2_62.
17. Poljakova T. A., Trojan N. A. Aktual'nye problemy sistematizacii zakonodatel'stva Rossii pod vlijaniem cifrovyh tehnologij v period cifrovoj transformacii // Vestnik Universiteta imeni O. E. Kutafina. 2023. № 2 (102).

Сведения об авторе

Евлоев Тамерлан Якубович — аспирант кафедры Организации судебной и прокурорско-следственной деятельности МГЮА им. О. Е. Кутафина (г. Москва, Российская Федерация). Электронная почта: vasil.andreev.97@internet.ru

Information about the author

Yevloyev Tamerlan Yakubovich — postgraduate student of the Department of Organisation of Judicial and Prosecutor-Investigative Activities of the Kutafin Moscow State Law Academy (Moscow, Russian Federation). E-mail: vasil.andreev.97@internet.ru

Конфликт интересов отсутствует.

There is no conflict of interest.

Дата поступления статьи / Received: 20.05.2025

Дата рецензирования / Received: 22.05.2025

Дата принятия к опубликованию / Accepted: 25.05.2025