

Научная статья  
УДК 342.951

## Государственно-частное партнерство в отношении объектов информационной инфраструктуры: административно-правовое исследование

Руслан Михайлович Ушаков

Юридический институт Российского университета дружбы народов имени Патриса Лумумбы  
Москва (117198, ул. Миклухо-Маклая, д. 6), Российская Федерация  
ru.ushushakov@yandex.ru  
<https://orcid.org/0000-0001-8090-4920>

### Аннотация:

**Введение.** В статье сквозь призму административного права рассматриваются актуальные проблемы и несовершенства отечественной нормативной конструкции государственно-частного (муниципально-частного) партнерства применительно к информационной инфраструктуре.

**Методы.** Методологию исследования образуют общенаучные методы (анализ, синтез, сравнение, индукция, дедукция), а также частнонаучные юридические методы (формально-юридический, метод юридической герменевтики).

**Результаты.** Установлено и обосновано, что административно-правовое регулирование государственно-частного (муниципально-частного) партнерства в отношении объектов информационной инфраструктуры характеризуется наличием несовершенств, обусловленных специфическим объектом регулирования. Их преодоление предполагает комплексный подход, включающий: 1) совершенствование законодательства о государственно-частном (муниципально-частном) партнерстве применительно к объектам информационной инфраструктуры в аспекте углубления легальных характеристик, дифференцирующих информацию, осуществление монетизации которой дозволено / не дозволено в процессе реализации проекта, 2) пересмотр положений, запрещающих участие иностранных лиц через подконтрольных им российских юридических лиц в проектах государственно-частного (муниципально-частного) партнерства, реализуемых в отношении объектов информационной инфраструктуры: следует законодательно разделить проекты на те, в которых «прокси-участие» иностранных субъектов невозможно (проекты с государственной тайной, в сфере обороны, национальной безопасности, в отношении объектов двойного назначения, критической информационной инфраструктуры) и остальные проекты, в которых их участие возможно в рамках создания подконтрольных российских юридических лиц, 3) установление обязательной предварительной экспертизы проектов в отношении объектов информационной инфраструктуры на соответствие требованиям технической и информационной безопасности, 4) конкретизацию в законодательстве действий публичного партнера по содействию в получении не только разрешений и согласований органов публичной власти, но и других видов организационной помощи, адресованной частному партнеру, 5) адаптацию оценки эффективности и сравнительного преимущества проектов с учетом специфики информационных технологий, и другие меры.

### Ключевые слова:

государственно-частное партнерство, муниципально-частное партнерство, информационные технологии, информационная инфраструктура, административно-правовое регулирование, государственное управление

### Для цитирования:

Ушаков Р. М. Государственно-частное партнерство в отношении объектов информационной инфраструктуры: административно-правовое исследование // Вестник Санкт-Петербургского университета МВД России. 2026. № 1 (109). С. 68–79.

Статья поступила в редакцию 22.10.2025;  
одобрена после рецензирования 12.12.2025;  
принята к публикации 20.03.2026.

Original article

## Public-private partnership in information infrastructure: an administrative law study

Ruslan M. Ushakov

Law Institute of the Peoples' Friendship University of Russia named after Patrice Lumumba  
6, Miklouho-Maklaya str., Moscow, 117198, Russian Federation  
ru.ushushakov@yandex.ru  
<https://orcid.org/0000-0001-8090-4920>

© Ушаков Р. М., 2026



**Abstract:**

**Introduction.** From an administrative law perspective this article analyses current challenges and shortcomings in the national regulatory framework governing public-private partnership (PPP) (municipal-private partnership (MPP)) in the field of information infrastructure.

**Methods.** The methodological framework of the study comprised general scientific methods (analysis, synthesis, comparison, induction, deduction) as well as specific legal methods (the formal-legal method and legal hermeneutics).

**Results.** The study finds and substantiates that the administrative-legal regulation of PPP/MPP for information infrastructure is marked by deficiencies stemming from the unique nature of its subject. Addressing these issues necessitates a comprehensive strategy, which includes the following measures: 1. Enhance PPP/MPP legislation for information infrastructure by establishing clear legal criteria to distinguish between monetisable and non-monetisable project data. 2. Amend restrictions on foreign "proxy participation" via controlled Russian entities, creating a legal distinction between prohibited sectors (state secrets, defense, national security, dual-use technologies, critical infrastructure) and permitted ones. 3. Introduce mandatory preliminary security expertise for information infrastructure projects to ensure compliance with technical and information safety standards. 4. Legally specify the public partner's duty to assist with not only permits and approvals but also broader organisational support. 5. Adapt project evaluation methodologies (efficiency, value-for-money) to the specificities of information technologies.

**Keywords:**

public-private partnership, municipal-private partnership, information technology, information infrastructure, administrative-legal regulation, public administration

**For citation:**

Ushakov R. M. Public-private partnership in information infrastructure: an administrative law study // Vestnik of Saint Petersburg University of the MIA of Russia. 2026. № 1 (109). P. 68–79.

The article was submitted October 22, 2025; approved after reviewing December 12, 2025; accepted for publication March 20, 2026.

## Введение

Согласно данным Аналитического центра при Правительстве Российской Федерации в стране повышается роль ИТ-отрасли в развитии экономики и общества, вклад которой в валовой внутренний продукт (далее – ВВП) России по валовой добавленной стоимости составляет 6 %<sup>1</sup>. Функционирование инфраструктуры транспорта, жилищно-коммунального хозяйства (далее – ЖКХ), здравоохранения, образования, культуры, в т. ч. при осуществлении функций органов публичной власти, все более зависит от внедрения новых технологий. В этой связи актуальность информационных технологий (далее – ИТ) для применения государственно-частного партнерства также возрастает, что проявляется в положениях документов стратегического планирования, определяющих потребности государства в реализации проектов по созданию информационной инфраструктуры.

Во-первых, в рамках Указа Президента Российской Федерации от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»<sup>2</sup> увеличение к 2030 году до 99 % доли предоставления массовых социально значимых государственных и муниципальных услуг в электронной форме и обеспечение в 2025–2030 гг. темпа роста инвестиций в отечественные решения в сфере ИТ вдвое выше темпа роста ВВП определено в качестве целевых показателей и задач, выполнение которых характеризует достижение национальной цели «Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы».

Во-вторых, согласно прогнозу долгосрочного социально-экономического развития Российской Федерации на период до 2030 года<sup>3</sup> переход на формирование рынков программных продуктов и предоставления услуг будет основной тенденцией развития ИТ; при активизации предпринимательской деятельности, росте доходов населения, ускорении промышленного производства ожидается повышение темпов развития ИТ, объем рынка которых увеличится в 3,7 раза по сравнению с 2011 годом.

В-третьих, Стратегия пространственного развития Российской Федерации на период до 2030 года с прогнозом до 2036 года<sup>4</sup> определяет, что планирование развития информационно-

<sup>1</sup> Вклад ИТ-отрасли в экономику России составил 6 % // Аналитический центр при Правительстве Российской Федерации : [сайт]. URL: <https://ac.gov.ru/news/page/vklad-it-otrasli-v-ekonomiku-rossii-sostavil-6-28110> (дата обращения: 20.09.2025).

<sup>2</sup> О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года : Указ Президента Российской Федерации от 7 мая 2024 г. № 309 // Собрание законодательства Российской Федерации (далее – СЗ РФ). 2024. № 20. Ст. 2584.

<sup>3</sup> Прогноз долгосрочного социально-экономического развития Российской Федерации на период до 2030 года // Правительство Российской Федерации : [официальный сайт]. URL: <http://static.government.ru/media/files/41d457592e04b76338b7.pdf> (дата обращения: 20.09.2025).

<sup>4</sup> Об утверждении Стратегии пространственного развития Российской Федерации на период до 2030 года с прогнозом до 2036 года : распоряжение Правительства Российской Федерации от 28 декабря 2024 г. № 4146-р // СЗ РФ. 2025. № 2. Ст. 74.

телекоммуникационной инфраструктуры (далее – ИТИ) и отрасли связи ориентируется на устранение цифрового неравенства субъектов Российской Федерации, обеспечение опережающего развития ИТИ и снятие инфраструктурных ограничений в целях ускоренного развития цифровых технологий, создание конкурентоспособной ИТИ на основе отечественных разработок.

В-четвертых, в Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг.<sup>5</sup> указано, что:

а) главным способом обеспечения эффективности цифровой экономики становится внедрение технологии обработки данных, что позволит уменьшить затраты при производстве товаров и оказании услуг;

б) основными задачами применения информационных и коммуникационных технологий для развития социальной сферы, системы государственного управления, взаимодействия граждан и государства являются, в т. ч., применение в органах государственной власти Российской Федерации новых технологий, обеспечивающих повышение качества государственного управления;

в) существенная роль отводится использованию инфраструктуры электронного правительства для оказания государственных и востребованных гражданами коммерческих и некоммерческих услуг, сокращению административной нагрузки на субъекты хозяйственной деятельности вследствие использования соответствующих технологий при проведении проверок органами контроля (надзора);

г) необходимо развивать центры обработки данных (далее – ЦОД), технические средства по обработке данных на территории Российской Федерации на основе отечественного программного обеспечения и оборудования;

д) в рамках приоритетного сценария совершенствуются законодательство Российской Федерации и административные процедуры, привлекаются частные инвестиции в информационную инфраструктуру;

е) реализация стратегии обеспечивается согласованными действиями органов власти и организаций, в рамках нее российские фонды, институты развития, государственные корпорации, компании с государственным участием и частные компании осуществляют инвестиции в сферу информационных и коммуникационных технологий.

В-пятых, с 2025 года реализуется национальный проект «Экономика данных и цифровая трансформация государства» (2025–2030 гг.), призванный повысить качество жизни граждан и эффективность ключевых отраслей социальной сферы, государственного и муниципального управления, сфер российской экономики, включая развитие инфраструктуры электронного правительства, внедрение искусственного интеллекта и др.<sup>6</sup>

Таким образом, в условиях недостаточности бюджетных средств привлечение инвестиций в сферу ИТ через механизмы государственно-частного партнерства (далее – ГЧП), муниципально-частного партнерства (далее – МЧП) является востребованным, что основано на приоритетах государства по ее развитию. Изложенное может быть реализовано в целях улучшения государственного и муниципального управления посредством внедрения новых технологий в деятельность органов публичной власти, публичных учреждений и предприятий, иных организаций публичной сферы, в функционирование публичного сектора экономики. Это могут быть, например, государственные информационные системы (далее – ГИС), аккумулирующие информацию для населения в различных социально значимых сферах (образование, здравоохранение, спорт) и обеспечивающие предоставление государственных и муниципальных услуг в электронной форме<sup>7</sup>, в т. ч. в рамках системы электронного правительства, информационные системы «Умный город», «Безопасный город», информационные решения по цифровизации и автоматизации транспорта (системы, видео- и фотофиксации нарушений правил дорожного движения, автоматизированные системы управления транспортом), ЖКХ (интеллектуальные системы ресурсосбережения и учета, автоматизации процессов в сфере переработки твердых коммунальных отходов), товарооборота отдельной продукции и др., т. е. направления, которые имеют высокую публичную значимость и могут быть делегированы для реализации частному партнеру. Преимущества применения ГЧП (МЧП) в сфере ИТ раскрываются в полной мере: частный партнер не только создает, но и осуществляет эксплуатацию и техническое обслуживание

<sup>5</sup> О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ Президента Российской Федерации от 9 мая 2017 г. № 203 // СЗ РФ. 2017. № 20. Ст. 2901.

<sup>6</sup> Национальный проект «Экономика данных и цифровая трансформация государства» // Правительство Российской Федерации : [официальный сайт]. URL: <https://digital.gov.ru/target/nacziionalnyj-proekt-ekonomika-dannyh-i-cifrovaya-transformacziya-gosudarstva> (дата обращения: 20.09.2025).

<sup>7</sup> Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме : постановление Правительства Российской Федерации от 8 июня 2011 г. № 451 (в ред. от 04.08.2025) // СЗ РФ. 2011. № 24. Ст. 3503.

информационной инфраструктуры на длительный срок, реализуя технические компетенции, а также софинансирует проект, разделяя риски, что выгодно для публичного партнера.

## Методы

Методологию исследования составляют общенаучные методы (анализ, синтез, сравнение, индукция, дедукция), а также частнонаучные юридические методы (формально-юридический и метод юридической герменевтики). Применение общенаучных методов позволяет определить содержание основных научных категорий, используемых в исследовании, выявить логику законодателя и основные тенденции административно-правового регулирования ГЧП (МЧП) в отношении объектов информационной инфраструктуры. Формально-юридический метод используется при анализе административно-правовых норм, отраженных в законодательстве о ГЧП (МЧП), а также в смежной и отраслевой нормативно-правовой базе. Метод юридической герменевтики реализуется в процессе авторского толкования указанного законодательства.

## Результаты

Комплекс объектов информационной инфраструктуры соглашений о государственно-частном партнерстве (далее – СГЧП) и о муниципально-частном партнерстве (далее – СМЧП) был введен в Федеральный закон от 13 июля 2015 г. № 224-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации»<sup>8</sup> (далее – ФЗ «О ГЧП») в 2018 году<sup>9</sup>. Как следует из п. 19 ч. 1 ст. 7 данного закона, к объектам СГЧП (СМЧП) относятся:

- 1) программы для ЭВМ;
- 2) базы данных;
- 3) информационные системы и (или);
- 4) сайты в сети «Интернет» или других информационно-телекоммуникационных сетях, в состав которых входят такие программы для ЭВМ и (или) базы данных, либо совокупность указанных объектов (объекты ИТ);
- 5) объекты ИТ и имущество, технологически связанное с одним или несколькими такими объектами и предназначенное для обеспечения их функционирования или осуществления иной деятельности, предусмотренной соглашением (технические средства обеспечения функционирования объектов ИТ)<sup>10</sup>.

Согласно пункту 20 ч. 1 ст. 7 указанного закона в качестве объектов соглашений также закреплены центры обработки данных (далее – ЦОД), с 1 марта 2026 г. определяемые в новой редакции как совокупность зданий, частей зданий или помещений, объединенных единым назначением, включающих комплекс систем инженерно-технического обеспечения, спроектированных и используемых для размещения оборудования, обеспечивающего обработку и (или) хранение данных<sup>11</sup>. Таким образом, существует три вида объектов информационной инфраструктуры СГЧП (СМЧП)<sup>12</sup>: объекты ИТ, объекты ИТ и технические средства обеспечения функционирования объектов ИТ, ЦОД.

Согласно данным цифровой платформы «Росинфра» по состоянию на август 2025 года на различных этапах реализации находились (находятся) 11 проектов<sup>13</sup> в отношении цифровой

<sup>8</sup> О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 13 июля 2015 г. № 224-ФЗ (ред. от 31.07.2025) // СЗ РФ. 2015. № 29 (ч. I). Ст. 4350.

<sup>9</sup> О внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 29 июня 2018 г. № 173-ФЗ // СЗ РФ. 2018. № 27. Ст. 3956.

<sup>10</sup> Программы для ЭВМ и базы данных являются интеллектуальной собственностью, что отличает их как объекты соглашений от иных объектов согласно ст. 7 Федерального закона от 13 июля 2015 г. № 224-ФЗ.

<sup>11</sup> О внесении изменений в статьи 2 и 6 Федерального закона «О связи» и отдельные законодательные акты Российской Федерации : Федеральный закон от 23 июля 2025 г. № 244-ФЗ // СЗ РФ. 2025. № 30 (ч. II). Ст. 4393.

<sup>12</sup> В отношении объектов ИТ, а также объектов ИТ и технических средств обеспечения функционирования объектов ИТ как объектов соглашений установлены особенности регулирования в рамках специальной главы Федерального закона от 13 июля 2015 г. № 224-ФЗ – 6.1. В данной главе определяются вопросы исключительных прав на результаты интеллектуальной деятельности, обязательные элементы соглашений, административные процедуры, в т. ч. замена частного партнера, решение о реализации проекта, которые зависят от вопросов принадлежности исключительных прав, и иные вопросы.

<sup>13</sup> Для методологической точности следует указать, что количество информационных проектов в рамках поиска по конкретным сферам (ЖКХ и др.) составляет большее число, однако их точный подсчет существенно осложнен в рамках возможностей платформы «Росинфра» и общего количества проектов.

инфраструктуры и связи в форме СГЧП (СМЧП), включая соглашения на основе регионального законодательства<sup>14</sup>. Тем самым практика реализации проектов в данной сфере активно формируется, в основном – это субъектовые цифровые информационные системы учета спортивных достижений<sup>15</sup> и цифровые образовательные платформы<sup>16</sup>. Например, проект по созданию и эксплуатации автоматизированной информационной системы «Цифровая образовательная платформа Ивановской области», публичным партнером в котором выступила Ивановская область в лице Департамента образования при общем объеме инвестиций 8 562 000 руб. и сроке соглашения 10 лет<sup>17</sup>. В качестве информации о проекте в «Росинфра» указано:

1) он направлен на повышение прозрачности образовательного процесса, эффективности взаимодействия участников образовательного сектора и качества оказания государственной услуги по предоставлению информации о текущей успеваемости обучающихся в формате электронного журнала и электронного дневника, эффективную информатизацию образовательного сектора региона посредством создания и развития соответствующей системы;

2) в регионах активно продвигаются типовые проекты: аналогичный проект реализован во многих субъектах Российской Федерации, включая Новгородскую область, Архангельскую область, Иркутскую область, Республику Дагестан и др.<sup>18</sup>

Таким образом, указанный проект, предназначенный для реализации функций органов исполнительной власти, является типовым, при этом в субъектах Российской Федерации выделяется две основные сферы для проектной деятельности в рамках информационных систем: образования и спорта. Данные проекты цифровизации социальной сферы, как правило, ориентированы на реализацию публичных услуг в электронном виде в рамках соответствующего распоряжения Правительства Российской Федерации<sup>19</sup>.

Уникальным и крупнейшим федеральным проектом в сфере ИТ является создание системы цифровой маркировки и прослеживания (мониторинга) оборота товаров<sup>20</sup>. Данный проект, не имеющий мировых аналогов, реализуется в рамках первого заключенного СГЧП в области ИТ, подписанного на Петербургском международном экономическом форуме на 15-летний срок при общих инвестициях Центра развития перспективных технологий (частный партнер) в проект около 220 млрд руб.<sup>21</sup> Создание и обеспечение функционирования данной системы, направленной на решение публичных задач, определено Федеральным законом от 28 декабря 2009 г. № 381-ФЗ «Об основах государственного регулирования торговой деятельности в Российской Федерации»<sup>22</sup>: ч. 1 ст. 20.1 предусматривает создание ГИС мониторинга за оборотом товаров, подлежащих обязательной маркировке средствами идентификации<sup>23</sup>. Распоряжением Правительства Российской Федерации о реализации проекта были:

а) утверждены существенные условия соглашения, заключаемого в целях создания, эксплуатации и технического обслуживания объекта, предназначенного для обеспечения маркировки и прослеживаемости отдельных видов товаров, и план-график соответствующих мероприятий;

<sup>14</sup> Росинфра : [сайт]. URL: <https://dpo.rosinfra.ru/base-projects/> (дата обращения: 30.09.2025).

<sup>15</sup> См., например: Создание, обеспечение функционирования, эксплуатация и техническое сопровождение автоматизированной информационной системы «Цифровая информационная система учета спортивных достижений Республики Саха (Якутия)» // Росинфра : [сайт]. URL: <https://dpo.rosinfra.ru/projects-office/12796/form/application> (дата обращения: 30.09.2025).

<sup>16</sup> См., например: СГЧП по созданию, обеспечению функционирования и технического сопровождения региональной информационной системы «Цифровая образовательная платформа Чеченской Республики» // Там же. URL: <https://dpo.rosinfra.ru/projects-office/12724/form/application> (дата обращения: 30.07.2025).

<sup>17</sup> См.: СГЧП в отношении автоматизированной информационной системы «Цифровая образовательная платформа Ивановской области» // Там же. URL: <https://dpo.rosinfra.ru/projects-office/7553/form/application> (дата обращения: 30.09.2025).

<sup>18</sup> URL: <https://dpo.rosinfra.ru/base-projects/> (дата обращения: 30.09.2025).

<sup>19</sup> Об утверждении Сводного перечня первоочередных государственных и муниципальных услуг, предоставляемых органами исполнительной власти субъектов Российской Федерации и органами местного самоуправления в электронном виде, а также услуг, предоставляемых в электронном виде учреждениями субъектов Российской Федерации и муниципальными учреждениями : распоряжение Правительства Российской Федерации от 17 декабря 2009 г. № 1993-р (в ред. от 28.12.2011) // СЗ РФ. 2009. № 52 (ч. II). Ст. 6626.

<sup>20</sup> Создание системы цифровой маркировки и прослеживания (мониторинга) оборота товаров // Росинфра : [сайт]. URL: <https://dpo.rosinfra.ru/projects-office/5916/form/application> (дата обращения: 30.09.2025).

<sup>21</sup> Первое в России соглашение о ГЧП в области ИТ подписано на ПМЭФ // Честный ЗНАК: Государственная система цифровой маркировки : [официальный сайт]. URL: [https://честныйзнак.рф/info/smi\\_o\\_nas/pervoe-v-rossii-soglashenie-o-gchp-v-oblasti-informatsionnykh-tehnologiy-podpisano-na-pmef/](https://честныйзнак.рф/info/smi_o_nas/pervoe-v-rossii-soglashenie-o-gchp-v-oblasti-informatsionnykh-tehnologiy-podpisano-na-pmef/) (дата обращения: 30.09.2025).

<sup>22</sup> Об основах государственного регулирования торговой деятельности в Российской Федерации : Федеральный закон от 28 декабря 2009 г. № 381-ФЗ (в ред. от 31.07.2025) // СЗ РФ. 2010. № 1. Ст. 2.

<sup>23</sup> На основе и во исполнение закона определяется в рамках актов Правительства Российской Федерации (См., например: О системе маркировки товаров средствами идентификации и прослеживаемости движения товаров : постановление Правительства Российской Федерации от 26 апреля 2019 г. № 515 (в ред. 29.09.2025) // СЗ РФ. 2019. № 19. Ст. 2279).

б) в качестве одной из целей реализации проекта установлено обеспечение получения оперативной и достоверной информации о движении товаров в рамках хозяйственной деятельности организаций;

в) определены полномочия публичного партнера, которые осуществляет от имени Российской Федерации Минпромторг России;

г) установлены отдельные права и обязанности публичного партнера, переданные Минкомсвязи России, Минсельхозу России, Минздраву России, ФНС России и др., выступающим на стороне публичного партнера, определены иные вопросы<sup>24</sup>.

Государственная система цифровой маркировки и прослеживаемости товаров имеет название «Честный знак», реализуется посредством присвоения товарам уникального кода, который используется для отслеживания перемещения товаров по всей логистической цепи и не позволяет реализовать контрафакт, проверка по данному коду доступна широкому кругу лиц, что обеспечивает прозрачность системы, при этом маркируется молочная продукция, упакованная вода, одежда, парфюмерная продукция и др.<sup>25</sup> Таким образом, данная система выступает значимым превентивным средством реализации правовой политики в сфере товарного оборота. Другим примером является федеральный проект, направленный на цифровизацию сферы ЖКХ (Федеральный цифровой сервис)<sup>26</sup>.

Таким образом, информационная инфраструктура прочно вошла в проектную практику ГЧП на федеральном и региональном уровнях. На уровне муниципалитетов, однако, изложенное не получило широкого распространения, что, полагаем, обусловлено ограниченностью финансов и компетенций партнеров, а также относительной недавним введением возможности заключения СМЧП в данной сфере (с 2022 года)<sup>27</sup>.

Существующие исследования, посвященные правовому анализу ГЧП (МЧП) в сфере ИТ, относительно малочисленны и, как правило, не являются административно-правовыми или системными, поскольку затрагивают отдельные аспекты темы [1; 2]. В науке справедливо указывается на высокую потребность в развитии инфраструктуры на основе ИТ [3, с. 201], выделяется низкий уровень развития базовой региональной телекоммуникационной инфраструктуры [4, с. 293], определяются роли ГЧП в условиях цифровизации экономики, а именно: помощь в привлечении частных инвестиций для разработки и внедрения цифровых инфраструктур; цифровые навыки и образование; цифровые услуги; содействие инновациям и стартапам; разработка регулирования и защиты прав потребителей [5, с. 319–320], исследуются роль ГЧП в цифровизации государственного управления [6, с. 201], особенности распределения исключительных прав [7], указывается на несовершенство законодательства о ГЧП в сфере ИТ [8, с. 153], исследуются иные аспекты [9–14]. Анализ административно-правового регулирования ГЧП (МЧП) предполагает сосредоточение внимания на вопросах компетенции органов публичной власти, административных процедурах, формах государственного контроля, административной ответственности и др. На основе проведенного исследования можно выделить проблемы нормативно-правового обеспечения и практического осуществления проектов ГЧП (МЧП) в отношении объектов информационной инфраструктуры, а также предложить меры по совершенствованию законодательства в целях защиты публичных интересов. В частности:

Во-первых, имеется невысокая заинтересованность отечественных компаний в участии в указанных проектах, в т. ч. из-за существенной ответственности перед государством, сложностей административных процедур и высоких издержек по подготовке технически сложного проекта. Барьером является отсутствие необходимого уровня технических компетенций у частного партнера для решения задач публичного партнера: в сфере ИТ, как правило, требуется высокий, нередко эксклюзивный, уровень квалификации и опыта. При этом существует общая проблема недостаточности квалификации публичного партнера, не зависящая от сферы реализации проектов, преодолеваемая прохождением дополнительных программ обучения, адресованных государственным и муниципальным служащим.

<sup>24</sup> О реализации проекта государственно-частного партнерства, которое осуществляется на основании соглашения, заключаемого в целях создания, эксплуатации и технического обслуживания объекта, предназначенного для обеспечения маркировки и прослеживаемости отдельных видов товаров : распоряжение Правительства Российской Федерации от 8 мая 2019 г. № 899-р // СЗ РФ. 2019. № 20. Ст. 2465.

<sup>25</sup> Честный ЗНАК: Государственная система цифровой маркировки : [официальный сайт]. URL: <https://chestnyy-znak.rf/o-chestnom-znake/nacionalnaya-sistema-markirovki/> (дата обращения: 30.09.2025).

<sup>26</sup> Федеральный цифровой сервис цифровой водоканал // Росинфра : [сайт]. URL: <https://dpo.rosinfra.ru/projects-office/11482/form/application> (дата обращения: 30.09.2025).

<sup>27</sup> О внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 29 декабря 2022 г. № 604-ФЗ // СЗ РФ. 2023. № 1 (ч. I). Ст. 51.

Во-вторых, отмечается пассивность и инертность органов публичной власти как потенциальных публичных партнеров<sup>28</sup>, предпочитающих другие инструменты для реализации проектов по созданию, эксплуатации и техническому обслуживанию объектов информационной инфраструктуры, в т. ч. государственные и муниципальные закупки. Полагаем, для стимулирования проектной деятельности целесообразно привлечь к ее координации автономную некоммерческую организацию (далее – АНО) «Цифровая экономика», являющуюся платформой взаимодействия бизнеса и государства по развитию цифровой экономики<sup>29</sup>.

В-третьих, коммерциализация публичных услуг осложняется из-за специфики сферы ИТ, обусловленной ограничением производства, передачи и распространения информации положениями законодательства о государственной тайне (и в целом об информации ограниченного доступа), о персональных данных и общим законодательством о информации. Частный партнер как создатель и эксплуататор информационных систем аккумулирует значительные объемы «чувствительной» информации, что обязывает его соблюдать существующие нормативно-правовые требования, требует особого внимания государства и дальнейшего взаимного согласования вышеуказанного законодательства. Несмотря на высказанную в доктрине позицию о трудностях монетизации данных ГИС, неготовности органов власти делиться ею [15, с. 67], полагаем, что существующее положение дел в целом оправданно: частный интерес по коммерциализации данных ГИС не должен быть выше публичных интересов по производству и обороту информации ограниченного доступа. Вместе с тем целесообразно совершенствование законодательства о ГЧП и МЧП применительно к объектам информационной инфраструктуры в аспекте углубления легальных характеристик, дифференцирующих информацию, осуществление монетизации которой дозволено (не дозволено) в процессе реализации проекта, в т. ч. с учетом смежного законодательства. При этом очевидно, что социальная функция информационных систем не должна «затеняться» сопутствующими коммерческими услугами, например, в рамках обеспечения доступа к электронным дневникам монетизация доступа к информации, осуществляемая в различных формах, нецелесообразна или вредна.

В-четвертых, проекты в отношении объектов ИТ, а также объектов ИТ и технических средств обеспечения функционирования объектов ИТ нередко интересны зарубежным инвесторам, однако текущее законодательство ограничивает для них проектное участие в отношении указанных объектов в качестве частных партнеров, в т. ч. в рамках создания российских юридических лиц, решения которых прямо или косвенно могут определять иностранные физические лица и (или) иностранные юридические лица, иностранные государства, их органы (ч. 10 ст. 5 ФЗ «О ГЧП») – т. е. исключается их участие полностью, что снижает потенциал применения данного механизма. В смежном инструменте достижения публичных целей – государственных закупках отсутствуют сходные ограничения и более того: в ч. 1 ст. 14 Федерального закона «О контрактной системе в сфере закупок»<sup>30</sup> устанавливается национальный режим, обеспечивающий происходящему из иностранного государства или группы иностранных государств товару, работе, услуге, соответственно выполняемой, оказываемой иностранным гражданином или иностранным юридическим лицом, равные условия с товаром российского происхождения, работой, услугой, соответственно выполняемой, оказываемой российским гражданином или российским юридическим лицом. Таким образом, обеспечены равные условия для иностранных и отечественных субъектов. Изложенное ставит вопрос о целесообразности и логической связности установленного в ФЗ «О ГЧП» запрета на участие иностранных лиц применительно к объектам информационной инфраструктуры со смежным законодательством о государственных закупках и необходимости введения соответствующих изъятий, дифференции правового регулирования ГЧП (МЧП).

Учитывая, что большинство информационных проектов ГЧП (МЧП) не предполагают реализации в особо чувствительных для интересов государства сферах, считаем, следует законодательно дифференцировать проекты на те, в которых «прокси-участие» иностранных субъектов невозможно (проекты с государственной тайной, в сфере обороны, национальной безопасности, в отношении объектов двойного назначения, критической информационной инфраструктуры) и остальные проекты, в которых их участие возможно в рамках создания подконтрольных российских юридических лиц (проектных компаний), поскольку созданный административный

<sup>28</sup> Это следует как из общего количества проектов, относительно небольшого, т. е. потенциал данного инструмента реализован к данному времени не в полной мере, так и из того, что запрос к будущим частным партнерам формирует именно публичный партнер, что в текущих условиях явно осуществляется недостаточно активно.

<sup>29</sup> Автономная некоммерческая организация «Цифровая экономика»: [сайт]. URL: <https://d-economy.ru/about> / (дата обращения: 20.09.2025).

<sup>30</sup> О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд: Федеральный закон от 5 апреля 2013 г. № 44-ФЗ (в ред. от 31.07.2025) // СЗ РФ. 2013. № 14. Ст. 1652.

барьер избыточен, не «откалиброван» под особенности информационной инфраструктуры, интересной в значительной степени зарубежным инвесторам.

В-пятых, целесообразно введение единого реестра прав на объекты ИТ, объекты ИТ и технические средства обеспечения функционирования объектов ИТ, созданные в рамках ГЧП (МЧП), по аналогии с существующим реестром ЦОД<sup>31</sup>. Отсутствие централизованного учета затрудняет контроль за использованием публичных активов, приводит к дублированию технических работок и к излишним затратам.

В-шестых, специфика сферы ИТ предполагает следующие меры по улучшению административно-процедурного сопровождения проектов:

1. Следует установить обязательную предварительную экспертизу проектов в отношении объектов информационной инфраструктуры на соответствие требованиям технической и информационной безопасности, что повысит ее защищенность. Изложенное основывается на обязательном участии технических экспертов, привлекаемых партнерами в целях: выдачи заключений в рамках оценки эффективности и сравнительного преимущества проекта, технических аварий и инцидентов, промежуточных отчетов частного партнера, итогов реализации проекта; помощи в подготовке технического задания по соглашению; сопровождения технической стороны проекта, в т. ч. в рамках консультирования сторон по соответствующим вопросам; и др.

2. Необходимо адаптировать оценку эффективности и сравнительного преимущества проектов с учетом специфики информационной инфраструктуры, включив такие критерии, как срок функционирования на рынке, в т. ч. в сфере реализации информационно-инфраструктурных проектов, наличие необходимой материально-технической и информационной базы, релевантность квалификации сотрудников частного партнера, планируемый уровень информационной и технической безопасности и меры по ее обеспечению в отношении объекта соглашения, действия по поддержанию доступности и непрерывности оказания цифровых услуг для населения и др.

3. Целесообразно оптимизировать процесс осуществления административных процедур под объективно обусловленную специфику информационной инфраструктуры, а также конкретизировать в законодательстве действия публичного партнера по содействию в получении не только разрешений и согласований органов публичной власти (ч. 10 ст. 15 ФЗ «О ГЧП»), но и других видов организационной помощи, адресованной частному партнеру для реализации соглашения, поскольку, в частности, для проектов информационной инфраструктуры в ряде случаев может быть значимо получение, например, аккредитации российских организаций, осуществляющих деятельность в области ИТ<sup>32</sup>, обязательной сертификации средств защиты информации<sup>33</sup>, при этом содействие публичного партнера является существенным фактором успеха проекта. Изложенное возможно реализовать посредством закрепления в подзаконном акте Правительства Российской Федерации примерного перечня видов помощи, оказываемой публичным партнером частному, при корректировке ч. 10 ст. 15 ФЗ «О ГЧП» с отражением в ней соответствующей отсылочной нормы, что конкретизирует обязанности публичного партнера и оптимизирует проектную деятельность частного партнера.

В-седьмых, механизм контроля за созданием, эксплуатацией и техническим обслуживанием объектов информационной инфраструктуры не является адекватным существующим вызовам. Полагаем, необходимо предусмотреть участие публичного партнера в меру имеющихся у него полномочий в проверке соблюдения требований технической и информационной безопасности, достаточности и оперативности применяемых частным партнером мер по ее обеспечению. Целесообразно добавить в конце абзаца ч. 2 ст. 14 ФЗ «О ГЧП» вместо точки запятую и предложение: «обеспечении технической и информационной безопасности в отношении объектов информационных технологий, информационных технологий и технических средств обеспечения функционирования объектов информационных технологий, центров обработки данных». Вместе с тем стандартные формы контроля (проверка отчетности, выездные проверки) не в полной мере и не всегда применимы для контроля безопасности информационной инфраструктуры.

<sup>31</sup> В 2025 году в законодательство были введены изменения, согласно которым Федеральным органом исполнительной власти в области связи ведется реестр ЦОД, расположенных на территории Российской Федерации (См.: СЗ РФ. 2025. № 30 (ч. II). Ст. 4393).

<sup>32</sup> Об утверждении Положения о государственной аккредитации российских организаций, осуществляющих деятельность в области информационных технологий : постановление Правительства Российской Федерации от 30 сентября 2022 г. № 1729 // СЗ РФ. 2022 № 40. Ст. 6845.

<sup>33</sup> О сертификации средств защиты информации : постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 (в ред. от 21.04.2010) // СЗ РФ. 1995. № 27. Ст. 2579.

Публичный партнер, как правило, не обладает техническими возможностями для осуществления такого контроля, для чего необходимо привлечение иных уполномоченных органов (Федеральной службы по техническому и экспортному контролю и др.), т. е. совместное участие в проверке публичного партнера и данных органов. Кроме того, наряду с общими технико-функциональными требованиями объектов информационной инфраструктуры в соглашениях должны определяться требования, критерии и меры технической и информационной безопасности, обеспечивающие и определяющие стабильность их работы<sup>34</sup>. Полагаем, следует выработать и определить изложенное в рамках примерного перечня посредством издания подзаконного акта Правительства Российской Федерации.

В то же время, с учетом Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»<sup>35</sup>, некоторые объекты СГЧП (СМЧП) могут быть отнесены к объектам критической информационной инфраструктуры (п. 7 ст. 2), что налагает на его владельца – частного партнера строгие обязательства по информированию уполномоченного государственного органа о компьютерных атаках, компьютерных инцидентах и др. обязанности (ст. 9), при этом непрерывность и комплексность обеспечения ее безопасности определены в качестве принципа (ст. 4). В целом в законодательстве не детализированы механизмы оперативного контроля и реагирования на инциденты в сфере технической и информационной безопасности в ходе реализации СГЧП (СМЧП). Существующие подзаконные акты регламентируют вопросы защиты информации, содержащейся в информационных системах<sup>36</sup>, однако объекты информационной инфраструктуры СГЧП (СМЧП) включают в себя не только указанные системы, что также нуждается в детализации. Кроме того, не урегулирован вопрос о распределении ответственности в случае кибератаки или иного инцидента в сфере технической или информационной безопасности на систему, созданную в рамках проекта ГЧП (МЧП), в частности, несет ли ответственность частный партнер за ущерб, причиненный таким инцидентом, и в какой мере, а отсутствие положений о действиях сторон при его наступлении является значимым правовым риском.

Полагаем, для решения вышеизложенных проблем следует:

1. Дополнить ст. 33.1 ФЗ «О ГЧП» новой частью в следующей редакции:

«В соглашениях, объектом которых являются объекты информационных технологий и (или) технические средства обеспечения функционирования объектов информационных технологий, которые отнесены в установленном порядке к объектам критической информационной инфраструктуры, должны содержаться следующие условия:

1) обязанность частного партнера соблюдать требования законодательства Российской Федерации о безопасности критической информационной инфраструктуры, включая своевременное информирование уполномоченного федерального органа исполнительной власти о компьютерных атаках и компьютерных инцидентах;

2) обязанность частного партнера обеспечивать возможность подключения создаваемого, эксплуатируемого и (или) технически обслуживаемого объекта соглашения к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

3) право публичного партнера и уполномоченных органов государственной власти на проведение контрольных (надзорных) мероприятий в части соблюдения требований законодательства в области обеспечения безопасности критической информационной инфраструктуры;

4) ответственность частного партнера за несоблюдение установленных законом требований в области безопасности критической информационной инфраструктуры, включая право публичного партнера на расторжение соглашения в одностороннем порядке в случае грубого или неоднократного нарушения указанных требований частным партнером».

<sup>34</sup> Например, в рамках проекта по созданию, обеспечению функционирования и технического сопровождения региональной информационной системы «Цифровая образовательная платформа Чеченской Республики» определены такие характеристики, как средний уровень доступности не ниже 98 % рабочего времени платформы, аварийные режимы работы (более 1 ч. простоя) не чаще 1 раза в месяц в течение учебных периодов, плановая производительность в части обработки запросов в секунду и др. (См.: СГЧП по созданию, обеспечению функционирования и техническому сопровождению региональной информационной системы «Цифровая образовательная платформа Чеченской Республики» // Росинфра : [сайт]. URL: <https://dpo.rosinfra.ru/projects-office/12724/form/application> (дата обращения: 30.09.2025)).

<sup>35</sup> О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26 июля 2017 г. № 187-ФЗ (в ред. от 07.04.2025) // СЗ РФ. 2017. № 31 (ч. I). Ст. 4736.

<sup>36</sup> См, например: Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений : приказ Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 // Официальный интернет-портал правовой информации (pravo.gov.ru). URL: <http://publication.pravo.gov.ru/document/0001202506170011> (дата обращения: 17.06.2025).

2. Разработать и утвердить в форме подзаконного акта Правительства Российской Федерации типовое дополнительное соглашение к СЧП (СМЧП) для проектов в отношении информационной инфраструктуры, которое будет включать:

а) перечень мер технической и информационной безопасности, которые обязан соблюдать частный партнер на протяжении всего периода функционирования объекта;

б) регламент взаимодействия сторон и порядок их взаимного оповещения в случае инцидента информационной или технической безопасности, включая уведомление, сроки и формы предоставления необходимой информации;

в) механизм распределения ответственности и возмещения ущерба в зависимости от того, по чьей вине произошел инцидент (невыполнение частным партнером мер защиты или виновные действия/бездействие публичного партнера);

г) обязательность проведения регулярного независимого аудита защищенности системы.

3. Организовать системную методическую поддержку проектов ГЧП (МЧП) в отношении информационной инфраструктуры со стороны профильных федеральных органов публичной власти (Минэкономразвития России, Минкомсвязи России, ФСБ России, ФСТЭК России и др.), осуществляемую в целях единообразия проектной практики на уровне субъектов Российской Федерации в аспекте обеспечения технической и информационной безопасности.

4. Установить административную ответственность частного партнера (в виде штрафов) за сокрытие информации об инцидентах технической и информационной безопасности и (или) несоблюдение установленных требований в данной сфере, повлекшее определенный ущерб (можно в рамках уточнения ст. 13.12. Кодекса Российской Федерации об административных правонарушениях<sup>37</sup>).

5. Дополнить статью 33.1 ФЗ «О ГЧП» новой частью в следующей редакции: «Нарушение требований технической и (или) информационной безопасности частным партнером, повлекшее существенный вред правам и интересам граждан, общества и государства, является основанием для расторжения соглашения публичным партнером в одностороннем порядке».

В-восьмых, отсутствует прямо предусмотренная законом возможность апробации инновационных проектов ГЧП (МЧП), реализуемых в отношении объектов информационной инфраструктуры, в рамках установления экспериментальных правовых режимов, что нецелесообразно: проекты на основе использования ИТ нередко нуждаются в адаптации правового регулирования к их особенностям, а несогласованность законодательства приводит к неопределенности или неоправданному ограничению данной возможности. Экспериментальные правовые режимы в значительной степени пересекаются по сферам деятельности, целям и совершаемым действиям с ГЧП (МЧП), предполагая предоставление государственных и муниципальных услуг, производство продукции, строительство, реконструкцию и эксплуатацию объектов, в т. ч. в рамках сфер транспорта, промышленности – и все на базе ИТ<sup>38</sup>, что связывает экспериментальные правовые режимы с исследуемым явлением. Однако в настоящее время законодательство, регламентирующее их, не взаимоувязано, необходимо гармонизировать ФЗ «О ГЧП» в части реализации проектов в отношении объектов информационной инфраструктуры и Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации»<sup>39</sup>, поскольку не ясно, возможно ли их совмещение и в какой форме.

В-девятых, в доктрине предлагается «разработать и освоить, и широко тиражировать методические рекомендации по управлению рисками, которые должны включать обзор лучших российских и мировых практик управления рисками в проектах ГЧП в сфере ИТ» [15, с. 70]. Полностью с данным предложением согласиться нельзя: сходные методические рекомендации должны быть комплексными, включать не только сферу ИТ, и реализовываться в рамках создания национального стандарта ГЧП<sup>40</sup>, на необходимость разработки которого со стороны ВЭБ.РФ<sup>41</sup> указал Президент Российской Федерации в рамках Восточного экономического форума (2025)<sup>42</sup>.

<sup>37</sup> Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. от 31.07.2025) // СЗ РФ. 2002. № 1 (ч. I). Ст. 1.

<sup>38</sup> См.: Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации» (в ред. 31.07.2025) // СЗ РФ. 2020. № 31 (ч. I). Ст. 5017.

<sup>39</sup> СЗ РФ. 2020. № 31 (ч. I). Ст. 5017.

<sup>40</sup> Включающего, в т. ч., свод методических рекомендаций высокого уровня обобщения по основным аспектам практики ГЧП (МЧП).

<sup>41</sup> О государственной корпорации развития «ВЭБ.РФ»: Федеральный закон от 17 мая 2007 г. № 82-ФЗ (ред. от 10.07.2023) // СЗ РФ. 2007. № 22. Ст. 2562.

<sup>42</sup> Партнерства построят по стандарту // Коммерсантъ: [сетевое издание]. URL: <https://www.kommersant.ru/doc/8010164> (дата обращения: 30.09.2025).

### 3 Заключение

Таким образом, административно-правовое регулирование ГЧП (МЧП) в отношении объектов информационной инфраструктуры характеризуется наличием несовершенств, обусловленных специфическим объектом регулирования. Их преодоление предполагает комплексный подход, включающий:

1) гармонизиацию законодательства об экспериментальных правовых режимах и о ГЧП (МЧП) применительно к объектам информационной инфраструктуры;

2) принятие комплекса законодательных изменений по совершенствованию механизма контроля за созданием, эксплуатацией и техническим обслуживанием данных объектов;

3) привлечение к координации проектной деятельности АНО «Цифровая экономика»;

4) принятие мер по улучшению административно-процедурного сопровождения проектов ГЧП (МЧП):

4.1) установление обязательной предварительной экспертизы проектов в отношении объектов информационной инфраструктуры на соответствие требованиям технической и информационной безопасности;

4.2) адаптацию оценки эффективности и сравнительного преимущества проектов с учетом специфики ИТ, включая такие критерии, как наличие необходимой материально-технической и информационной базы, релевантность квалификации сотрудников частного партнера, планируемый уровень информационной и технической безопасности и меры по ее обеспечению в отношении объекта соглашения, действия по поддержанию доступности и непрерывности оказания цифровых услуг для населения и др.;

4.3) конкретизацию в законодательстве действий публичного партнера по содействию в получении не только разрешений и согласований органов публичной власти, но и других видов организационной помощи, адресованной частному партнеру, посредством закрепления в подзаконном акте Правительства Российской Федерации примерного перечня видов данной помощи;

5) совершенствование законодательства о ГЧП (МЧП) применительно к объектам информационной инфраструктуры в аспекте детализации легальных характеристик, дифференцирующих информацию, осуществление монетизации которой дозволено (не дозволено) в процессе реализации проекта;

6) пересмотр положений, запрещающих участие иностранных лиц через подконтрольных им российских юридических лиц в проектах ГЧП (МЧП), реализуемых в отношении объектов информационной инфраструктуры: следует законодательно разделить проекты на те, в которых «прокси-участие» иностранных субъектов невозможно (проекты с государственной тайной, в сфере обороны, национальной безопасности, в отношении объектов двойного назначения, критической информационной инфраструктуры) и остальные проекты, в которых их участие возможно в рамках создания подконтрольных российских юридических лиц;

7) введение единого реестра прав на объекты ИТ, объекты ИТ и технические средства обеспечения функционирования объектов ИТ, созданные в рамках ГЧП (МЧП), по аналогии с существующим реестром ЦОД.

### Список источников

1. Редкоус В. М. Особенности регулирования отношений государственно-частного партнерства в отношении объектов информационных технологий или объектов информационных технологий и технических средств обеспечения функционирования объектов информационных технологий // *Аграрное и земельное право*. 2023. № 4 (220). С. 68–72. [http://doi.org/10.47643/1815-1329\\_2023\\_4\\_68](http://doi.org/10.47643/1815-1329_2023_4_68)

2. Савченко Я. В., Нураев Т. А. Законодательство как фактор развития государственно-частного партнерства в сфере информационных технологий // *Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право*. 2022. Т. 22, вып. 1. С. 86–95. <https://doi.org/10.18500/1994-2540-2022-22-1-86-95>

3. Проняева Л. И., Кружкова И. И. Реализация проектов государственно-частного партнерства в ИТ-сфере: состояние и условия // *Среднерусский вестник общественных наук*. 2020. Т. 15, № 1. С. 186–203. <https://doi.org/10.22394/2071-2367-2020-15-1-186-203>

4. Ведерникова Е. В. Реализация проектов государственно-частного партнерства в сфере информационных услуг // *Вестник Пермского национального исследовательского политехнического университета. Социально-экономические науки*. 2023. № 3. С. 287–300. [10.15593/2224-9354/2023.3.20](https://doi.org/10.15593/2224-9354/2023.3.20)

5. Караваева Е. В., Байбурун Р. Р. Роль государственно-частного партнерства в условиях цифровизации экономики // *Вестник Алтайской академии экономики и права*. 2023. № 10-3. С. 316–321. <https://doi.org/10.17513/vaael.3050>

6. Сергеева Н. В. Цифровизация государственного управления и публично-частное партнерство // *Oeconomia et Jus*. 2024. № 4. С. 51–63. <https://doi.org/10.47026/2499-9636-2024-4-51-63>

7. Сергеева Н. В. Государственно-частное партнерство в ИТ-сфере: особенности распределения исключительных прав // *Вестник экономики, права и социологии*. 2024. № 3. С. 132–135. <https://doi.org/10.24412/1998-5533-2024-3-132-135>

8. Шор И. М. Применение государственно-частного партнерства в сфере информационных технологий // Вестник Волгоградского государственного университета. Экономика. 2022. Т. 24, № 3. С. 146–157. <https://doi.org/10.15688/ek.jvolsu.2022.3.12>

9. Байбулатова Д. В. Государственно-частное партнерство как инструмент стимулирования инновационной деятельности бизнеса в сфере цифровых технологий // Экономика науки. 2023. Т. 9, № 3. С. 61–75. <https://doi.org/10.22394/2410-132X-2023-9-3-61-75>

10. Савченко Я. В., Нураев Т. А. Государственно-частное партнерство в сфере информационно-коммуникационных технологий в отечественной и зарубежной практике: специфика и динамика развития // Beneficium. 2022. № 1 (42). С. 100–109. [https://doi.org/10.34680/BENEFICIUM.2022.1\(42\).100-109](https://doi.org/10.34680/BENEFICIUM.2022.1(42).100-109)

11. Громова Е. А. Создание цифровых технологий в рамках государственно-частного партнерства: опыт БРИКС // Вестник Южно-Уральского государственного университета. Серия: Право. 2019. Т. 19, № 1. С. 42–45. <https://doi.org/10.14529/law19010>

12. Веселовский М. Я. Государственно-частное партнерство в инновационной сфере: современное состояние и перспективы // МИР (Модернизация. Инновации. Развитие). 2015. Т. 6, № 3 (23). С. 8–17. <https://doi.org/10.18184/2079-4665.2015.6.3.8.17>

13. Меджидов М. М. Роль государственно-частного партнерства в оптимизации деятельности государства в сфере информационно-коммуникационных технологий // Право и управление. XXI век. 2014. № 1 (30). С. 101–107.

14. Гергиев И. Э., Кайсинов А. А. Развитие государственно-частного партнерства в сфере информационных технологий // Инновационная наука. 2019. № 10. С. 43–45.

15. Виноградова Т. Г., Семилетова Я. И., Рахманова А. Б. Эффективные информационные технологии в секторе государственно-частного партнерства: особенности и факторы развития // Вестник науки. 2021. Т. 3, № 10 (43). С. 62–71.

## References

1. Redkous V. M. Osobennosti regulirovaniya otnoshenij gosudarstvenno-chastnogo partnerstva v otnoshenii ob"ektov informacionnyh tekhnologij ili ob"ektov informacionnyh tekhnologij i tekhnicheskikh sredstv obespecheniya funkcionirovaniya ob"ektov informacionnyh tekhnologij // Agrarnoe i zemel'noe pravo. 2023. № 4 (220). S. 68–72. [http://doi.org/10.47643/1815-1329\\_2023\\_4\\_68](http://doi.org/10.47643/1815-1329_2023_4_68)

2. Savchenko Ya. V., Nuraev T. A. Zakonodatel'stvo kak faktor razvitiya gosudarstvenno-chastnogo partnerstva v sfere informacionnyh tekhnologij // Izvestiya Saratovskogo universiteta. Novaya seriya. Seriya: Ekonomika. Upravlenie. Pravo. 2022. T. 22, vyp. 1. S. 86–95. <https://doi.org/10.18500/1994-2540-2022-22-1-86-95>

3. Pronyaeva L. I., Kruzhkova I. I. Realizaciya proektov gosudarstvenno-chastnogo partnerstva v IT-sfere: sostoyanie i usloviya // Srednerusskij vestnik obshchestvennyh nauk. 2020. T. 15, № 1. S. 186–203. <https://doi.org/10.22394/2071-2367-2020-15-1-186-203>

4. Vedernikova E. V. Realizaciya proektov gosudarstvenno-chastnogo partnerstva v sfere informacionnyh uslug // Vestnik Permskogo nacional'nogo issledovatel'skogo politekhnicheskogo universiteta. Social'no-ekonomicheskie nauki. 2023. № 3. S. 287–300. <https://doi.org/10.15593/2224-9354/2023.3.20>

5. Karavaeva E. V., Bajburin R. R. Rol' gosudarstvenno-chastnogo partnerstva v usloviyah cifrovizacii ekonomiki // Vestnik Altajskoj akademii ekonomiki i prava. 2023. № 10–3. S. 316–321. <https://doi.org/10.17513/vaael.3050>

6. Sergeeva N. V. Cifrovizaciya gosudarstvennogo upravleniya i publichno-chastnoe partnerstvo // Oeconomia et Jus. 2024. № 4. S. 51–63. <https://doi.org/10.47026/2499-9636-2024-4-51-63>

7. Sergeeva N. V. Gosudarstvenno-chastnoe partnerstvo v IT-sfere: osobennosti raspredeleniya iskluchitel'nyh prav // Vestnik ekonomiki, prava i sociologii. 2024. № 3. S. 132–135. <https://doi.org/10.24412/1998-5533-2024-3-132-135>

8. Shor I. M. Primenenie gosudarstvenno-chastnogo partnerstva v sfere informacionnyh tekhnologij // Vestnik Volgogradskogo gosudarstvennogo universiteta. Ekonomika. 2022. T. 24, № 3. S. 146–157. <https://doi.org/10.15688/ek.jvolsu.2022.3.12>

9. Bajbulatova D. V. Gosudarstvenno-chastnoe partnerstvo kak instrument stimulirovaniya innovacionnoj deyatelnosti biznesa v sfere cifrovnyh tekhnologij // Ekonomika nauki. 2023. T. 9, № 3. S. 61–75. <https://doi.org/10.22394/2410-132X-2023-9-3-61-75>

10. Savchenko Ya. V., Nuraev T. A. Gosudarstvenno-chastnoe partnerstvo v sfere informacionno-kommunikacionnyh tekhnologij v otechestvennoj i zarubezhnoj praktike: specifiika i dinamika razvitiya // Beneficium. 2022. № 1 (42). S. 100–109. [https://doi.org/10.34680/BENEFICIUM.2022.1\(42\).100-109](https://doi.org/10.34680/BENEFICIUM.2022.1(42).100-109)

11. Gromova E. A. Sozdanie cifrovnyh tekhnologij v ramkah gosudarstvenno-chastnogo partnerstva: opyt BIRKS // Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Pravo. 2019. T. 19, № 1. S. 42–45. <https://doi.org/10.14529/law19010>

12. Veselovskij M. Ya. Gosudarstvenno-chastnoe partnerstvo v innovacionnoj sfere: sovremennoe sostoyanie i perspektivy // MIR (Modernizaciya. Innovacii. Razvitie). 2015. T. 6, № 3 (23). S. 8–17. <https://doi.org/10.18184/2079-4665.2015.6.3.8.17>

13. Medzhidov M. M. Rol' gosudarstvenno-chastnogo partnerstva v optimizacii deyatelnosti gosudarstva v sfere informacionno-kommunikacionnyh tekhnologij // Pravo i upravlenie. XXI vek. 2014. № 1 (30). S. 101–107.

14. Gergiev I. E., Kajsinov A. A. Razvitie gosudarstvenno-chastnogo partnerstva v sfere informacionnyh tekhnologij // Innovacionnaya nauka. 2019. № 10. S. 43–45.

15. Vinogradova T. G., Semiletova Ya. I., Rahmanova A. B. Effektivnye informacionnye tekhnologii v sektore gosudarstvenno-chastnogo partnerstva: osobennosti i faktory razvitiya // Vestnik nauki. 2021. T. 3, № 10 (43). S. 62–71.