УДК 342.9

К ВОПРОСУ О РАЗВИТИИ ВИДОВ ОТВЕТСТВЕННОСТИ ЗА ДЕЙСТВИЯ ФИЗИЧЕСКИХ И ЮРИДИЧЕСКИХ ЛИЦ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Дейнеко Алексей Геннадьевич[1],
канд. юрид. наук,
e-mail: adeineko@hse.ru,
[1]*Национальный исследовательский университет «Высшая школа экономики», г. Москва, Россия*

В исследовании рассматриваются нормативные положения, появившиеся в российском информационном законодательстве в последние годы и характеризующиеся особым кругом субъектов, оснований, источников и содержания мер юридической ответственности. Путем анализа таких нормативных положений выявлен новый подход к правовому регулированию, при котором учитывается экономическая и техническая природа киберпространства. Благодаря этому эффективность мер информационно-правовой ответственности оценивается нами как более высокая по сравнению с действием классических видов юридической ответственности в условиях трансграничного и анонимного киберпространства.

Наряду с применением органами публичной власти мер воздействия на субъектов информационных правоотношений, нами отмечена практика применения таких мер хозяйствующими субъектами, в частности, лицами, владеющими или управляющими цифровыми платформами. Это позволяет утверждать о возможности выделения категории договорной информационно-правовой ответственности.

Вместе с тем, несистематизированный круг субъектов отношений, складывающихся в киберпространстве, а также ряд других насущных проблем информационного права обуславливают отсутствие системности в порядке применения мер информационно-правовой ответственности. Это обстоятельство рассматривается нами как дополнительный аргумент в пользу кодификации информационного законодательства.

Ключевые слова: информационное право, информационно-правовая ответственность, информационные правонарушения, публичное право, цифровая трансформация, информационное общество, цифровые платформы

ON THE ISSUE OF THE DEVELOPMENT OF TYPES OF RESPONSIBILITY FOR THE ACTIONS OF INDIVIDUALS AND LEGAL ENTITIES IN THE INFORMATIONAL SPACE

Deineko A.G.[1],
Candidate of Legal Sciences,
e-mail: adeineko@hse.ru,
[1]*National Research University Higher School of Economics, Moscow, Russia*

The paper describes the normative provisions that have appeared in Russian information regulations in recent years and are characterized by a special range of subjects, grounds, sources and content of responsibility measures. The analysis of such regulatory frameworks made it possible to reveal a new approach to legal regulation, which takes into account the economic and technical nature of Cyberspace. Due to this, we assess the effectiveness of information and legal measures to be higher than that of classical types of legal responsibility in cross-border and anonymous cyberspace. Along with the application of measures by public authorities to influence information legal relations subjects, we have also noted the practice of business entities applying such measures, in particular, individuals who own or manage digital platforms. This allows us to establish the possibility of categorizing contractual information and legal responsibility.

At the same time, the wide range of subjects involved in relations developing in cyberspace, along with a number of other pressing issues in information law, contribute to inconsistencies in the application of information

and legal measures. We consider this circumstance as an additional argument in favor of the codification of information legislation.

Keywords: Information Law, Information Responsibility, Information Offenses, Public Law, Digital Transformation, Information Society, Digital Platforms

DOI 10.21777/2587-9472-2024-3-7-14

Актуальность исследования обусловлена тем обстоятельством, что стремительное развитие общественных отношений, связанных с повсеместным применением информационных технологий, сформировало практику принудительного воздействия на субъектов информационных отношений, которое может осуществляться как органами публичной власти, так и хозяйствующими субъектами, управляющими цифровыми платформами и иными интернет-ресурсами. По своим основаниям и содержанию данное принудительное воздействие не укладывается в традиционные категории ответственности, известные правовой науке.

В качестве **задач исследования** нами были определены: анализ взаимосвязи норм информационного законодательства с нормами иных отраслей, определяющих конкретные меры юридической ответственности за правонарушения в информационной сфере, исследование оснований возникновения и содержания мер информационно-правовой ответственности, выработка предложений по совершенствованию российского законодательства. Вопрос о самостоятельном характере информационно-правовой ответственности, ее соотношения с мерами предупредительного, пресекательного, восстановительного и обеспечительного характера остается дискуссионным в российской правовой науке, в связи с чем формат нашего исследования предполагает не окончательное разрешение дискуссии, а выработку дополнительных аргументов к ней.

В рамках исследования нами использовались общенаучные **методы** анализа и синтеза, дедукции и индукции, а также специальные юридические методы, такие как метод юридического толкования и сравнительно-правовой метод. Подчеркнем, что при написании данного исследования нами не использовались генеративные алгоритмы искусственного интеллекта или аналогичные им технологии, позволяющие генерировать псевдонаучный текст.

Основная часть

На протяжении большей части периода становления в нашей стране информационно-правовой науки вопрос о выделении информационно-правовой ответственности в качестве самостоятельного вида юридической ответственности по существу не ставился и не обсуждался. Данное понятие подменялось понятием ответственности за правонарушения в сфере информации, информационных технологий и защиты информации, закреплённым в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1] (далее – Закон об информации). Бланкетная норма ч. 1 ст. 17 Закона об информации, упоминает о четырёх видах ответственности: дисциплинарной, гражданско-правовой, административной и уголовной, каждый из которых подробно исследован в правовой науке [1].

Заметим, что авторы Закона об информации воздержались от упоминания пятого «классического» вида юридической ответственности – материальной, что на наш взгляд, не выглядит бесспорным. В аналогичных бланкетных нормах, например в законодательстве о природных лечебно-оздоровительных ресурсах, можно встретить все пять видов ответственности[2]. Остановимся на этом вопросе подробнее.

Как известно, трудовое законодательство устанавливает в качестве основания возникновения материальной ответственности работника перед работодателем причинение последнему прямого дей-

[1] Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 12 декабря 2023 г.) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Ст. 19 Федерального закона от 23 февраля 1995 г. № 26-ФЗ (ред. от 26 мая 2021 г.) «О природных лечебных ресурсах, лечебно-оздоровительных местностях и курортах» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

ствительного ущерба, под которым понимается «реальное уменьшение наличного имущества работодателя или ухудшение состояния указанного имущества»[3]. В силу того, что информация с 2006 года не является объектом гражданских прав в российском законодательстве, называть её имуществом в этом контексте было бы некорректно. Вместе с тем Трудовой кодекс Российской Федерации упоминает в качестве частного случая возложение на работника *полной* материальной ответственности за «разглашение сведений, составляющих охраняемую законом тайну»[4].

В десятках федеральных законов и подзаконных актов упоминается множество видов тайн, систематизировать которые непросто[5]. Так, заслуживает внимания классификация Д.В. Огородова, который предлагает выделять тайны публично-правового (военная, государственная и служебная тайны) и частноправового (личная, семейная, коммерческая и профессиональная тайны) характера [2, с. 10]. Но вне зависимости от специфики правовой природы названных тайн их содержание охватывается определением информации, как «сведений (сообщений, данных) независимо от формы их представления», закреплённым в тезаурусе Закона об информации[6].

Таким образом, любой случай несанкционированного разглашения информации, составляющей охраняемую законом тайну, является, по существу, информационным правонарушением. За такое информационное правонарушение может наступать материальная ответственность, например в случаях, когда действия работника, взаимодействующего с информационной системой работодателя, привели к нарушению режима конфиденциальности информации, содержащейся в системе. Основанием для определения объема ответственности работника в приведённом примере может служить размер административного штрафа, наложенного на работодателя уполномоченным органом власти за нарушение требований информационного законодательства, размер имущественной претензии третьего лица в связи с раскрытием их коммерческой тайны и иные данные.

Следовательно, закреплённый в ст. 17 Закона об информации перечень видов ответственности является неполным уже по той причине, что в нем не указана материальная ответственность работника. Перейдем далее к вопросу о том, имеются ли основания для выделения шестого вида юридической ответственности – информационно-правовой.

Рассматривая вопрос об основаниях выделения видов юридической ответственности, коллеги по Кафедре ЮНЕСКО по авторскому праву, смежным, культурным и информационным правам НИУ «Высшая школа экономики» пришли к выводу, что критериями такого выделения является специфика источника, оснований ответственности и содержания мер ответственности[7]. Наряду с указанными критериями, М.П. Авдеенкова предлагает также выделять виды ответственности, исходя из особого круга субъектов, совершающих правонарушения, и субъектов, уполномоченных на применение мер принудительного воздействия [3]. Проанализируем данные критерии подробнее.

Специфика источников информационно-правовой ответственности заключается в их неконсолидированности по сравнению с источниками, определяющими основания других видов юридической ответственности. Данный признак роднит информационно-правовую ответственность с конституционно-правовой. Кодификация информационного законодательства, необходимость которой, на наш взгляд, давно назрела, помогла бы систематизировать перечень мер, основания и порядок привлечения к информационно-правовой ответственности. В пользу такой кодификации неоднократно высказывались видные отечественные правоведы [4].

---

[3] Ст. 238 Трудового кодекса Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (ред. от 6 апреля 2024 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[4] П. 7 ст. 243 Трудового кодекса Российской Федерации.

[5] Ст. 5 Закона Российской Федерации от 21 июля 1993 г. № 5485-1 (ред. от 4 августа 2023 г., с изм. и доп., вступ. в силу с 1 февраля 2024 г.) «О государственной тайне»; ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 (ред. от 12 декабря 2023 г., с изм и доп., вступ. в силу с 1 мая 2024 г.) «О банках и банковской деятельности»; ст. 102 Налогового кодекса Российской Федерации (части первой) от 31 июля 1998 г. № 146-ФЗ (ред. от 23 марта 2024 г.); ст. 13 Федерального закона от 21 ноября 2011 г. № 323-ФЗ (ред. от 25 декабря 2023 г., с изм. и доп., вступ. в силу с 1 апреля 2024 г.) «Об основах охраны здоровья граждан Российской Федерации»; ст. 8 Федерального закона от 31 мая 2002 г. № 63-ФЗ (ред. от 22 апреля 2024 г.) «Об адвокатской деятельности и адвокатуре в Российской Федерации» и мн. др.

[6] Ст. 2 Закона об информации.

[7] Информационное право: учебник и практикум для вузов / М.А.Федотов [и др.]; под ред. М.А. Федотова. – 2-е изд., перераб. и доп. – Москва: Юрайт, 2023. – С. 711.

В отсутствие кодифицированного акта «квазикодекс» в виде Закона об информации ограничивается бланкетной нормой, а наиболее полный перечень мер ответственности содержится в Федеральном законе от 1 июля 2021 г. № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети “Интернет” на территории Российской Федерации» (далее – Закон о приземлении)[8].

Логика таких мер ответственности проста: если государство не в состоянии «дотянуться» до владельцев или администраторов интернет-ресурсов, распространяющих запрещенную или вредную информацию и находящихся за пределами российской юрисдикции, то эффективной мерой воздействия в такой ситуации будет контроль за локализованными в национальной юрисдикции рекламодателями, кредитными организациями и операторами связи. Лишение или существенное сокращение источников финансирования деятельности таких интернет-ресурсов значительно уменьшит их стимулы к продолжению работы в российском сегменте киберпространства. Это впрочем, не касается деятельности интернет-ресурсов, которые изначально создаются с целью распространения соответствующей информации и уходят от ответственности, пользуясь системным характером проблемы юрисдикции в киберпространстве [5].

В числе мер ответственности, упомянутых в Законе о приземлении, которые вряд ли возможно отнести к одному из пяти «классических» видов юридической ответственности, можно отнести:

1) полную или частичную блокировку либо замедление скорости доступа к информационным ресурсам, распространяющим запрещённую или недостоверную информацию;

2) запрет на размещение рекламы на таких ресурсах или рекламы таких ресурсов на сторонних интернет-сайтах;

3) ограничение осуществления переводов денежных средств в пользу юридического лица, администрирующего такой ресурс;

4) запрет на поисковую выдачу информации о таких ресурсах в поисковых системах, либо предупредительная надпись (баннер) рядом со ссылкой на такой ресурс в результатах поисковой выдачи;

5) ограничение сбора и трансграничной передачи персональных данных такими ресурсами.

Первая из указанных мер появилась в российском законодательстве задолго до Закона о приземлении, первоначально она применялась и продолжает применяться в законодательстве о противодействии нарушениям интеллектуальных прав. В наших исследованиях проблемы «цифрового пиратства» мы неоднократно указывали на невысокую эффективность метода блокировок [6]. Во-первых, технические меры по блокировке доступа к информационным ресурсам легко нивелируются современными технологиями, позволяющими видоизменить или скрыть IP-адрес пользователя и обойти блокировку. Во-вторых, «побочным эффектом» применения таких мер является ограничение доступа к добросовестным интернет-ресурсам, которые используют «плавающие» (изменчивые) IP-адреса, или же IP-адреса, которые находятся в одной ветке с заблокированным.

Поправки к Закону об информации 2017 года установили запрет на использование программного обеспечения, позволяющего пользователям скрывать или изменять свои IP-адреса, если при этом они посещают заблокированные интернет-ресурсы. Примечательно, что ответственность за нарушение законодательства была возложена не на пользователей, а на владельцев информационно-телекоммуникационных сетей (в т.ч., VPN-сетей) и интернет-ресурсов. При этом сокрытие или изменение IP-адресов в иных целях (например, для обеспечения безопасности военкоров, работающих в зоне боевых действий) по-прежнему допускается законом.

Значимые изменения в алгоритме блокировок произошли в 2019 году, когда поправками к Закону об информации и Федеральному закону от 7 июля 2003 г. № 126-ФЗ «О связи» на собственников или владельцев линий связи, пересекающих географическую границу Российской Федерации, была возложена обязанность информировать уполномоченный орган публичной власти (Роскомнадзор) о целях использования оборудования (для формирования реестра точек обмена трафиком), а также установить в своих сетях «технические устройства, обеспечивающие автоматизированную блокировку запрещённых ресурсов и выявление источников происхождения интернет-траффика»[9].

---

[8] Федеральный закон от 1 июля 2021 г. № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети “Интернет” на территории Российской Федерации» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[9] Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон “О связи” и Федеральный закон “Об информации, информационных технологиях и о защите информации”» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

Таким образом, если ранее провайдеры стационарной и мобильной связи должны были самостоятельно обеспечивать блокировку запрещённых в нашей стране ресурсов, получая соответствующие предписания Роскомнадзора (пусть и в виде электронных документов), то теперь такие блокировки реализуются самим Роскомнадзором в автоматизированном режиме. В данном случае можно утверждать о технико-юридическом механизме реализации меры информационно-правовой ответственности. Вместе с тем практика «замедления» популярного зарубежного видеохостинга в 2024 году продемонстрировала, что на высоко конкурентном рынке интернет-услуг хозяйствующие субъекты нередко сами оказываются заинтересованными в предоставлении пользователям качественного доступа к замедляемым ресурсам (например, путем маскировки трафика в собственных сетях).

Наряду с такими «государственными» блокировками широко практикуются блокировки, осуществляемые владельцами цифровых платформ (социальных сетей, экосистем, маркетплейсов, метавселенных и др.) в отношении отдельных пользовательских аккаунтов в случае нарушения пользователями правил использования цифровых платформ. Несмотря на то, что зарегистрировать новый аккаунт в социальной сети обычно не составляет труда, в отдельных случаях такая мера показывает высокую эффективность. В качестве примера можно привести цифровые платформы краткосрочной аренды средств индивидуальной мобильности или автомобилей (кикшеринга или каршеринга), блокирующие доступ пользователей к аренде транспортных средств, если они систематически или грубо нарушают правила дорожного движения. Пользовательские аккаунты на таких цифровых платформах привязаны к документам, удостоверяющим личность, и банковским картам, поэтому их замена в целях преодоления блокировки сопряжена с известными трудностями.

Такую ответственность можно именовать договорной информационно-правовой ответственностью, поскольку источником применения мер принудительного воздействия является не нормативный правовой акт, а договор, заключаемый пользователем с собственником транспортных средств при помощи соответствующей цифровой платформы. Обычно такие договоры облекаются в форму лицензионного соглашения (определяющего порядок пользования платформой, как объектом интеллектуальной собственности), различного рода условий сервиса (*ToS, Terms of Service*) и условий использования (*ToU, Terms of Use*).

Таким образом, важным условием эффективности применения меры юридической ответственности в виде блокировки является сочетание собственно юридических и технических мер. Другим способом обеспечить эффективность привлечения к информационно-правовой ответственности является сочетание юридического и экономического воздействия.

Специфика экономической природы киберпространства заключается в том, что внимание пользователей становится главным ресурсом, за который конкурируют интернет-ресурсы. Повышенное внимание к ресурсу позволяет его владельцу генерировать высокие рекламные доходы. В числе таких «экономико-правовых» мер – запрет рекламораспространителям заключать контракты на размещение рекламы на информационных ресурсах, нарушающих требования законодательства. Впервые подобный механизм был апробирован в 2018 году в Меморандуме стран Европейского Союза применительно к интернет-ресурсам, неправомерно распространяющим объекты авторских и смежных прав[10]. При этом, обязательство рекламодателей не распространять рекламу на «пиратских» интернет-ресурсах не имело обратной силы, сохраняя действие ранее заключенных рекламных договоров. В 2020 году к указанному Меморандуму присоединилась и наша страна в лице Роскомнадзора[11].

Третья мера ответственности также характеризуется экономико-правовой природой, но при этом реализуется через систему государственного финансового контроля. В соответствии со ст. 14 Закона о приземлении, обязанность по ограничению денежных переводов в пользу юридического лица, администрирующего интернет-ресурс и нарушающего российское законодательство, возлагается на кредитные организации и операторов связи, а общий контроль за исполнением ими такой обязанности осуществляет Банк России. Как мы отмечали выше, данные субъекты локализованы в российской юрисдикции, что существенно облегчает органам публичной власти взаимодействие с ними.

---

[10] Memorandum of Understanding on Online Advertising and Intellectual Property Rights, Jun 25, 2018 [Электронный ресурс]. – URL: https://ec.europa.eu/docsroom/documents/30226 (дата обращения: 10.06.2024 г.).

[11] Официальный сайт Роскомнадзора [Электронный ресурс]. – URL: https://rkn.gov.ru/news/rsoc/news73070.htm (дата обращения: 10.06.2024 г.).

Четвертая из названных мер ответственности преследует целью, с одной стороны, обеспечение ограничения доступа российских пользователей к недостоверной или запрещённой информации (в случае запрета на поисковую выдачу), а с другой – также и их информирование о том, что определённый интернет-ресурс функционирует с нарушениями российского законодательства. Так, с 2022 года некоторые результаты поисковой выдачи поисковых систем по запросам на общественно-политические темы содержат уведомление вида «*РКН: сайт нарушает законы РФ*».

Операторы поисковых систем обязаны размещать такие уведомления в течение суток с момента получения соответствующего решения Роскомнадзора[12]. В этой ситуации оператор поисковой системы выступает в роли информационного посредника (не в частноправовом, а в публично-правовом смысле) и с большой долей вероятности выполнит предписание органа публичной власти. Данная мера воздействия, на наш взгляд, обладает и косвенным экономическим эффектом, поскольку некоторая доля пользователей, увидев такое уведомление в результатах поисковой выдачи, возможно, примет решение не переходить на такие интернет-ресурсы, в результате чего их показатели посещаемости несколько снизятся.

Наконец, в пятой из перечисленных мер информационно-правовой ответственности обязанность реализации ограничений по сбору и использованию персональных данных пользователей возлагается на сами интернет-ресурсы, а также на широкий круг участников общественных отношений по обороту персональных данных, включая органы публичной власти и коммерческие организации[13]. Данная мера ответственности представляется нам наименее проработанной на данном этапе в связи с тем, что персональные данные составляют значительную часть оборота данных в киберпространстве и обладают высокой ценностью. Как отмечает Э.В. Талапина, проблема защиты размещенных в киберпространстве персональных данных сохраняет свою актуальность даже после смерти гражданина, являющегося их носителем [7, с. 126].

Что же касается критерия субъектов, подлежащих привлечению к такой ответственности, и субъектов, уполномоченных привлекать к такой ответственности, то их круг чрезвычайно широк, и вместе с тем, не систематизирован. В 2023 году мы опубликовали исследование механизмов функционирования публично-правовых норм в киберпространстве, где отметили, что в роли субъектов общественных отношений, складывающихся в киберпространстве, выступает широкий круг лиц, относящихся к частному и публичному праву, многие из которых до сих пор не получили своего легального определения [8]. Эта особенность не позволяет предложить для информационно-правовой ответственности путь включения в уже существующие виды ответственности, который прошла, например, ответственность за нарушения таможенного законодательства, «растворившись» в уголовном и административном законодательстве.

Применение государством мер информационно-правовой ответственности требует поддержания надлежащего уровня безопасности критической информационной инфраструктуры. Ещё в 2000 году Ю.А. Нисневич предупреждал, что широкое заимствование зарубежного программного обеспечения (и шире – информационных технологий) приведет к тому, что «национальный научно-технический потенциал нашей страны резко сократится, фундаментальные и прикладные научные исследования, проектные и опытно-конструкторские работы будут проводиться в минимальных объемах, а производственный потенциал переключится на внедрение и сопровождение технических систем и средств зарубежного производства» [9, с. 78].

Для того чтобы избежать указанных последствий необходима реализация комплекса мер, направленных на создание «цифрового суверенитета» государства [10]. На решение данной задачи направлены принятые в 2018–2019 годах федеральные законы, установившие требования к безопасности информационных систем, относящихся к критической информационной инфраструктуре, и обусловившие создание национальной системы доменных имён (НСДИ)[14]. Можно констатировать, что реализация указанных актов не привела к изоляции российского сегмента киберпространства, падению скорости передачи данных или иным неблагоприятным последствиям. Органами публичной власти,

[12] П. 2 ст. 11 Закона о приземлении.

[13] Ст. 16 Закона о приземлении.

[14] Федеральные законы от 26 июля 2017 г. № 187-ФЗ (ред. от 10 июля 2023 г.) «О безопасности критической информационной инфраструктуры Российской Федерации»; от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон “О связи” и Федеральный закон “Об информации, информационных технологиях и о защите информации”» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

ответственными за реализацию правовых новелл, по всей видимости, был учтен как положительный, так и отрицательный опыт построения аналогичной суверенной инфраструктуры доступа к киберпространству в зарубежных странах, прежде всего, в Китае [11].

Заключение

Проведенный анализ позволяет нам сделать вывод о том, что уголовная, гражданская и иная ответственность за информационные правонарушения не тождественна информационно-правовой ответственности, рассмотренной в данной статье. Рассмотренные меры имеют ярко выраженную специфику источника, оснований, содержания и субъектов ответственности, что позволяет отграничить их от других известных правовой науке видов юридической ответственности. В то же время, эти меры нуждаются в систематизации, которая может быть обеспечена путем кодификации информационного законодательства. Принятие информационного кодекса позволит зафиксировать самостоятельный характер информационно-правовой ответственности и увязать ее с кругом субъектов информационных правоотношений.

Практическая реализация проанализированных в исследовании мер ответственности не лишена недостатков, но уже сейчас можно положительно оценить подход законодателя, который учёл при проектировании правовых норм трансграничную природу киберпространства, а также экономическую основу складывающихся в нем общественных отношений.

Список литературы

1. *Кузьмин И.А.* Система юридической ответственности, как объект научных исследований // Государство и право. – 2018. – № 10. – С. 61–70.
2. *Огородов Д.В.* Правовые отношения в информационной сфере: автореф. дис. ... канд. юрид. наук 12.00.14. – Москва: Институт государства и права РАН, 2002.
3. *Авдеенкова М.П.* Элементы системы юридической ответственности и особенности их взаимодействия // Современное право. – 2008. – № 5. – С. 44–49.
4. *Полякова Т.А, Минбалеев А.В., Наумов В.Б.* К вопросу о кодификации информационного законодательства в условиях цифровой трансформации общества // Государство и право. – 2024. – № 1. – С. 81–91. – DOI: 10.31857/S1026945224010087.
5. *Kohl U.* Jurisdiction in Cyberspace: Research Handbook on International Law and Cyberspace – Cheltenham, 2015.
6. *Дейнеко А.Г.* Авторское право в киберпространстве: монография. – Москва: Юрлитинформ, 2017. – 152 с.
7. *Талапина Э.В.* Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды Института государства и права РАН. – 2018. – Т. 13, № 5. – С. 117–150.
8. *Дейнеко А.Г.* Публичное право в киберпространстве (публично-правовое регулирование информационных отношений): монография. – Москва: Проспект, 2023. – 248 с.
9. *Нисневич Ю.А.* Информация и власть. – Москва: Мысль, 2000.
10. *Duarte M.* Network Sovereignty: Building the Internet Across Indian Country. – Seattle, WA: University of Washington Press, 2017.
11. *Трощинский П.В., Молотников А.Е.* Особенности нормативно-правового регулирования цифровой экономики и цифровых технологий в Китае // Правоведение. – 2019. – Т. 63, № 2. – С. 309–326.

References

1. *Kuz'min I.A.* Sistema yuridicheskoj otvetstvennosti, kak ob"ekt nauchnyh issledovanij // Gosudarstvo i pravo. – 2018. – № 10. – S. 61–70.
2. *Ogorodov D.V.* Pravovye otnosheniya v informacionnoj sfere: avtoref. dis. ... kand. yurid. nauk 12.00.14. – Moskva: Institut gosudarstva i prava RAN, 2002.
3. *Avdeenkova M.P.* Elementy sistemy yuridicheskoj otvetstvennosti i osobennosti ih vzaimodejstviya // Sovremennoe pravo. – 2008. – № 5. – S. 44–49.

4. *Polyakova T.A, Minbaleev A.V., Naumov V.B.* K voprosu o kodifikacii informacionnogo zakonodatel'stva v usloviyah cifrovoj transformacii obshchestva // Gosudarstvo i pravo. – 2024. – № 1. – S. 81–91. – DOI: 10.31857/S1026945224010087.
5. *Kohl U.* Jurisdiction in Cyberspace: Research Handbook on International Law and Cyberspace – Cheltenham, 2015.
6. *Dejneko A.G.* Avtorskoe pravo v kiberprostranstve: monografiya. – Moskva: Yurlitinform, 2017. – 152 s.
7. *Talapina E.V.* Zashchita personal'nyh dannyh v cifrovuyu epohu: rossijskoe pravo v evropejskom kontekste // Trudy Instituta gosudarstva i prava RAN. – 2018. – T. 13, № 5. – S. 117–150.
8. *Dejneko A.G.* Publichnoe pravo v kiberprostranstve (publichno-pravovoe regulirovanie informacionnyh otnoshenij): monografiya. – Moskva: Prospekt, 2023. – 248 s.
9. *Nisnevich Yu.A.* Informaciya i vlast'. – Moskva: Mysl', 2000.
10. *Duarte M.* Network Sovereignty: Building the Internet Across Indian Country. – Seattle, WA: University of Washington Press, 2017.
11. *Troshchinskij P.V., Molotnikov A.E.* Osobennosti normativno-pravovogo regulirovaniya cifrovoj ekonomiki i cifrovyh tekhnologij v Kitae // Pravovedenie. – 2019. – T. 63, № 2. – S. 309–326.