

ВАСИЯН Роман Иванович,
доцент Департамента гуманитарного
и социально-экономического образования,
ФГАОУ ВО «Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина»,
заместитель генерального директора
по правовому обеспечению и корпоративному управлению
АО «Концерн “Уралвагонзавод”»,
Екатеринбург, Россия,
e-mail: R_Vasiyan@mail.ru

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРАВОВОЙ ОХРАНЫ И ЗАЩИТЫ ПРАВ СУБЪЕКТОВ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статье исследуются актуальные проблемы правовой охраны и защиты прав субъектов экономической деятельности в условиях цифровой трансформации в Российской Федерации. Обосновывается, что традиционные гражданско-правовые и публично-правовые способы защиты не всегда способны обеспечить надлежащую охрану прав субъектов в цифровой среде, поскольку цифровые платформы, смарт-контракты, большие данные, персональные данные, электронная коммерция и автоматизированные информационные системы формируют новые модели экономического оборота. Особое внимание уделяется разграничению понятий «охрана» и «защита» прав в цифровой среде, правовому статусу владельцев агрегаторов, защите информации, персональных данных и больших данных. Рассматриваются проблемы квалификации больших данных как самостоятельного объекта разноотраслевого правового регулирования. Делается вывод о необходимости совершенствования законодательства об информации, персональных данных, цифровых платформах, электронно-цифровой коммерции, антимонопольном регулировании и экономической безопасности.

Ключевые слова: цифровая трансформация, субъекты экономической деятельности, защита прав, охрана прав, цифровая среда, персональные данные, большие данные, цифровые платформы, электронная коммерция, экономическая безопасность.

VASIYAN Roman Ivanovich,
Associate Professor, Department of Humanitarian
and Socio-Economic Education
Ural Federal University named after the
First President of Russia B. N. Yeltsin
Deputy General Director for Legal Support
and Corporate Governance
JSC Concern Uralvagonzavod,
Yekaterinburg, Russia

CURRENT PROBLEMS OF LEGAL PROTECTION AND DEFENCE OF THE RIGHTS OF ECONOMIC ENTITIES IN THE CONTEXT OF DIGITAL TRANSFORMATION IN THE RUSSIAN FEDERATION

Annotation. The article examines current problems of legal protection and defence of the rights of economic entities in the context of digital transformation in the Russian Federation. It is argued that traditional civil law and public law remedies are not always sufficient to ensure proper protection of rights in the digital environment, since digital platforms, smart contracts, big data, personal data, e-commerce and automated information systems create new models of economic turnover. Special attention is paid to the distinction between legal protection and legal defence of rights in the digital environment, the legal status of online aggre-

gators, information protection, personal data protection and big data regulation. The article considers the problem of qualifying big data as an independent object of cross-sectoral legal regulation. The conclusion is made that legislation on information, personal data, digital platforms, e-commerce, antimonopoly regulation and economic security requires further development.

Key words: *digital transformation, economic entities, legal defence of rights, legal protection of rights, digital environment, personal data, big data, digital platforms, e-commerce, economic security.*

Введение

Цифровая трансформация существенно изменила условия осуществления экономической деятельности. Если ранее цифровые технологии рассматривались преимущественно как вспомогательные инструменты документооборота, расчётов и коммуникации, то в настоящее время они всё чаще определяют саму модель экономического поведения субъектов. Договоры заключаются через электронные платформы, расчёты осуществляются с использованием цифровых платёжных инструментов, сведения о потребителях и контрагентах обрабатываются в автоматизированных системах, а рыночная стратегия хозяйствующих субъектов все чаще строится на анализе больших массивов данных.

В таких условиях традиционные способы охраны и защиты прав субъектов экономической деятельности оказываются недостаточными. Они формировались применительно к аналоговой экономике, где объект, субъект, момент нарушения и способ восстановления права чаще были очевидны. В цифровой среде эти элементы нередко становятся размытыми: правонарушение может быть совершено автоматически, данные могут обрабатываться распределённо, а причинение вреда может быть связано не с одним действием, а с совокупностью алгоритмических операций.

Показателен пример смарт-контракта. В отличие от обычного гражданско-правового договора, смарт-контракт исполняется автоматически при наступлении заранее заданных условий. После внесения соответствующего программного кода в блокчейн возможность оперативного изменения условий либо приостановления исполнения существенно ограничивается. В результате защита права не всегда может осуществляться теми же способами, которые применяются при исполнении обычного договора. Сходные проблемы возникают в сфере цифровой конкуренции. Посягательства на права субъектов экономической деятельности могут выражаться не только в прямом нарушении договора или причинении имущественного вреда, но и в использовании сетевых эффектов, алгоритмического ценообразования, манипулирования поисковой выдачей, ограничения доступа к платформенной инфраструктуре, недобросовестного использования больших данных. При формально- юриди-

ческом подходе такие действия не всегда очевидно противоправны, хотя фактически способны ограничивать конкуренцию и нарушать интересы участников рынка.

Экономико-правовая природа указанных процессов подчёркивается и в исследованиях, посвящённых инновационной деятельности предприятий в условиях цифровой экономики. Так, А. В. Чешин отмечает, что цифровизация инновационной деятельности требует комплексного учёта экономических и правовых факторов, поскольку внедрение цифровых решений меняет не только технологический, но и организационно-правовой контур деятельности предприятий [14, с. 426–433].

Цель настоящей статьи состоит в выявлении актуальных проблем правовой охраны и защиты прав субъектов экономической деятельности в условиях цифровой трансформации и в обосновании направлений совершенствования российского законодательства в данной сфере.

Материалы и методы исследований

Материалами исследования выступили положения Конституции Российской Федерации, Гражданского кодекса Российской Федерации, Закона Российской Федерации «О защите прав потребителей», федеральных законов «Об информации, информационных технологиях и о защите информации», «О персональных данных», «О связи», «О национальной платёжной системе», Постановление Конституционного Суда Российской Федерации от 17.02.2026 № 7-П, ГОСТ Р ИСО/МЭК 20546–2021, а также международные и зарубежные акты, включая GDPR и Директиву ЕС 2022/2555.

В качестве научной базы использованы труды и публикации, посвящённые цифровой экономике, цифровой трансформации управления, экономической безопасности, большим данным, инновационному предпринимательству и правовой охране субъектов экономической деятельности. Методологическую основу исследования составили формально-юридический, системный, сравнительно-правовой и межотраслевой методы. Формально-юридический метод позволил проанализировать содержание действующих правовых норм. Системный метод применялся при рассмотрении цифровой среды как совокупности частноправовых, публично-правовых,

информационных, предпринимательских и финансово-правовых отношений. Сравнительно-правовой метод использовался при обращении к опыту Европейского союза, США и Китая. Межотраслевой подход позволил показать, что охрана и защита прав субъектов экономической деятельности в цифровой среде не могут быть сведены только к гражданско-правовым способам защиты.

Результаты и обсуждение

Правовое регулирование отношений, связанных с охраной и защитой прав субъектов экономической деятельности в цифровой сфере, получило отражение в нормах различных отраслей законодательства. Конституционной основой такого регулирования выступают положения статьи 71 Конституции Российской Федерации, относящиеся к ведению Российской Федерации обеспечение безопасности личности, общества и государства при применении информационных технологий и обороте цифровых данных [1].

При этом цифровая безопасность не может пониматься исключительно как техническая защищённость информационных систем. Речь идёт о более широком явлении, включающем защиту прав личности, интересов общества, государства и субъектов экономической деятельности. Цифровая экономика создаёт новые возможности для предпринимательства, но одновременно усиливает зависимость хозяйствующих субъектов от платформ, информационной инфраструктуры, алгоритмов обработки данных и устойчивости цифровых сервисов.

Цифровая трансформация затрагивает также сферу публичного управления. Электронные реестры, межведомственный обмен данными, цифровые государственные сервисы, автоматизированный контроль, платформенные механизмы взаимодействия бизнеса и государства становятся частью регуляторной среды. Л. В. Дмитриева справедливо указывает, что цифровая трансформация управления предполагает изменение не только технических инструментов, но и самих подходов к организации управленческих процессов [15, с. 176–197]. Поэтому защита прав субъектов экономической деятельности в цифровой среде должна рассматриваться во взаимосвязи частноправовых и публично-правовых механизмов.

Одним из наиболее заметных направлений правового регулирования цифровой экономики является защита прав потребителей в электронной коммерции. Развитие маркетплейсов, агрегаторов, сервисов доставки, электронных платёжных решений и дистанционной торговли привело к появлению новых посредников между продавцом и потребителем.

Значимым актом в данной сфере является Федеральный закон от 29.07.2018 № 250-ФЗ, которым в Закон Российской Федерации «О защите прав потребителей» были внесены положения о владельце агрегатора информации о товарах и услугах [5]. Законодатель закрепил обязанности владельца агрегатора по предоставлению информации о себе и продавце, а также установил отдельные правила ответственности за предоставление потребителю недостоверной или неполной информации. Однако правовая модель агрегатора остаётся неоднозначной. С одной стороны, агрегатор не всегда является продавцом в классическом смысле. С другой стороны, в современной электронной коммерции он нередко выполняет гораздо более широкие функции: принимает оплату, организует доставку, устанавливает правила взаимодействия продавца и покупателя, участвует в разрешении споров, определяет условия возврата денежных средств. В такой ситуации агрегатор перестаёт быть нейтральным информационным посредником и фактически приобретает регуляторное влияние внутри цифровой платформы.

Дополнительное значение для данной сферы имеет Постановление Конституционного Суда Российской Федерации от 17.02.2026 № 7-П, которым были выявлены проблемы правового регулирования возврата товара надлежащего качества, приобретённого дистанционным способом [6]. Конституционный Суд указал на необходимость урегулировать порядок такого возврата с учётом баланса интересов продавца и покупателя. Данная позиция важна не только для потребительского права, но и для понимания общей тенденции: цифровая торговля требует специальных юридических механизмов, поскольку классические правила розничной купли-продажи не всегда учитывают специфику дистанционного взаимодействия.

Защита прав потребителей в цифровой среде должна строиться не только на формальном информировании покупателя. Необходимы механизмы реальной проверяемости информации, прозрачности платформенных правил, ответственности агрегаторов за свои цифровые сервисы, а также справедливого распределения рисков между продавцом, потребителем, агрегатором, перевозчиком и платёжной организацией. Другое важное направление связано с правовым обеспечением охраны и защиты информации. В соответствии со статьёй 16 Федерального закона от 27.07.2006 № 149-ФЗ защита информации представляет собой принятие правовых, организационных и технических мер, направленных на защиту информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий [7].

Данное нормативное определение имеет большое значение, однако вызывает ряд вопросов. Во-первых, оно во многом описывает защиту информации через «обеспечение защиты информации», что не устраняет терминологической неопределённости. Во-вторых, в нём преимущественно отражён превентивный и технический аспект, тогда как юридическая защита права предполагает также пресечение нарушения, восстановление нарушенного положения, возмещение убытков, применение мер ответственности и иных правовых последствий.

В связи с этим представляется необходимым разграничивать охрану и защиту прав субъектов экономической деятельности в цифровой среде.

Охрана прав субъектов экономической деятельности в цифровой среде - это деятельность государства, иных публичных субъектов, организаций и самих участников цифровых правоотношений, направленная на создание нормативных, организационных, технических и договорных условий, предупреждающих нарушение прав и законных интересов в цифровом пространстве.

Защита прав субъектов экономической деятельности в условиях цифровой трансформации - это деятельность компетентных органов, иных уполномоченных лиц и самих участников правоотношений, направленная на пресечение нарушения либо реальной угрозы нарушения цифровых прав и законных интересов, восстановление нарушенного положения, возмещение убытков, компенсацию вреда и применение иных мер юридического воздействия. Такой подход позволяет устранить смешение профилактических и восстановительных механизмов. Охрана действует до нарушения либо в целях его предупреждения. Защита возникает тогда, когда право уже нарушено либо имеется реальная угроза нарушения.

Развитие цифровой экономики в регионах России также показывает, что правовая защищённость субъектов предпринимательства зависит не только от формального наличия норм, но и от цифровой инфраструктуры, кадровых возможностей, организационной готовности и доступности цифровых сервисов. А. В. Минаков и А. Е. Суглобов обращают внимание на проблемы регионального развития цифровой экономики, включая неравномерность цифровой инфраструктуры и различия в условиях цифровизации [16, с. 63–72]. Это означает, что охрана прав субъектов экономической деятельности в цифровой среде должна учитывать не только нормативные, но и фактические условия доступа к цифровым инструментам. Часть 2 статьи 16 Федерального закона № 149-ФЗ связывает государственное регулирование отношений в сфере защиты

информации с установлением требований о защите информации и ответственности за нарушение законодательства об информации [7]. Однако такое понимание государственного регулирования представляется чрезмерно узким.

Государственное регулирование должно включать не только установление требований и ответственности, но и мониторинг цифровой среды, контроль исполнения требований, оценку рисков, развитие стандартов информационной безопасности, взаимодействие с участниками рынка, предупреждение нарушений, международное сотрудничество, а также формирование единых подходов к обработке и защите данных.

Отдельный вопрос касается ответственности обладателя информации и оператора информационной системы. В статье 16 Федерального закона № 149-ФЗ установлены обязанности по обеспечению защиты информации, однако не вполне ясно, как должна распределяться ответственность в случае, если вред причинён совместными действиями либо бездействием обладателя информации и оператора информационной системы. Представляется, что в отношении с потерпевшим субъектом более эффективной была бы модель солидарной ответственности с последующим распределением ответственности между обязанными лицами с учётом степени их вины.

Международный опыт подтверждает, что регулирование защиты информации всё чаще строится на сочетании технических стандартов, организационных требований и публичного контроля. В США применяются механизмы контроля безопасности NIST SP 800-53 для федеральных информационных систем [11]. В Европейском союзе действует Директива 2022/2555, известная как NIS2, которая обязывает государства-члены развивать национальные стратегии кибербезопасности и меры защиты цепочек поставок программного обеспечения [12]. В Китае используется комплексная система контроля информационного пространства, включая идентификацию пользователей, фильтрацию трафика и иные технические средства государственного контроля.

Для Российской Федерации особое значение имеет развитие собственной модели регулирования, сочетающей защиту прав субъектов экономической деятельности, обеспечение цифрового суверенитета, сохранение конкуренции и устойчивость цифровой инфраструктуры.

Третьим важным направлением является обеспечение прав и законных интересов субъектов, связанных с обработкой персональных данных. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ персональные данные - это любая информация, относящаяся к прямо или

косвенно определённого или определяемому физическому лицу [8]. Данное определение по своей природе является широким. Оно позволяет охватывать новые виды цифровых идентификаторов, однако одновременно порождает неопределённость. В судебной практике возникали вопросы о том, могут ли относиться к персональным данным адрес электронной почты, ID пользователя, IP-адрес, файлы cookies, номер телефона, данные систем аналитики и иные цифровые следы. Так, в деле LinkedIn суды признали нарушающей требования законодательства деятельность интернет-ресурсов по сбору, использованию и хранению персональных данных граждан Российской Федерации. В другом деле, связанном с ПАО «Ростелеком», суд указал, что сведения об абонентах и оказываемых им услугах связи являются информацией ограниченного доступа и подлежат защите в соответствии с законодательством Российской Федерации.

В связи с этим можно выделить два подхода к определению персональных данных. Первый основан на широком понимании этой категории и предполагает оценку каждого случая с учётом конкретных обстоятельств. Второй связан с идеей законодательного закрепления закрытого перечня сведений, относимых к персональным данным. Однако оба подхода имеют недостатки. Широкое понимание создаёт неопределённость, а закрытый перечень быстро устаревает в условиях развития цифровых технологий. Более продуктивным представляется подход, при котором персональные данные определяются через совокупность юридических и технологических критериев. В этой связи можно предложить следующее уточнение: персональные данные – это информация ограниченного доступа, имеющая специальный правовой режим, прямо обозначенная в законодательстве как персональные данные либо позволяющая с использованием иных данных и цифровых технологий прямо или косвенно идентифицировать физическое лицо. Такой подход позволяет учитывать развитие цифровой среды и одновременно не превращает любую информацию о человеке в персональные данные автоматически.

Защиту прав и законных интересов субъектов персональных данных следует понимать как деятельность судебных, административных и иных компетентных органов, операторов, иных обязанных лиц и самих субъектов персональных данных, направленную на пресечение неправомерной обработки персональных данных, восстановление нарушенного положения, удаление, блокирование или уточнение данных, возмещение убытков и компенсацию морального вреда. С учетом роста числа споров о правовом режиме

цифровых идентификаторов целесообразно подготовить обзор судебной практики Верховного Суда Российской Федерации по вопросам квалификации отдельных видов сведений в качестве персональных данных.

Особое место в цифровой экономике занимает феномен больших данных. С юридической конструкцией защиты персональных данных он связан непосредственно, поскольку персональные данные могут входить в состав больших данных. Однако большие данные не сводятся к персональным данным. Они включают различные массивы сведений, имеющих разные правовые режимы: коммерческую информацию, публичные данные, технические данные, обезличенные сведения, статистическую информацию, данные платформ, сведения о потребительском поведении.

В ГОСТ Р ИСО/МЭК 20546–2021 большие данные определяются как большие массивы данных, отличающиеся такими характеристиками, как объём, разнообразие, скорость обработки и вариативность, требующие использования технологий масштабирования для эффективного хранения, обработки, управления и анализа [10]. Однако для права такого технического определения недостаточно. Сам по себе большой объём информации ещё не превращает её в самостоятельный правовой феномен. Юридическое значение больших данных возникает тогда, когда их обработка влияет на права и законные интересы субъектов: потребителей, предпринимателей, операторов платформ, правообладателей, инвесторов, государства. Ранее в законопроекте № 571124-7 предлагалось использовать категорию «большие пользовательские данные», под которыми понималась совокупность не содержащей персональных данных информации о физических лицах и их поведении, собираемой из различных источников, в том числе из сети Интернет. Хотя данный законопроект не привёл к формированию завершённой правовой модели больших данных, сама постановка вопроса сохранила актуальность.

В правовом смысле большие данные можно определить как комплексный мега-информационный массив, отвечающий определённым технологическим признакам и выступающий самостоятельным объектом разноотраслевого правового регулирования в целях упорядочения его сбора, хранения, обработки, анализа, передачи, использования и защиты прав субъектов соответствующих отношений. Такое понимание позволяет избежать двух крайностей. С одной стороны, большие данные не следует рассматривать только как технический объект. С другой стороны, их нельзя механически сводить к объекту

гражданских прав. Большие данные могут затрагивать гражданско-правовые, предпринимательские, административные, финансовые, антимонопольные и публично-правовые отношения.

В экономической сфере большие данные становятся ресурсом, влияющим на конкурентоспособность хозяйствующих субъектов, инвестиционную привлекательность проектов и создание новых цифровых продуктов. Вместе с тем они несут риски: несанкционированный доступ, нарушение конфиденциальности, деанонимизация, дискриминация контрагентов, манипулирование рынком, усиление доминирующего положения цифровых платформ. Здесь проявляется связь регулирования больших данных с экономической безопасностью. Цифровая экономика даёт предпринимателям новые возможности, но усиливает зависимость бизнеса от информационной инфраструктуры, платформ и операторов данных. В исследованиях А. В. Минакова и А. Е. Суглобова подчёркивается, что развитие цифровой экономики регионов России невозможно рассматривать только как внедрение технологий; оно связано также с преодолением институциональных и инфраструктурных ограничений [16, с. 63–72].

Большие данные являются не только технологическим ресурсом, но и фактором рыночной власти. Субъект, обладающий доступом к значительным массивам данных о потребителях, ценах, спросе, логистике, поисковых запросах, платежах и поведении пользователей, получает конкурентные преимущества перед иными участниками рынка.

В условиях цифровых платформ это преимущество может усиливаться за счёт сетевых эффектов. Чем больше пользователей взаимодействует с платформой, тем больше данных она собирает; чем больше данных она обрабатывает, тем точнее становится её алгоритмическая модель; чем точнее модель, тем выше зависимость пользователей и предпринимателей от данной платформы. В результате появляется риск формирования цифровой монополии. В этой связи защита прав субъектов экономической деятельности должна включать не только гражданско-правовые способы восстановления нарушенного права, но и антимонопольные инструменты. Необходимо регулировать доступ к данным, прозрачность алгоритмов ранжирования, недискриминационные условия доступа предпринимателей к платформенной инфраструктуре, ответственность за злоупотребление доминирующим положением на цифровых рынках.

Экономическая безопасность в условиях цифровой трансформации также связана с развитием цифровых финансовых инструментов. Для субъектов малого и инновационного бизнеса

важное значение имеют венчурное финансирование, краудфандинг, краудинвестинг и иные платформенные способы привлечения капитала. А. В. Минаков рассматривает венчурное финансирование и краудфандинг как инструменты поддержки экономической безопасности субъектов малого инновационного бизнеса [17, с. 42–46]. Эти механизмы расширяют доступ предпринимателей к капиталу, но требуют правовых гарантий для инвесторов, владельцев платформ и получателей финансирования. В более широком контексте цифровая трансформация связана с задачами экономической безопасности государства. А. В. Минаков и С. Б. Лапина подчёркивают значение экономической безопасности в условиях внешних ограничений и санкционного давления [18, с. 305–312]. В цифровой сфере это означает необходимость защиты национальной информационной инфраструктуры, устойчивости цифровых сервисов, технологического суверенитета и прав субъектов экономической деятельности.

Заключение

Проведённый анализ позволяет сделать вывод о том, что цифровая трансформация существенно меняет содержание правовой охраны и защиты прав субъектов экономической деятельности. Традиционные способы защиты сохраняют своё значение, однако в цифровой среде они не всегда способны обеспечить эффективное восстановление нарушенного права.

Охрана прав субъектов экономической деятельности в цифровой среде должна пониматься как система превентивных, нормативных, организационных, технических и договорных мер, направленных на предупреждение нарушений. Защита прав связана с пресечением уже совершённого нарушения либо реальной угрозы его совершения, восстановлением нарушенного положения, компенсацией вреда, возмещением убытков и применением иных мер юридического воздействия.

Особое значение имеет разграничение понятий «охрана информации», «защита информации» и «защита прав субъектов информационных правоотношений». Действующее законодательство не всегда последовательно использует эти категории, что затрудняет правоприменение. Требуется дальнейшее уточнение Федерального закона «Об информации, информационных технологиях и о защите информации», законодательства о персональных данных, цифровых платформах, больших данных и электронно-цифровой коммерции.

Персональные данные требуют специального правового режима, но их определение должно учитывать не только формальный при-

знак связи с физическим лицом, но и технологическую возможность идентификации субъекта с использованием совокупности данных. Большие данные, в свою очередь, следует рассматривать как самостоятельный комплексный объект разнотраслевого правового регулирования, а не только как разновидность информации или цифровой актив. В условиях цифровой экономики защита прав субъектов экономической деятельности должна быть связана с обеспечением конкуренции, прозрачности цифровых платформ, недопущением злоупотребления доминирующим положением, устойчивостью информационной инфраструктуры и экономической безопасностью. Решение этих задач возможно только при согласованном развитии гражданского, предпринимательского, информационного, антимонопольного, финансового и административного законодательства.

Список литературы:

- [1] Конституция Российской Федерации: принята всенародным голосованием 12.12.1993; с изм., одобренными в ходе общероссийского голосования 01.07.2020 // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru/> (дата обращения: 07.06.2026).
- [2] Гражданский кодекс Российской Федерации. Часть первая от 30.11.1994 № 51-ФЗ // Собрание законодательства Российской Федерации. 1994. № 32. Ст. 3301.
- [3] Закон Российской Федерации от 07.02.1992 № 2300-1 «О защите прав потребителей» // Собрание законодательства Российской Федерации. 1996. № 3. Ст. 140.
- [4] Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платёжной системе» // Собрание законодательства Российской Федерации. 2011. № 27. Ст. 3872.
- [5] Федеральный закон от 29.07.2018 № 250-ФЗ «О внесении изменений в Закон Российской Федерации “О защите прав потребителей”» // Собрание законодательства Российской Федерации. 2018. № 31. Ст. 4839.
- [6] Постановление Конституционного Суда Российской Федерации от 17.02.2026 № 7-П // Конституционный Суд Российской Федерации. URL: <https://www.ksrf.ru/news/37787/> (дата обращения: 07.06.2026).
- [7] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448.
- [8] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3451.
- [9] Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // Собрание законодательства Российской Федерации. 2003. № 28. Ст. 2895.
- [10] ГОСТ Р ИСО/МЭК 20546–2021. Информационные технологии. Большие данные. Обзор и словарь. М.: Стандартинформ, 2021. URL: <https://docs.cntd.ru/document/1200180276> (дата обращения: 07.06.2026).
- [11] NIST Special Publication 800-53. Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology. URL: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final> (дата обращения: 07.06.2026).
- [12] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union // EUR-Lex. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng> (дата обращения: 07.06.2026).
- [13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data // EUR-Lex. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (дата обращения: 07.06.2026).
- [14] Чешин А. В. Экономико-правовые аспекты инновационной деятельности предприятий в условиях цифровой экономики // Инновационное развитие экономики России: вызовы и решения: материалы V Всероссийской научно-практической конференции, Москва, 20 апреля 2023 года. М.: Российский государственный университет правосудия, 2024. С. 426–433.
- [15] Дмитриева Л. В. Практики и подходы цифровой трансформации к совершенствованию регионального управления // Социальные и экономические системы. 2022. № 6–7(36). С. 176–197.
- [16] Минаков А. В., Суглобов А. Е. Проблемы развития цифровой экономики регионов России // Вопросы региональной экономики. 2022. № 4(53). С. 63–72.
- [17] Минаков А. В. Венчурное финансирование и краудфандинг как инструменты поддержки экономической безопасности субъектов малого инновационного бизнеса // Экономическое развитие России. 2018. Т. 25, № 8. С. 42–46.
- [18] Минаков А. В., Лапина С. Б. Обеспечение экономической безопасности государства в условиях санкций западных стран // Вестник экономической безопасности. 2021. № 2. С. 305–312. DOI: 10.24412/2414-3995-2021-2-305-312.
- [19] Карлеба В. А., Логинов Е. Л. Мониторинг оборота и легализации финансовых активов криминального происхождения: учебное пособие. М.: ЦОКР МВД России, 2007. 287 с.

[20] Обеспечение экономической безопасности реализации федеральных целевых программ: монография / А. Е. Городецкий, А. С. Зуева, М. М. Имамов [и др.]. М.: Московский университет МВД России им. В. Я. Кикотя, 2012. 204 с.

References:

[1] Constitution of the Russian Federation: adopted by popular vote on 12.12.1993; with amendments approved during the all-Russian vote on 01.07.2020 // Official Internet Portal of Legal Information. URL: <http://pravo.gov.ru/> (date of access: 07.06.2026).

[2] Civil Code of the Russian Federation. Part One of 30.11.1994 No. 51-FZ // Collected Legislation of the Russian Federation. 1994. No. 32. Art. 3301.

[3] Law of the Russian Federation of 07.02.1992 No. 2300-1 "On the Protection of Consumer Rights" // Collected Legislation of the Russian Federation. 1996. No. 3. Art. 140.

[4] Federal Law of June 27, 2011 No. 161-FZ "On the National Payment System" // Collected Legislation of the Russian Federation. 2011. No. 27. Article 3872.

[5] Federal Law of July 29, 2018 No. 250-FZ "On Amendments to the Law of the Russian Federation "On Protection of Consumer Rights"" // Collected Legislation of the Russian Federation. 2018. No. 31. Article 4839.

[6] Resolution of the Constitutional Court of the Russian Federation of February 17, 2026 No. 7-P // Constitutional Court of the Russian Federation. URL: <https://www.ksrf.ru/news/37787/> (date of access: June 7, 2026).

[7] Federal Law of July 27, 2006 No. 149-FZ "On Information, Information Technologies, and Information Protection" // Collected Legislation of the Russian Federation. 2006. No. 31. Article 3448.

[8] Federal Law of July 27, 2006 No. 152-FZ "On Personal Data" // Collected Legislation of the Russian Federation. 2006. No. 31. Article 3451.

[9] Federal Law of July 7, 2003 No. 126-FZ "On Communications" // Collected Legislation of the Russian Federation. 2003. No. 28. Article 2895.

[10] GOST R ISO/IEC 20546-2021. Information technology. Big data. Review and dictionary. M.: Standartinform, 2021. URL: <https://docs.cntd.ru/document/1200180276> (access date: 06/07/2026).

[11] NIST Special Publication 800-53. Security and Privacy Controls for Information Systems and

Organizations. National Institute of Standards and Technology. URL: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final> (accessed 06/07/2026).

[12] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union // EUR-Lex. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng> (accessed: 07.06.2026).

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data // EUR-Lex. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (accessed: 07.06.2026).

[14] Cheshin A. V. Economic and legal aspects of innovative activities of enterprises in the digital economy // Innovative development of the Russian economy: challenges and solutions: materials of the V All-Russian scientific and practical conference, Moscow, April 20, 2023. Moscow: Russian State University of Justice, 2024. pp. 426–433.

[15] Dmitrieva L. V. Practices and approaches of digital transformation to improving regional governance // Social and economic systems. 2022. No. 6–7(36). pp. 176–197.

[16] Minakov A. V., Suglobov A. E. Problems of developing the digital economy of Russian regions // Issues of regional economics. 2022. No. 4(53). pp. 63–72.

[17] Minakov A. V. Venture financing and crowdfunding as tools for supporting the economic security of small innovative businesses // Economic development of Russia. 2018. Vol. 25, No. 8. pp. 42–46.

[18] Minakov A. V., Lapina S. B. Ensuring the economic security of the state under sanctions from Western countries // Bulletin of Economic Security. 2021. No. 2. pp. 305–312. DOI: 10.24412/2414-3995-2021-2-305-312.

[19] Karleba V. A., Loginov E. L. Monitoring the turnover and legalization of financial assets of criminal origin: a tutorial. Moscow: TsOKR of the Ministry of Internal Affairs of Russia, 2007. 287 p.

[20] Ensuring economic security for the implementation of federal target programs: monograph / A. E. Gorodetsky, A. S. Zueva, M. M. Imamov [et al.]. Moscow: Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot, 2012. 204 p.

