

УДК 342.3

DOI: 10.19073/2658-7602-2026-23-2-192-203

EDN: AMYPPP



Оригинальная научная статья

Цифровая суверенность государства в российском праве

А. С. Агафонов 

Уральский государственный юридический университет им. В. Ф. Яковлева, Екатеринбург,
Российская Федерация

✉ aga.fonov@inbox.ru

Аннотация. Исследование посвящено цифровой суверенности (цифровому суверенитету) государства, которая выступает сегодня предметом междисциплинарной научной дискуссии. В настоящей статье утверждается, что единый подход к пониманию цифрового суверенитета в юридической науке пока что не сложился, в связи с чем выдвигается идея о том, что отечественная юридическая литература в контексте цифрового суверенитета формировалась в основном под влиянием технологических и программных вызовов (в условиях реализации принципа технологической обусловленности, который, как следует из идей И. Л. Бачило, В. А. Копылова, П. У. Кузнецова и А. Б. Венгерова, послужил одной из предпосылок формирования информационного права России). Анализируются различные отечественные подходы к пониманию цифрового суверенитета (П. В. Степанова, В. А. Никонова, А. А. Стрельцова и др.), выделяются их ключевые аспекты и преимущества. На основании данного анализа осуществляется критическое осмысление теории цифровой суверенности государства. В результате исследования положений действующего законодательства выявляются пробелы в правовой регламентации цифрового суверенитета, включая отсутствие его легального определения. Кроме того, в настоящей статье рассматриваются понятия «цифровые сети», «программное обеспечение» и «цифровые технологии» в контексте российской правовой действительности, в их содержании выделяются категории, напрямую относящиеся к цифровому суверенитету в рамках действующего отечественного законодательства. Констатируется, что цифровая суверенность государства не становилась ранее предметом публично-правовых диссертационных исследований, отечественными правоведами не предпринимались попытки моделирования цифровой суверенности государства посредством категориального ряда, включающего технологическую суверенность, цифровую суверенность и государственный суверенитет. В заключении исследования формулируется авторское определение понятия цифрового суверенитета, после чего констатируется, что соответствующее понимание, основанное на публично-правовых аспектах, может быть использовано в качестве основы для правовой регламентации понятия «цифровой суверенитет» в обозримом будущем, а также для построения теоретической модели цифровой суверенности государства.

Ключевые слова: цифровой суверенитет; технологический суверенитет; информационная безопасность; программное обеспечение; база данных; средства вычислительной техники; информационное право

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования: Агафонов А. С. Цифровая суверенность государства в российском праве // Сибирское юридическое обозрение. 2026. Т. 23, № 2. С. 192–203. DOI: <https://doi.org/10.19073/2658-7602-2026-23-2-192-203>. EDN: <https://elibrary.ru/amyppp>

Original scientific article

State Digital Sovereignty in Russian Law

A. S. Agafonov 

Ural State Law University named after V. F. Yakovlev, Yekaterinburg, Russian Federation

✉ aga.fonov@inbox.ru

Abstract. This study is devoted to the state's digital sovereignty, which is currently the subject of interdisciplinary scholarly debate. The article argues that no unified approach to the understanding of digital sovereignty has yet emerged in legal scholarship. In this regard, the Author advances the idea that Russian legal literature on digital sovereignty has developed primarily under the influence of technological and software-related challenges, in the context of the principle of technological conditioning. As follows from the ideas of I. L. Bachilo, V. A. Kopylov, P. U. Kuznetsov, and A. B. Vengerov, this principle served as one of the prerequisites for the formation of Russian information law. The article analyzes various Russian approaches to the understanding of digital sovereignty, including those of P. V. Stepanov, V. A. Nikonov, A. A. Streltsov, and others, and identifies their key aspects and advantages. On the basis of this analysis, the study offers a critical reconsideration of the theory of state digital sovereignty. An examination of current legislation reveals gaps in the legal regulation of digital sovereignty, including the absence of its statutory definition. In addition, the article considers the concepts of "digital networks," "software," and "digital technologies" in the context of Russian legal reality and identifies, within their content, categories directly related to digital sovereignty under current Russian legislation. The article states that state digital sovereignty has not previously been the subject of public-law dissertation research and that Russian legal scholars have not attempted to model state digital sovereignty through a categorical framework comprising technological sovereignty, digital sovereignty, and state sovereignty. In conclusion, the Author formulates a definition of digital sovereignty and states that this understanding, grounded in public-law aspects, may serve as a basis for the future legal regulation of the concept of "digital sovereignty," as well as for the construction of a theoretical model of state digital sovereignty.

Keywords: digital sovereignty; technological sovereignty; information security; software; database; computer hardware; information law

Conflict of interest. The Author declares no conflict of interest.

For citation: Agafonov A. S. State Digital Sovereignty in Russian Law. *Siberian Law Review*. 2026;23(2):192-203. DOI: <https://doi.org/10.19073/2658-7602-2026-23-2-192-203>. EDN: <https://elibrary.ru/amyppp> (In Russ.)

СОДЕРЖАНИЕ

I. Введение	193
II. Цифровой суверенитет в российском праве	194
III. Цифровой суверенитет в публично-правовом пространстве	197
IV. Два структурных элемента цифрового суверенитета	198
V. Заключение	201
Список литературы	202

I. ВВЕДЕНИЕ

В отечественной юридической науке активно развивается исследование цифровой суверенности государства (далее – цифро-

вой суверенитет). Этот феномен рассматривается в различных аспектах и контекстах.

В то же время единый подход к пониманию цифрового суверенитета

в юридической науке пока что не сложилось, что подтверждается позицией Т. А. Полякова, которая выдвигает идею о том, что рассматриваемое понятие не имеет правовой определенности, то есть точного юридического определения [1, с. 13].

Так, российские специалисты в области права рассматривают цифровой суверенитет как верховенство государственной власти в виртуальной среде, как элемент государственного суверенитета, как возможность государства самостоятельно определять степень и способы своего участия или неучастия в отношениях, связанных с применением цифровых технологий, для реализации собственных интересов, как верховенство и независимость государственной власти при формировании и реализации информационной политики в национальном сегменте и глобальном информационном пространстве, как право государства определять свою информационную политику и обеспечивать информационную и цифровую безопасность и т. д.

Для формирования представления о цифровом суверенитете в юридической науке необходимо обратиться к исследованиям российских ученых и рассмотреть специфику их исследовательских подходов.

Перед этим необходимо сделать одно важное уточнение. Указанные выше подходы в отечественной юридической литературе формировались в основном под влиянием технологических и программных вызовов (в условиях реализации принципа технологической обусловленности, восходящего к научно-техническому прогрессу, который, как следует из идей И. Л. Бачило, В. А. Копылова [2, с. 50], П. У. Кузнецова¹ и А. Б. Венгерова [3, с. 27], послужил одной из предпосылок формирования информационного права России в целом), а также угроз современной действительности, что подтверждается разобщи-

и несистематизированным характером исследуемой теории, раскрывающей содержание цифровой суверенности Российской Федерации.

На это обоснованно указывает и П. У. Кузнецов, отмечая, что в юридической науке еще не сформулированы теоретические основы цифровой формы государственного суверенитета: «Пока нет и единого выработанного понятия, отражающего логический терминологический ряд в части, касающейся обозначения государственного суверенитета в информационном пространстве и цифровой среде обитания человека» [4, с. 66].

Представляется целесообразным проанализировать некоторые существующие подходы к пониманию цифровой суверенности государства, выделить в них ключевые положения и особенности. При этом важно отметить, что в настоящем исследовании рассмотрены не все существующие подходы, а лишь те из них, анализ которых позволяет провести критическую оценку исследуемой теории, что поможет достичь цели настоящего исследования — определения правового содержания цифровой суверенности государства на основе исследования положений действующего законодательства в соответствующей области.

Необходимо отметить, что в настоящем исследовании термин «цифровой суверенитет» является сокращенной формой для обозначения категории «цифровая суверенность государства», понятия «суверенитет» и «суверенность» не отождествляются.

II. ЦИФРОВОЙ СУВЕРЕНИТЕТ В РОССИЙСКОМ ПРАВЕ

Исследуя различные аспекты цифрового суверенитета, в том числе правовое обеспечение и влияние на национальную безопасность, П. В. Степанов определяет данное понятие как верховенство

¹ См.: Кузнецов П. У. Информационное право : учеб. М. : Юстиция, 2019. 335 с.

государственной власти в виртуальной среде [5]. В рамках исследования национального сегмента информационно-телекоммуникационной сети Интернет, включающего домены, признанные национальными, ресурсы, размещенные на серверах в пределах страны, а также коммуникационные сети национальных операторов связи, П. В. Степанов стремится соотнести цифровые границы с государственными границами. Наряду с этим ученый, анализируя суверенитет как правовую категорию, утверждает, что национальные версии интернет-ресурсов должны подчиняться национальному законодательству соответствующего государства.

Данный подход характеризуется рядом существенных преимуществ. Во-первых, П. В. Степанов указывает на недостаточную разработанность в отечественной юридической науке вопросов, касающихся сущности и правовых средств обеспечения цифрового суверенитета, в то же время отмечая, что цифровой суверенитет сегодня выступает в качестве одной из центральных категорий государства и права. Во-вторых, П. В. Степанов раскрывает цифровой суверенитет государства через категорию «национальный сегмент Интернета», используя определение из Модельного закона Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств, устанавливающего основы регулирования Интернета². В-третьих, ученый предлагает концепцию решения территориальной проблемы суверенитета в цифровой среде.

В свою очередь В. А. Никонов, понимая цифровой суверенитет как возможность государства самостоятельно определять

степень и способы своего участия или неучастия в отношениях, связанных с применением цифровых технологий, для реализации собственных интересов, исследует ряд его аспектов (правовой, технологический, политический, управленческий, социальный, геополитический и др.) [6]. Например, в правовом аспекте автор акцентирует внимание на формировании и поддержании нормативно-правовой базы, регулирующей функционирование цифрового пространства и обеспечивающей независимость государства в данной сфере. С технологической точки зрения В. А. Никонов подчеркивает необходимость развития национальной цифровой инфраструктуры и внедрения передовых технологий, включая разработку национальных операционных систем и инструментов для работы с большими данными. В рамках информационной безопасности автор затрагивает вопросы защиты национальной информационной среды от внешних угроз, таких как кибератаки и цифровой шпионаж.

Достоинством данного подхода следует признать стремление к всестороннему рассмотрению цифрового суверенитета, что позволяет подчеркнуть значимость разработки национальных эффективных и конкурентоспособных программных продуктов в целях его обеспечения. Кроме того, представляется, что акцент на геополитическом аспекте сделан не случайно.

Примечательно, что в юридической науке имеется позиция, при которой цифровой суверенитет должен выступать основой построения различных международных систем. В частности, А. А. Стрельцов, утверждая, что цифровой суверенитет должен стать основой формирования системы международной

² См.: *Об основах регулирования Интернета* : модел. закон Межпарламент. Ассамблеи государств – участников Содружества Независимых Государств : принят на 36-м пленарном заседании МПА СНГ (постановление № 36-9 от 16 мая 2011 г.) // Межпарламент. Ассамблеи государств – участников Содружества Независимых Государств. 2011. URL: <https://iacis.ru/public/upload/files/1/278.pdf?ysclid=mpicrg9yh939094633> (дата обращения: 23.04.2026).

информационной безопасности, определяет его через реализацию государством своего суверенитета посредством упорядочения социального взаимодействия граждан в информационно-телекоммуникационной среде (далее – ИКТ-среда) и во всех сферах жизнедеятельности общества, а также через верховенство в вопросах применения норм права к реализуемым в ИКТ-среде социальным отношениям и защиту субъектов жизнедеятельности общества от угроз нарушения безопасности в информационном пространстве [7, с. 45–46].

В качестве достоинства такого подхода можно констатировать акцент А. А. Стрельцова на том, что цифровой суверенитет позволяет государству, во-первых, защищать свои национальные интересы в информационной сфере, во-вторых, контролировать и управлять информационно-коммуникационными технологиями в рамках своих границ, в-третьих, сохранять свою культурную идентичность.

В рамках подхода И. А. Петроченкова под цифровым суверенитетом понимается свойство субъектов информационно-правовых отношений самостоятельно или посредством кооперации осуществлять под контролем государства независимое воздействие на информацию и информационные технологии [8]. Ученым выдвигается идея, что соответствующее воздействие на информацию и информационные технологии должно среди прочего осуществляться посредством нормативного правового регулирования (как в пределах территориальных границ государства, так и в экстерриториальном и международном информационном пространстве). И. А. Петроченков включает в цифровой суверенитет категорию суверенитета данных, который подразделяется на слабый (касается защиты данных пользователей и цифровых прав частными компаниями) и сильный (связан с государ-

ственной политикой, направленной на национальную безопасность).

Преимуществом рассматриваемого подхода является акцент ученого на необходимости независимости государства от внешнего влияния в информационной сфере.

Г. Б. Романовский и О. В. Романовская рассматривают цифровой суверенитет как ответ на вызовы, связанные с трансграничностью цифрового мира, размывающей национальную юрисдикцию [9]. Авторы акцентируют, что цифровой суверенитет предполагает наличие развитой технологической инфраструктуры. Данная инфраструктура позволяет государству осуществлять контроль над цифровыми процессами и защищать свои интересы в информационном пространстве. Также Г. Б. Романовский и О. В. Романовская подчеркивают, что цифровой суверенитет возможен лишь при наличии соответствующей технологической базы. Цифровой суверенитет неразрывно связан с обеспечением информационной безопасности, включая защиту персональных данных. Особое значение придается технологической составляющей и правовому регулированию цифрового суверенитета. Без разработки и внедрения соответствующих программ, методов, инструментов и алгоритмов эффективное правовое регулирование данной сферы невозможно.

Признание ключевой роли технологий в контексте цифрового суверенитета является важным преимуществом данного подхода. Следует отметить и взаимосвязь между цифровым суверенитетом и информационной безопасностью, а также необходимость разработки и внедрения эффективной правовой регламентации.

Заслуживает внимания подход А. К. Жаровой, в рамках которого под цифровым суверенитетом понимается способность государства обеспечивать защиту информации в соответствии с действующим законодательством [10]. А. К. Жарова полагает, что концепция цифрового суверенитета

направлена на обеспечение защиты цифровой информации и предотвращение ее несанкционированного раскрытия при использовании иностранных технологий.

Анализ научной литературы по вопросам цифрового суверенитета свидетельствует об отсутствии фундаментальных монографий и диссертационных исследований по данной тематике в отечественной правовой науке. Цифровой суверенитет упоминается исключительно в отдельных научных публикациях и не стал предметом широких системных исследований.

В частности, исследуя информационно-правовой механизм обеспечения государственного суверенитета Российской Федерации, А. А. Ефремов разрабатывает авторское определение категории «государственный суверенитет в информационном пространстве», под которым понимает юридическое свойство (признак) государства как особого субъекта информационно-правовых отношений, осуществляющего их правовое регулирование как в пределах своей территории (внутригосударственное информационное пространство), экстерриториальных режимов, так и при участии в международно-правовом регулировании (глобальное и региональные информационные пространства)³.

III. ЦИТРОВЫЙ СУВЕРЕНИТЕТ В ПУБЛИЧНО-ПРАВОВОМ ПРОСТРАНСТВЕ

Анализ существующих отечественных концепций цифрового суверенитета государства дает возможность для их критического осмысления. Важно отметить, что соответствующая критическая оценка направлена не на опровержение или умаление научных результатов, полученных специалистами отечественной юридической науки, а на обозначение вопросов цифровой суверенности государства, ко-

торые до сих пор не получили теоретической конкретизации.

Так, в отечественной теории цифровой суверенности государства не сформулировано четкое понятие, раскрывающее содержание категории «цифровой суверенитет». Существующие подходы имеют общие черты лишь в отдельных аспектах (к примеру, в рамках констатации того, что цифровой суверенитет выступает гарантией национальной безопасности государства). На сегодняшний день такое положение дел создает неопределенность в понимании содержания цифрового суверенитета и, следовательно, объема исследуемого понятия.

Цифровой суверенитет необходимо рассматривать с точки зрения самостоятельного понятия, которое взаимосвязано и взаимозависимо с технологическим суверенитетом и государственным суверенитетом, но не входит в их содержание, имея собственное наполнение (объем), как и технологический суверенитет и государственный суверенитет представляют собой отдельные понятия, выступают самостоятельными категориями, имеющими собственную правовую регламентацию, и не могут входить в содержание цифрового суверенитета.

Кроме того, в отечественной теории остается не определённым место института цифровой суверенности государства в системе информационного права.

Анализ положений действующего законодательства позволяет констатировать, что в части правовой регламентации цифровой суверенитет лишь упоминается в некоторых правовых актах, при этом легальное определение в законодательстве Российской Федерации отсутствует.

Так, в Распоряжении Правительства Российской Федерации от 25 июня 2022 г. № 1693-р «Об утверждении комплексной программы развития авиационной отрасли Российской Федерации до 2030 года»

³ См: *Ефремов А. А.* Информационно-правовой механизм обеспечения государственного суверенитета Российской Федерации : дис. ... д-ра юрид. наук. М., 2021. 418 с.

упоминается понятие «цифровой суверенитет гражданской авиации»⁴, в Приказе Минпромторга России от 29 мая 2019 г. № 1869 «Об утверждении концепции создания российского сегмента евразийской сети промышленной кооперации и субконтрактации» используется термин «цифровой суверенитет по защите информации»⁵.

Принимая во внимание перманентный характер связи между цифровым суверенитетом и технологическим суверенитетом, а также легальное определение последнего, представляется, что основой для формирования термина, отражающего содержание цифрового суверенитета, может служить дефиниция (по аналогии с подходом П. В. Степанова), закрепленная в ст. 2 Постановления № 55-9 Межпарламентской Ассамблеи государств – участников СНГ «О модельном законе “О цифровой трансформации отраслей промышленности государств – участников СНГ”»⁶, где под цифровым суверенитетом понимается способность государства самостоятельно создавать и использовать в различных сферах деятельности собственные цифровые сети, программное обеспечение и цифровые технологии, которые являются критически важными для обеспечения благосостояния населения государства, его национальной безопасности и конкурентоспособности национальной экономики, а также возможность государства определять и проводить самостоятельную внутреннюю и внешнюю политику в цифровом пространстве.

IV. ДВА СТРУКТУРНЫХ ЭЛЕМЕНТА ЦИФРОВОГО СУВЕРЕНИТЕТА

Исходя из анализа содержания представленной дефиниции, можно выделить ряд признаков данного понятия. Понятие цифрового суверенитета (по аналогии

с понятием технологического суверенитета) охватывает не столько цифровые сети, программное обеспечение и цифровые технологии, сколько две способности государства в данной области. Первая способность государства выражается в самостоятельном создании и использовании в различных сферах деятельности собственных цифровых сетей, программного обеспечения и цифровых технологий, которые имеют критическое значение для обеспечения благосостояния населения государства, его национальной безопасности и конкурентоспособности национальной экономики. Вторая способность государства выражается в определении и проведении самостоятельной внутренней и внешней политики в цифровом пространстве.

Исследуя первую способность государства в рамках цифрового суверенитета, необходимо провести анализ действующего отечественного правового регулирования в области цифровых сетей, программного обеспечения и цифровых технологий.

Так, в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»⁷ (далее – ФЗ № 149-ФЗ) не используется термин «цифровая сеть». Вместо этого используется понятие «информационно-телекоммуникационная сеть», под которой понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (ст. 2 ФЗ № 149-ФЗ). Использование информационно-телекоммуникационных сетей на территории Российской Федерации регламентируется ст. 15 ФЗ № 149-ФЗ.

Рассматривая легальную дефиницию «информационно-телекоммуникационная

⁴ Доступ из СПС «КонсультантПлюс».

⁵ Доступ из СПС «КонсультантПлюс».

⁶ Доступ из СПС «КонсультантПлюс».

⁷ Доступ из СПС «КонсультантПлюс».

сеть» можно выделить три содержательных признака:

1) речь идет о технологической системе, содержание которой в ФЗ № 149-ФЗ не раскрывается. Из буквального толкования следует, что имеется в виду именно система, основное место в которой занимают технологии, что, в свою очередь, связано с технологическим суверенитетом;

2) назначение технологической системы проявляется в передаче по линиям связи информации. Линиями связи при этом выступают линии передачи, физические цепи и линейно-кабельные сооружения связи, что следует из ст. 2 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»⁸, в том числе с соблюдением которого, по смыслу ст. 15 ФЗ № 149-ФЗ, осуществляется использование информационно-телекоммуникационных сетей на территории Российской Федерации, что также относится к технологическому суверенитету;

3) доступ к технологической системе осуществляется с использованием средств вычислительной техники.

Содержание понятия «средства вычислительной техники» раскрыто в преамбуле руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»⁹, в которой под средствами вычислительной техники понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем. Указанные программные и технические (не технологические) элементы, в свою очередь, относятся к цифровому суверенитету, поскольку они обеспечивают функционирование систем обработки данных, то есть технологий.

Следовательно, разбор легальной дефиниции «информационно-телекоммуникационная сеть» на содержательные элементы позволяет отнести к цифровому суверенитету лишь средства вычислительной техники, с помощью которых обеспечивается (осуществляется) доступ к технологическим системам, предназначенным для передачи информации по линиям связи.

По результатам анализа правового регулирования в области программного обеспечения можно констатировать, что в базовом отечественном нормативном правовом акте в сфере информации, информационных технологий и защиты информации не используется понятие «программное обеспечение». Вместо этого используется понятие «программа для электронной вычислительной машины» (далее – программа для ЭВМ), которое также используется в гражданском законодательстве Российской Федерации. В статье 1261 Гражданского кодекса Российской Федерации (далее – ГК РФ) содержится определение программы для ЭВМ, под которой понимается представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

Кроме того, соответствующее определение используется и в рамках уголовного законодательства Российской Федерации, а именно в гл. 28 (ст.ст. 273, 274.1) Уголовного кодекса Российской Федерации, что прямо следует из п. 4 Постановления Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах

⁸ Доступ из СПС «КонсультантПлюс».

⁹ См.: *Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации* : утв. Решением Гостехкомиссии России 30 марта 1992 г. Доступ из СПС «КонсультантПлюс».

судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»»¹⁰.

Вызывает интерес, что аббревиатуру ПО (программное обеспечение) можно найти в п. 3.47 ГОСТ Р 51904-2002 «Государственный стандарт Российской Федерации. Программное обеспечение встроенных систем. Общие требования к разработке и документированию»¹¹ и п. 2 табл. 1 ГОСТ 19781-90 «Государственный стандарт Союза ССР. Обеспечение систем обработки информации программное. Термины и определения»¹². Так, в указанных документах под программным обеспечением понимается совокупность программ и программных документов, необходимых для эксплуатации этих программ, то есть тех же данных и материалов, полученных в ходе разработки, которые определены ст. 1261 ГК РФ, что позволяет сделать вывод об идентичности рассматриваемых понятий с точки зрения некоторых содержательных элементов.

В то же время дефиниция «программа для ЭВМ» по своему содержанию шире, так как включает в себя еще и порождаемые программой для ЭВМ аудиовизуальные отображения.

Фундаментальной нормой права, регулирующей общественные отношения в сфере программ для ЭВМ, является ст. 12.1 ФЗ № 149-ФЗ, которой предусмотрено создание Единого реестра российских программ для электронных вычислительных машин и баз данных (далее – Реестр российского программного обеспечения). Данный реестр направлен,

во-первых, на расширение использования российских программ для электронных вычислительных машин и баз данных, во-вторых, на подтверждение их происхождения из Российской Федерации, в-третьих, на оказание правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки. Необходимо учитывать, что наряду с понятием «программа для ЭВМ» в Реестре российского программного обеспечения используется и дефиниция «база данных», под которой понимается представленная в объективной форме совокупность самостоятельных материалов, систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью ЭВМ (ч. 2 ст. 1260 ГК РФ).

Таким образом, в содержание цифрового суверенитета Российской Федерации, в соответствии с положениями российского законодательства, должны включаться понятия «программа для ЭВМ» и «база данных», а не «программное обеспечение».

Далее констатируем, что в ФЗ № 149-ФЗ не используется понятие «цифровые технологии». В то же время указанная дефиниция используется в рамках национальной программы «Цифровая экономика Российской Федерации»¹³ федерального проекта «Цифровые технологии». Ключевой целью названного федерального проекта является обеспечение технологической независимости государства и возможности коммерциализации отечественных исследований и разработок, а также ускорение технологического развития российских компаний и обеспечение конкурентоспособности разрабатываемых ими продуктов и решений на глобальном

¹⁰ Доступ из СПС «КонсультантПлюс».

¹¹ Доступ из СПС «КонсультантПлюс».

¹² Доступ из СПС «КонсультантПлюс».

¹³ См.: *Паспорт* национального проекта «Национальная программа «Цифровая экономика Российской Федерации» : утв. президиумом Совета при Президенте Рос. Федерации по стратег. развитию и нац. проектам, протокол от 4 июня 2019 г. № 7. Доступ из СПС «КонсультантПлюс».

рынке¹⁴. Проект направлен на технологический суверенитет, а не на цифровой, поскольку речь идет (в плане цели) именно о технологической самостоятельности государства.

Одновременно дефиниция «цифровые технологии» имеет место в ГОСТ Р 33.505-2003, где под ними понимаются технологии, использующие электронно-вычислительную аппаратуру для записи кодовых импульсов в определенной последовательности и с определенной частотой¹⁵.

Следовательно, в рамках цифровых технологий речь идет именно о технологическом суверенитете, а технологическом.

Таким образом, в отечественном праве в содержание цифрового суверенитета должны входить не цифровые сети, программное обеспечение и цифровые технологии, а электронно-вычислительные средства, программы для ЭВМ и базы данных.

Отдельно следует отметить, что характерной особенностью указанных понятий выступает их критическая важность для обеспечения благосостояния населения государства, его национальной безопасности и конкурентоспособности национальной экономики, что объясняется приведенными выше положениями.

V. ЗАКЛЮЧЕНИЕ

Системный анализ подходов к пониманию цифровой суверенности государства в отечественной литературе и их критическая оценка позволяют сделать вывод о том, что в отечественной литературе не сформировался единый подход к пониманию цифровой суверенности государства. Цифровая суверенность государства ранее не исследовалась на уровне публично-правовых дис-

сертационных исследований, отечественными правоведами не осуществлялось попыток ее моделирования через категориальный ряд, включающий технологическую суверенность, цифровую суверенность и государственный суверенитет.

Кроме того, в отечественной теории цифровой суверенности государства не выработано четкое понятие, раскрывающее содержание категориального (терминологического) ряда, а также не определено место цифровой суверенности государства в системе информационного права как отрасли научного знания.

На основании проведенного исследования положений отечественного законодательства можно предложить обоснованное с точки зрения отечественного права понимание цифровой суверенности государства (цифрового суверенитета) как способности государства самостоятельно создавать и использовать в различных сферах деятельности собственные средства вычислительной техники, программы для электронных вычислительных машин и базы данных, которые являются критически важными для обеспечения благосостояния населения государства, его национальной безопасности и конкурентоспособности национальной экономики, а также возможность государства определять и проводить самостоятельную внутреннюю и внешнюю политику в информационной сфере.

Соответствующее понимание, основанное на публично-правовых аспектах, может быть использовано в качестве основы для правовой регламентации легальной дефиниции «цифровой суверенитет» в обозримом будущем, а также для построения теоретической модели цифровой суверенности государства.

¹⁴ См.: *Паспорт* федерального проекта «Цифровые технологии»: утв. президиумом Правительств. комиссии по цифровому развитию, использованию информ. технологий для улучшения качества жизни и условий ведения предприним. деятельности, протокол от 28 мая 2019 г. № 9. Доступ из СПС «КонсультантПлюс».

¹⁵ См.: *ГОСТ Р 33.505-2003*. Государственный стандарт Российской Федерации. Единый российский страховой фонд документации. Порядок создания страхового фонда документации, являющейся национальным научным, культурным и историческим наследием: принят и введен в действие Постановлением Госстандарта России от 29 июля 2003 г. № 255-ст. Доступ из СПС «КонсультантПлюс».

Список литературы

1. Полякова Т. А. Правовое обеспечение национального суверенитета в информационном пространстве в условиях цифровой трансформации государства // Седьмые Бачиловские чтения : сб. ст. участников междунар. науч.-практ. конф. / отв. ред.: Т. А. Полякова, А. В. Минбалеев, В. Б. Наумов, Н. А. Троян, А. А. Смирнов. М. : Ин-т гос-ва и права РАН, 2024. С. 9–18.
2. Бачило И. Л., Копылов В. А. Есть ли основания для создания отрасли «Информационное право» // Информационное общество. 1999. № 6. С. 49–50.
3. Венгеров А. Б. Право и информация в условиях автоматизации управления: теоретические вопросы. М. : Юрид. лит., 1978. 206 с.
4. Кузнецов П. У. Методологические особенности цифрового состояния государственного суверенитета // Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности : сб. докл. участников XVIII междунар. форума (Москва, 16–18 сент. 2024 г.). М. : Нац. Ассоц. междунар. информ. безопасности, 2024. С. 66–70.
5. Степанов П. В. Подходы к пониманию цифрового суверенитета России // Журнал российского права. 2024. Т. 28, № 4. С. 37–51. DOI: <https://doi.org/10.61205/jrp.2024.4.1>
6. Цифровой суверенитет современного государства: содержание и структурные компоненты (по материалам экспертного исследования) / В. А. Никонов, А. С. Воронов, В. А. Сажина, С. В. Володенков, М. В. Рыбакова // Вестник Томского государственного университета. Философия. Социология. Политология. 2021. № 60. С. 206–216. DOI: <https://doi.org/10.17223/1998863X/60/18>
7. Стрельцов А. А. Цифровой суверенитет как основа формирования системы международной информационной безопасности // Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности : сб. докл. участников XVIII междунар. форума (Москва, 16–18 сент. 2024 г.). М. : Нац. Ассоц. междунар. информ. безопасности, 2024. С. 44–46.
8. Петроченков И. А. К вопросу о концепции цифрового суверенитета // Конституционное и муниципальное право. 2022. № 7. С. 69–73. DOI: <https://doi.org/10.18572/1812-3767-2022-7-69-73>
9. Романовский Г. Б., Романовская О. В. О цифровом суверенитете // Конституционное и муниципальное право. 2022. № 9. С. 25–31. DOI: <https://doi.org/10.18572/1812-3767-2022-9-25-31>
10. Жарова А. К. Обеспечение информационного суверенитета Российской Федерации // Юрист. 2021. № 11. С. 28–33. DOI: <https://doi.org/10.18572/1812-3929-2021-11-28-33>

References

1. Polyakova T. A. Legal Support of National Sovereignty in the Information Space: in the Context of the Digital Transformation of the State. In: Polyakova T. A., Minbaleev A. V., Naumov V. B., Troyan N. A., Smirnov A. A. (Eds.). *The Seventh Bachilov Readings*. Moscow: Institute of State and Law of the Russian Academy of Sciences Publ.; 2024. P. 9–18. (In Russ.)
2. Bachilo I. L., Kopylov V. A. Are There Grounds for Establishing Information Law as a Branch of Law? *Information Society*. 1999;6:49–50. (In Russ.)
3. Vengerov A. B. *Law and Information in the Context of Automated Governance: Theoretical Issues*. Moscow: Yuridicheskaya literatura Publ.; 1978. 206 p. (In Russ.)
4. Kuznetsov P. U. Methodological Features of the Digital State of Sovereignty. In: *Proceedings of the XVIII International Forum “Partnership between the State, Business, and Civil Society in Ensuring International Information Security.”* Moscow, 2024. P. 67–70. (In Russ.)
5. Stepanov P. V. Approaches to Understanding Russia’s Digital Sovereignty. *Journal of Russian Law*. 2024;28(4):37–51. DOI: <https://doi.org/10.61205/jrp.2024.4.1> (In Russ.)
6. Nikonov V. A., Voronov A. S., Sazhina V. A., Volodenkov S. V., Rybakova M. V. Digital Sovereignty of a Modern State: Content and Structural Components (Based On Expert Research). *Tomsk State University Journal of Philosophy, Sociology and Political Science*. 2021;60:206–216. DOI: <https://doi.org/10.17223/1998863X/60/18> (In Russ.)
7. Strel'tsov A. A. Digital Sovereignty as a Basis for the Formation of an International Information Security System. In: *Proceedings of the XVIII International Forum “Partnership between the State, Business, and Civil Society in Ensuring International Information Security.”* Moscow, 2024. P. 44–46. (In Russ.)
8. Petrochenkov I. A. On the Issue of the Concept of Digital Sovereignty. *Constitutional and Municipal Law*. 2022;7:69–73. DOI: <https://doi.org/10.18572/1812-3767-2022-7-69-73> (In Russ.)
9. Romanovsky G. B., Romanovskaya O. V. On Digital Sovereignty. *Constitutional and Municipal Law*. 2022;9:25–31. DOI: <https://doi.org/10.18572/1812-3767-2022-9-25-31> (In Russ.)
10. Zharova A. K. Ensuring the Information Sovereignty of the Russian Federation. *Jurist*. 2021;11:28–33. DOI: <https://doi.org/10.18572/1812-3929-2021-11-28-33> (In Russ.)

ИНФОРМАЦИЯ ОБ АВТОРЕ

Андрей Сергеевич Агафонов, аспирант кафедры информационного права Уральского государственного юридического университета им. В. Ф. Яковлева (ул. Комсомольская, 21, Екатеринбург, 620066, Российская Федерация); ORCID: <https://orcid.org/0009-0005-2888-7955>; e-mail: aga.fonov@inbox.ru

ABOUT THE AUTHOR

Andrey S. Agafonov, postgraduate student of the Department of Information Law at the Ural State Law University named after V. F. Yakovlev (21 Komsomolskaya st., Yekaterinburg, 620066, Russian Federation); ORCID: <https://orcid.org/0009-0005-2888-7955>; e-mail: aga.fonov@inbox.ru

Поступила | Received
01.08.2025

Поступила после рецензирования
и доработки | Revised
27.08.2025

Принята к публикации | Accepted
26.09.2025