

DOI: <https://doi.org/10.60797/IRJ.2026.167.92> EDN: HZVDJR**СТАНОВЛЕНИЕ ЦИФРОВОГО СУВЕРЕНИТЕТА РОССИИ И ПРОБЛЕМА ИДЕНТИФИКАЦИИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ**

Научная статья

**Гапонов А.А.<sup>1,\*</sup>, Кузьмин И.М.<sup>2</sup>**<sup>1</sup> ORCID : 0009-0000-7335-1117;<sup>2</sup> ORCID : 0009-0009-3931-7607;<sup>1,2</sup> Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Российская Федерация

\* Корреспондирующий автор (gaponov.2013[at]bk.ru)

Предложена: 15.04.2026; Принята: 05.05.2026; Опубликовано: 18.05.2026

**Аннотация**

В статье характеризуется процесс формирования цифрового суверенитета Российской Федерации в контексте трансформации подходов к государственному управлению информационным пространством. Анализируется эволюция нормативно-правового регулирования от Закона о «суверенном интернете» 2019 г. до Федерального закона № 156-ФЗ «О создании многофункционального сервиса обмена информацией» (2025 г.). Особое внимание уделяется взаимосвязи между обеспечением цифрового суверенитета и решением проблемы идентификации физических лиц в цифровой среде, включая правовые аспекты использования биометрических персональных данных. На примере правового режима национального мессенджера «МАХ» рассматриваются конкретные меры государственной политики по легализации коммуникационной инфраструктуры, а также выявляются правовые коллизии и недостатки действующего регулирования.

**Ключевые слова:** цифровой суверенитет, информационное пространство, идентификация, аутентификация, национальный мессенджер, МАХ, информационная безопасность.

**THE DEVELOPMENT OF RUSSIA'S DIGITAL SOVEREIGNTY AND THE ISSUE OF IDENTIFICATION IN THE DIGITAL SPHERE**

Research article

**Gaponov A.A.<sup>1,\*</sup>, Kuzmin I.M.<sup>2</sup>**<sup>1</sup> ORCID : 0009-0000-7335-1117;<sup>2</sup> ORCID : 0009-0009-3931-7607;<sup>1,2</sup> Vladimir State University named after Alexander Grigoryevich and Nikolai Grigoryevich Stoletov, Vladimir, Russian Federation

\* Corresponding author (gaponov.2013[at]bk.ru)

Suggested: 15.04.2026; Accepted: 05.05.2026; Published: 18.05.2026

**Abstract**

The article examines the process of establishing the Russian Federation's digital sovereignty in the context of changing approaches to state governance of the information space. The evolution of regulatory and legal frameworks from the 2019 "Sovereign Internet" Act to Federal Law No. 156-FZ "On the Creation of a Multifunctional Information Exchange Service" (2025) is analysed. Particular attention is paid to the interconnection between ensuring digital sovereignty and resolving the issue of identifying individuals in the digital environment, including the legal aspects of using biometric personal data. On the example of the legal regime of the national messaging app "MAX", specific state policy measures for the legalisation of the communications infrastructure are examined, and legal conflicts and shortcomings in the current regulatory framework are identified.

**Keywords:** digital sovereignty, information space, identification, authentication, national messaging app, MAX, information security.

**Введение**

Три десятилетия назад Джон Перри Барлоу в «Декларации независимости киберпространства» утверждал невозможность распространения государственного суверенитета на цифровую среду. Однако в международной практике и научной литературе закрепилось иное понимание: суверенитет государства выходит за пределы физической территории и охватывает внутритерриториальные пространства, включая цифровое [1].

Актуальность исследования обусловлена рядом факторов. Во-первых, глобальная цифровая трансформация породила новые вызовы суверенитету: зависимость от иностранных платформ, трансграничное движение данных без должного контроля, а также киберугрозы со стороны различных акторов. Во-вторых, конституционные поправки 2020 года расширили сферу ведения Российской Федерации, включив в неё информационные технологии и оборот цифровых данных, что стало основой для формирования концепции цифрового суверенитета. В-третьих, после 2022



года вопросы цифрового суверенитета приобрели стратегическое значение и были закреплены в Стратегии национальной безопасности Российской Федерации как часть приоритета информационной безопасности.

Цель настоящей статьи — выявить взаимосвязь между становлением цифрового суверенитета России и решением проблемы идентификации физических лиц в информационном пространстве, а также оценить эффективность конкретных правовых и организационных мер, реализуемых в данной сфере.

### Методы и принципы исследования

Теоретической основой работы послужил конструктивный подход к пониманию суверенитета как социальной идеи, связывающей территорию, общество и власть и формирующейся в результате действий влиятельных агентов внутри государства (Т. Бирстекер, К. Вебер). В отношении цифрового суверенитета данный подход дополняет традиционную триаду технологическим измерением. В работе использованы следующие методы: формально-юридический (анализ нормативных правовых актов), сравнительно-правовой (сопоставление подходов к регулированию идентификации в различных правовых системах), конкретно-социологический (анализ правоприменительной практики, включая судебные споры), а также метод системного анализа (выявление взаимосвязей между элементами правового механизма обеспечения цифрового суверенитета).

### Основные результаты

В российской правовой доктрине общепризнанное определение цифрового (информационного) суверенитета находится на этапе становления. Как отмечают С. В. Нарутто, С. Ю. Колмаков и И. М. Япрынец, юридическая доктрина не выработала единого комплексного подхода к пониманию цифрового суверенитета, которое охватывало бы всю специфику субъектов и особенностей правоотношений в информационно-коммуникационной сфере [2]. Но стоит отметить выработанный А. А. Ефремовым подход к пониманию государственного суверенитета в информационном пространстве, в рамках которого государственный суверенитет рассматривается как 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]. Данный подход обладает существенной теоретической значимостью, поскольку отражает комплексный характер информационных отношений и подчеркивает роль государства в регулировании цифровой среды на национальном и международном уровнях.

Вместе с тем в рамках настоящего исследования представляется более обоснованным использование категории «цифровой суверенитет». В наиболее общем виде цифровой суверенитет понимается как способность государства контролировать свои цифровые данные и информацию, обеспечивать безопасность и защиту цифровых технологий и инфраструктуры, а также самостоятельно определять правовой режим функционирования национального сегмента сети Интернет. Это обусловлено тем, что понятие информационного суверенитета носит достаточно широкий характер и охватывает весь спектр информационных отношений, тогда как цифровой суверенитет акцентирует внимание именно на технологической составляющей современной цифровой среды: данных, цифровой инфраструктуре, программных решениях, сетевых платформах и функционировании сети Интернет. В доктрине выделяются следующие компоненты, с которыми связывается гарантирование информационной безопасности государства: поисковая система, социальные сети, операционная система и программное обеспечение, микроэлектроника, сетевое оборудование, национальный сегмент сети Интернет, платежная система, собственные средства защиты, криптографические алгоритмы и протоколы. При этом, как отмечает Е. В. Алферова, в условиях цифровизации сохраняется классическое понимание государственного суверенитета как неотъемлемого свойства государства, а формирование концепции цифрового суверенитета требует его доктринального осмысления и правового закрепления [4].

В Стратегии национальной безопасности РФ развитие безопасного информационного пространства признано одним из национальных интересов, а информационная безопасность — стратегическим национальным приоритетом [5]. В Доктрине информационной безопасности РФ целями обеспечения информационной безопасности государства объявлялись достижение и поддержание информационного суверенитета [6].

Проблема идентификации физических лиц в цифровом пространстве напрямую связана с реализацией цифрового суверенитета по двум основаниям. Во-первых, без эффективных механизмов установления личности участников правоотношений государство не способно полноценно защищать права граждан в цифровой среде. Во-вторых, контроль над процедурами идентификации и аутентификации обеспечивает возможность противодействия анонимным киберугрозам, включая мошенничество, распространение противоправного контента и кибератаки.

Со слов Д. С. Провалинского, в условиях развернувшейся с 24 февраля 2022 г. информационной войны в цифровом пространстве против Российской Федерации государство вынужденно прибегло к блокировке ряда зарубежных интернет-ресурсов (Instagram и Facebook), нарушавших как собственные правила платформ, так и российское законодательство [7].

В данном контексте, как указывает С. Д. Ковалев, мессенджеры перестали быть лишь средством общения, трансформировавшись в инструмент формирования общественного влияния, что обусловило поддержанный на государственном уровне курс на укрепление цифрового суверенитета и его логическое продолжение — создание национального сервиса обмена информацией, закреплённое Федеральным законом от 24 июня 2025 г. № 156-ФЗ, направленным на повышение доступности сервисов и обеспечение конфиденциальности передаваемой информации [8], [9].

В развитие этих положений Распоряжением Правительства РФ от 12.07.2025 № 1880-р закреплено, что создание и функционирование сервиса возложены на ООО «Коммуникационная платформа» — дочернюю структуру VK,

обладающую исключительными правами на программу «Цифровая платформа МАХ» [10]. Таким образом, национальный мессенджер «МАХ» был легализован в качестве государственно-частного проекта с особым правовым статусом.

Следует отметить, что в средствах массовой информации и иных источниках встречается использование русскоязычного написания наименования мессенджера — «Макс». Однако подобное обозначение представляется не вполне корректным, поскольку фактически является не официальным наименованием сервиса, а его русскоязычной транслитерацией. В связи с этим в рамках настоящей статьи используется оригинальное наименование «МАХ», что позволяет обеспечить точность терминологии и единообразие научного изложения. Подобная позиция об использовании только англоязычного наименования приложения без транслитерации обуславливается подходом государственных органов к наименованию мессенджера в нормативных правовых актах, а также отсутствием зарегистрированного товарного знака на использование наименования мессенджера в русской транслитерации «Макс».

Практика применения законодательства о национальном мессенджере выявила ряд правовых проблем, которые нашли отражение в судебных спорах и обращениях в контрольно-надзорные органы.

Первая группа споров связана с антимонопольным регулированием. В декабре 2025 года депутат Государственной Думы Михаил Матвеев направил запрос в Федеральная антимонопольная служба о «агрессивном продвижении» мессенджера МАХ с использованием административного ресурса. Указывались признаки нарушений конкуренции: использование термина «государственный мессенджер» для частного продукта, создание технических преимуществ (включение в «белый список»), а также его приоритетная интеграция в государственные сервисы.

Дополнительную дискуссию вызвали сообщения в средствах массовой информации о фактическом принуждении работников бюджетной сферы и обучающихся к использованию МАХ, включая обязательную регистрацию и подписку на отдельные каналы без проведения необходимого обучения пользователей и разъяснения порядка работы с сервисом. При этом в ряде случаев речь шла не только об организационных мерах, но и о возможном нарушении законодательства. Так, по информации, находившейся в распоряжении депутата, Кунцевская межрайонная прокуратура установила нарушения законодательства в одной из школ Москвы при принятии локального акта об обязательном использовании мессенджера. В результате прокурорского реагирования директору образовательного учреждения был принесен протест, а сама ситуация была связана с нарушением положений Федерального закона «Об образовании в Российской Федерации», регулирующих права обучающихся и порядок организации образовательного процесса.

Указанные обстоятельства позволяют рассматривать проблему не только через призму антимонопольного регулирования, но и в контексте допустимых пределов цифровизации публичной сферы, соблюдения принципа добровольности использования цифровых сервисов, а также обеспечения цифровой грамотности пользователей при внедрении новых платформенных решений. Одновременно сама ситуация демонстрирует риски формирования преимущественного положения отдельных цифровых платформ вследствие их тесной интеграции с государственными структурами и сервисами, что в условиях монополии может в будущем привести к деградации цифровых институтов и технологического отставания государства.

Обращаясь к зарубежному опыту создания национальных мессенджеров, следует уделить внимание китайскому WeChat, японскому LINE и корейскому KakaoTalk. Их развитие демонстрирует общую закономерность: данные сервисы изначально возникали как коммерческие продукты и распространялись в условиях рыночной конкуренции, без их прямого создания или обязательного внедрения со стороны государства. Массовое использование этих платформ сформировалось естественным образом за счёт удобства функционала, качества сервисов и высокой адаптации к повседневным потребностям пользователей.

Лишь после того, как указанные мессенджеры заняли устойчивые позиции на рынке и фактически стали основными средствами цифровой коммуникации, государства начали их поддерживать и интегрировать в систему публичных цифровых сервисов. При этом характерной особенностью зарубежной практики является отсутствие исходного административного вытеснения конкурирующих решений или законодательного закрепления монопольного положения отдельных платформ.

Такой подход позволяет развивать мессенджеры как сильные рыночные продукты, конкурентоспособность которых формируется за счёт инновационности, качества и пользовательского доверия. В результате их широкое распространение и последующая государственная поддержка выступают следствием естественного рыночного отбора, а не административного навязывания или нормативного закрепления обязательности использования. Это позволяет странам с таким подходом быть независимыми от иностранных мессенджеров, и в то же время сильный цифровой продукт удовлетворяет потребности свободного рынка.

Вторая группа споров связана с использованием МАХ в преступных целях, что ставит под сомнение эффективность механизмов идентификации. С апреля 2025 года зафиксировано 162 случая мошенничества с его использованием. В сентябре 2025 года ФСБ России сообщила о задержании подозреваемых по делам о мошенничестве (ст. 159 УК РФ). Хотя число таких преступлений ниже, чем в WhatsApp и Telegram, сам факт их наличия указывает на недостаточную эффективность идентификации через национальный мессенджер.

Третья группа касается распространения недостоверной информации о мессенджере. Само наличие мифов о критических уязвимостях мессенджера свидетельствует о недостаточной информационной работе и, что более важно, о правовой неопределенности: законодательство не содержит четких гарантий того, что доступ правоохранительных органов к данным пользователей «МАХ» не будет осуществляться в упрощенном (внесудебном) порядке.

## **Заключение**

Проведенное исследование позволяет сформулировать следующие выводы.



Становление цифрового суверенитета России прошло путь от доктринальных дискуссий (2010-е гг.) до конкретных законодательных решений (2019–2025 гг.). Конституционные поправки 2020 г. создали необходимую правовую основу для отнесения информационных технологий и оборота цифровых данных к ведению Российской Федерации.

Проблема идентификации физических лиц в цифровом пространстве является ключевым элементом обеспечения цифрового суверенитета. Федеральный закон № 572-ФЗ создал правовой механизм использования биометрических персональных данных, однако сохраняется ряд проблем: недостаточная защищенность централизованных баз биометрических данных, риск косвенного принуждения граждан к их предоставлению, отсутствие единых стандартов защиты у операторов [11].

Создание национального мессенджера «МАХ» представляет собой наиболее масштабный проект по деофшоризации коммуникационной инфраструктуры. Однако правовой режим мессенджера содержит внутренние противоречия: с одной стороны, он позиционируется как частный продукт, с другой — получает преимущества от государства. Это создает риски нарушения антимонопольного законодательства, что подтверждается обращениями в ФАС и судебными спорами.

Судебная практика, связанная с мессенджером «МАХ», только формируется, но уже выявила несколько проблемных узлов: недостаточная обоснованность блокировок иностранных мессенджеров с точки зрения соблюдения конституционных прав граждан; использование «МАХ» в преступных целях, ставящее под сомнение эффективность механизмов идентификации; отсутствие прозрачного порядка доступа правоохранительных органов к данным пользователей.

Для совершенствования правового регулирования видится перспективным разработать единую методику оценки эффективности механизмов идентификации в государственных информационных системах; закрепить исчерпывающий перечень оснований доступа правоохранительных органов к данным пользователей национальных цифровых платформ; создать независимый механизм общественного контроля за обработкой персональных данных.

### Конфликт интересов

Не указан.

### Рецензия

Волков Ю.В., Уральский государственный юридический университет им. В.Ф. Яковлева, Екатеринбург Российская Федерация  
DOI: <https://doi.org/10.60797/IRJ.2026.167.92.1>

### Conflict of Interest

None declared.

### Review

Volkov Y.V., Ural State Law University nm. V.F. Yakovlev, Ekaterinburg Russian Federation  
DOI: <https://doi.org/10.60797/IRJ.2026.167.92.1>

### Список литературы / References

1. Конохов М.В. О некоторых проблемах обеспечения государственного суверенитета Российской Федерации в информационном пространстве на современном этапе развития международных отношений / М.В. Конохов // Аграрное и земельное право. — 2024. — № 3. — С. 249–254.
2. Нарутто С.В. Информационный суверенитет: конституционно-правовые основы в условиях развития цифрового государства / С.В. Нарутто, С.Ю. Колмаков, И.М. Япрынец // Образование и право. — 2022. — № 10. — С. 14–22.
3. Ефремов А. А. Информационно-правовой механизм обеспечения государственного суверенитета Российской Федерации: автореф. дис. д-р. юр. наук / Ефремов Алексей Александрович. — Москва, 2021. — 37 с.
4. Алферова Е.В. Государственный суверенитет в информационном (цифровом) пространстве: доктринальные и законодательные подходы / Е.В. Алферова // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. «Государство и право». — 2024. — № 2. — С. 171–186.
5. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 № 400 // Собрание законодательства РФ. — 2021. — № 27. — Ч. II. — Ст. 5351.
6. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // Собрание законодательства РФ. — 2016. — № 50. — Ст. 7074.
7. Провалинский Д.И. Правовое обеспечение суверенитета в цифровом пространстве / Д.И. Провалинский // Pravosudie/Justice. — 2024. — Т. 6. — № 2. — С. 98–108.
8. Ковалев С.Д. Создание национального мессенджера, шаг к цифровому суверенитету России / С.Д. Ковалев // Аграрное и земельное право. — 2025. — № 9. — С. 197–199.
9. Российская Федерация. Законы. О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации : федер. закон : [от 24.06.2025 № 156-ФЗ] // Собрание законодательства РФ. — 2025. — № 26. — Ст. 4782.
10. Об организации, обеспечивающей создание и функционирование многофункционального сервиса обмена информацией: Распоряжение Правительства РФ от 12.07.2025 № 1880-р // Собрание законодательства РФ. — 2025. — № 29. — Ст. 5421.
11. Российская Федерация. Законы. Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации : федер. закон : [от 29.12.2022 № 572-ФЗ] // Собрание законодательства РФ. — 2023. — № 1. — Ч. I. — Ст. 40.



### Список литературы на английском языке / References in English

1. Konokhov M.V. O nekotoryh problemah obespecheniya gosudarstvennogo suvereniteta Rossijskoj Federacii v informacionnom prostranstve na sovremennom etape razvitiya mezhdunarodnyh otnoshenij [On some problems of ensuring the state sovereignty of the Russian Federation in the information space at the current stage of development of international relations] / M.V. Konokhov // Agrarnoe i zemel'noe pravo [Agrarian and land law]. — 2024. — № 3. — P. 249–254. [in Russian]
2. Naruto S.V. Informacionnyj suverenitet: konstitucionno-pravovye osnovy v usloviyah razvitiya cifrovogo gosudarstva [Information sovereignty: constitutional and legal foundations in the context of the development of a digital state] / S.V. Naruto, S.Yu. Kolmakov, I.M. Yaprincev // Obrazovanie i pravo [Education and Law]. — 2022. — № 10. — P. 14–22. [in Russian]
3. Efremov A.A. Informacionno-pravovoj mekhanizm obespecheniya gosudarstvennogo suvereniteta Rossijskoj Federacii [Information and legal mechanism for ensuring state sovereignty of the Russian Federation]: abstract. diss. ... of PhD in Legal Sciences / Efremov Alexey Alexandrovich. — Moscow, 2021. — 37 p. [in Russian]
4. Alferova E.V. Gosudarstvennyj suverenitet v informacionnom (cifrovom) prostranstve: doktrinal'nye i zakonodatel'nye podhody [State Sovereignty in the Information (Digital) Space: Doctrinal and Legislative Approaches] / E.V. Alferova // Social'nye i gumanitarnye nauki. Otechestvennaya i zarubezhnaya literatura. Ser. «Gosudarstvo i pravo» [Social and Humanitarian Sciences. Domestic and Foreign Literature. Series: State and Law]. — 2024. — № 2. — P. 171–186. [in Russian]
5. O Strategii nacional'noj bezopasnosti Rossijskoj Federacii [On the National Security Strategy of the Russian Federation]: Decree of the President of the Russian Federation of July 2, 2021, No. 400 // Sobranie zakonodatel'stva RF [Collected Legislation of the Russian Federation]. — 2021. — № 27. — Pt. II. — Art. 5351. [in Russian]
6. Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii [On Approval of the Doctrine of Information Security of the Russian Federation]: Decree of the President of the Russian Federation of 05.12.2016 No. 646 // Sobranie zakonodatel'stva RF [Collected Legislation of the Russian Federation]. — 2016. — № 50. — Art. 7074. [in Russian]
7. Provalinsky D. I. Pravovoe obespechenie suvereniteta v cifrovom prostranstve [Legal support for sovereignty in the digital space] / D.I. Provalinsky // Pravosudie/Justice. — 2024. — Vol. 6. — № 2. — P. 98–108. [in Russian]
8. Kovalev S. D. Sozdanie nacional'nogo messendzhera, shag k cifrovomu suverenitetu Rossii [Creation of a national messenger, a step towards Russia's digital sovereignty] / S.D. Kovalev // Agrarnoe i zemel'noe pravo [Agrarian and land law]. — 2025. — № 9. — P. 197–199. [in Russian]
9. Rossiiskaya Federatsiya. Zakony. O sozdanii mnogofunkcional'nogo servisa obmena informaciej i o vnesenii izmenenij v otдел'nye zakonodatel'nye akty Rossijskoj Federacii [Russian Federation. Laws. On the Creation of a Multifunctional Information Exchange Service and Amendments to Certain Legislative Acts of the Russian Federation] : Federal Law : [of June 24, 2025 No. 156-FZ] // Sobranie zakonodatel'stva RF [Collected Legislation of the Russian Federation]. — 2025. — № 26. — Art. 4782. [in Russian]
10. Ob organizacii, obespechivayushchej sozdanie i funkcionirovanie mnogofunkcional'nogo servisa obmena informaciej [On the organization ensuring the creation and operation of a multifunctional information exchange service]: Order of the Government of the Russian Federation of July 12, 2025, No. 1880 r // Sobranie zakonodatel'stva RF [Collected Legislation of the Russian Federation]. — 2025. — № 29. — Art. 5421. [in Russian]
11. Rossiiskaya Federatsiya. Zakoni. Ob osushchestvlenii identifikacii i (ili) autentifikacii fizicheskikh lic s ispol'zovaniem biometricheskikh personal'nyh dannyh, o vnesenii izmenenij v otдел'nye zakonodatel'nye akty Rossijskoj Federacii i priznanii utrativshimi silu otдел'nyh polozhenij zakonodatel'nyh aktov Rossijskoj Federacii [Russian Federation. Laws. On the implementation of identification and (or) authentication of individuals using biometric personal data, on amendments to certain legislative acts of the Russian Federation and on the recognition of certain provisions of legislative acts of the Russian Federation as invalid] : Federal Law : [of 29.12.2022 No. 572-FZ] // Sobranie zakonodatel'stva RF [Collected Legislation of the Russian Federation]. — 2023. — № 1. — Pt. I. — Art. 40. [in Russian]