

Индекс УДК 341.9

Код ГРНТИ 10.89.00

DOI: 10.22204/2587-8956-2026-124-01-55-62



А.К. ЖАРОВА*

Безопасность цифрового профиля гражданина как ключевой элемент цифрового суверенитета государства**

Вопрос о соотношении цифрового суверенитета государства и цифровых профилей его граждан требует особого внимания. В данном контексте возникает необходимость выполнения государством обязанности по обеспечению безопасности в информационной сфере. Государственный контроль выступает в качестве инструмента противодействия угрозам национальной безопасности в информационном пространстве. Государство, обеспечивая состояние защищённости от внутренних и внешних угроз в информационной сфере, обязано гарантировать прозрачность, ограниченность, подконтрольность и правовую регламентацию методов создания и использования цифровых профилей граждан.

В статье подтверждается гипотеза, что необходимым и достаточным условием для защиты цифровых профилей является достижение технологического суверенитета, выражающегося в государственном контроле над технологиями цифрового профилирования. Обеспечение технологического суверенитета способствует достижению цифрового суверенитета.

Решая проблему обеспечения цифрового суверенитета в условиях санкций, Российская Федерация в период с 2022 по 2025 г. осуществила значительные институциональные изменения в сфере технологической политики.

Ключевые слова: цифровой суверенитет, технологический суверенитет, информационная сфера, информационный суверенитет, санкции, цифровой профиль, закон, правовое регулирование, защищённость, государственная политика

Развитие информационной инфраструктуры порождает фундаментальное противоречие между двумя, на первый взгляд, взаимодополняющими задачами: обеспечением государственного цифрового суверенитета и защитой прав граждан в условиях

цифровизации. Переход от одной задачи к другой сопряжён с рядом серьёзных проблем, касающихся безопасности данных, приватности, контроля и распределения властных полномочий.

Суверенитет является основным признаком государства, который определяет

* **Жарова Анна Константиновна** — доктор юридических наук, ведущий научный сотрудник Института государства и права РАН.

E-mail: anna_jarova@mail.ru

** Статья подготовлена в рамках государственного задания «Достижение верховенства международного права в установлении мирового порядка и охране прав человека» (FMUZ-2024-0046).

право носителя верховной государственной власти независимо, самостоятельно формировать, а также осуществлять свою волю [1, 2], в том числе и в информационной сфере. Поскольку информационная сфера — это «сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации»¹, то логично предположить, что верховенство государственной власти должно распространяться и на область информационных технологий. Эту мысль подтверждают используемые в законодательстве термины «технологический суверенитет» и «цифровой суверенитет».

Обеспечение цифрового суверенитета ставит государство перед дилеммой, которую невозможно разрешить чисто технологическим путём. Поскольку, с одной стороны, для обеспечения цифрового суверенитета государство должно контролировать свою цифровую инфраструктуру, персональные данные граждан и информационные потоки. С другой стороны, граждане всё чаще требуют контроля над собственными данными и автономии в цифровой сфере. И в этом случае цифровой профиль (ЦП) гражданина является инструментом государственного управления и в таком контексте становится не только благом, но и узлом противоречивых интересов.

В настоящее время ЦП человека — это не только совокупность определённым образом структурированной информации о нём, но и сервисы, которые позволяют организациям получать информацию о своих клиентах не только из государственных информационных систем (ИС), но и из Интернета [3].

В связи с этим в статье сформулирована гипотеза, что необходимым и достаточ-

ным условием для защиты ЦП является достижение технологического суверенитета, выражающегося, в том числе, в государственном контроле над технологиями цифрового профилирования. Причём обеспечить цифровой суверенитет без технологического суверенитета невозможно.

Понятие цифрового профиля

Формирование ЦП человека представляет собой систематический процесс сбора, обработки и анализа данных о физических лицах, включая информацию, доступную в сети Интернет. ЦП может содержать персональные данные, конфиденциальную информацию, сведения о поведенческих особенностях, действиях, социальном статусе, связях и взаимодействиях человека [4], причём область применения постоянно расширяется [5]. Изначально технология ЦП использовалась преимущественно в маркетинговых и рекламных целях, но впоследствии стала активно применяться в сферах обеспечения безопасности на различных уровнях государственного управления и правосудия [6, 7].

Термин «цифровой профиль» имеет юридически закреплённое значение в зависимости от сферы его применения. Например, это государственная информационная инфраструктура, которая позволяет банкам и страховым компаниям получать достоверную информацию о гражданине через «цифровое окно»². Система ЦП, реализованная на базе единой системы идентификации и аутентификации, предоставляет организациям возможность получать из государственных ИС сведения с согласия гражданина³. ЦП иностранного гражданина как государственный информационный

¹ Модельный закон о международном информационном обмене (принят в Санкт-Петербурге 26.03.2002 г. Постановлением 19-7 на 19-м пленарном заседании Межпарламентской Ассамблеи государств — участников СНГ) // Информационный бюллетень. Межпарламентская Ассамблея государств — участников Содружества Независимых Государств. 2002. № 29. С. 134–143.

² Доступ к данным цифрового профиля физического лица // <https://www.programbank.ru/site/office-personal-data> (дата обращения: 24.12.2025).

³ Письмо Минцифры России от 01.12.2025 г. № МШ-П24-117737 «О взаимодействии с инфраструктурой цифрового профиля» (документ опубликован не был) // СПС «КонсультантПлюс».



Ил. 1. Состав инфраструктуры ЦП физического лица

ресурс¹ должен быть создан до 30.06.2026 г. ЦП клиента, наряду с платформой удалённой идентификации (Единая биометрическая система), Системой быстрых платежей и платформой маркетплейс, является одним из основных инфраструктурных проектов, основанных на использовании цифровых технологий, в отношении которых (в первую очередь Банком России) устанавливаются требования информационной безопасности². Под ЦП гражданина понимается «совокупность всех данных о гражданине, которые имеются в распоряжении государственных органов и государственных ИС, а также совокупность технических средств, которые позволяют управлять этими дан-

ными, в том числе предоставлять их третьим лицам с согласия и в интересах самого гражданина» (п. 2.3)³.

Создана инфраструктура ЦП физического лица как централизованная структура, которая объединяет различные категории информации о человеке: от документов и места проживания до медицинских записей, налоговых данных и истории посещений. Структура ЦП физического лица представлена на ил. 1. и заимствована с официального сайта Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации⁴.

Таким образом, понятие ЦП человека имеет двойственную природу — это

¹ Указ Президента РФ от 09.07.2025 г. № 467 «О государственном информационном ресурсе «Цифровой профиль иностранного гражданина» // Собрание законодательства Российской Федерации (СЗ РФ). 2025. № 28. Ст. 3955.

² Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов. Текст документа приведён в соответствии с публикацией на сайте <https://www.cbr.ru> по состоянию на 28.09.2020 г. // СПС «Консультант Плюс».

³ Приказ Минцифры России от 30.06.2022 г. № 505 (ред. от 29.12.2023) «Об утверждении методик расчёта показателей федеральных проектов национальной программы «Цифровая экономика Российской Федерации» // СПС «КонсультантПлюс».

⁴ Сценарии использования инфраструктуры цифрового профиля физического лица https://adm.digital.gov.ru/app/uploads/2025/08/1620f0_c_scenarii_ispolzovaniya_czp_fl_v1_47.pdf.

не только удобный инструмент получения государственных услуг, но и мощнейшая технология сбора и анализа данных о пользователе. В контексте ЦП как инструмента для получения информации о пользователе Интернета обычно рассматриваются понятия «цифровой след» и «цифровая тень», анализ которых позволяет получать данные, которые пользователь не предоставлял добровольно [8].

Например, системы веб-аналитики могут создавать уникальные ЦП интернет-пользователей, даже если те не прошли процедуру авторизации на сайте, используя технологию Device Fingerprinting (цифровой отпечаток устройства). Для этого специальные скрипты собирают и анализируют множество параметров устройства, метаданных действий интернет-пользователя, формируя уникальный идентификатор, который позволяет определять пользователя на различных веб-ресурсах.

Таким образом, формирование и использование ЦП становится неотъемлемым компонентом в развитии цифровой среды [9]. Возможности различных технологий анализа данных позволяют рассматривать понятие ЦП в широком смысле как многокомпонентную и многоуровневую структуру, формирование которой осуществляется на основе анализа данных, содержащихся во всех ИС, а также в информационно-телекоммуникационных сетях¹.

Безопасность цифрового профиля человека как основа обеспечения технологического суверенитета

Технологический суверенитет в первую очередь связан с областью разработки и стандартизации любых видов информационных и коммуникационных технологий. Эту мысль подтверждает определение

понятия «технологического суверенитета», данное в распоряжении Правительства РФ от 20 мая 2023 г. «Об утверждении Концепции технологического развития на период до 2030 года», как «наличие в стране (под национальным контролем) критических и сквозных технологий собственных линий разработки и условий производства продукции на их основе, обеспечивающих устойчивую возможность государства и общества достигать собственные национальные цели развития и реализовывать национальные интересы. Технологический суверенитет обеспечивается в двух основных формах: исследования, разработка и внедрение критических и сквозных технологий (по установленному перечню) и производство высокотехнологичной продукции, основанной на указанных технологиях»².

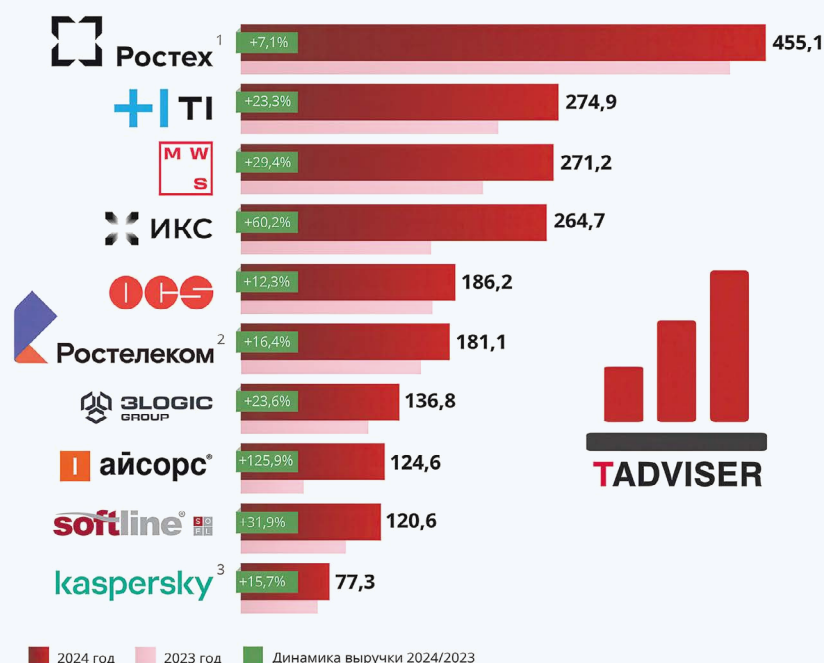
Поскольку ЦП человека — элемент информационной инфраструктуры, то в ситуации, когда управление данной инфраструктурой осуществляется иностранными компаниями, обеспечение защиты ЦП приобретает значимость, выходящую за рамки регулирования персональных данных и договорных отношений, и становится вопросом цифрового суверенитета. В таком случае возникает закономерный вопрос: можно ли обеспечить безопасность ЦП гражданина, когда большинство ИТ-компаний являлись зарубежными и в целях подорыва суверенитета Российской Федерации в 2022 г. начали уходить с рынка России, ограничив использование своих программных продуктов, в их числе Microsoft, IBM, Adobe, Apple³. Эту цель подтверждает также принятый 18.12.2023 г. Советом ЕС 12-й пакет санкций в отношении России. В нём содержатся требования о прекращении лицензий, которые были закуплены российскими потребителями на несколько лет

¹ Сценарии использования инфраструктуры цифрового профиля физического лица https://adm.digital.gov.ru/app/uploads/2025/08/1620f0_c_szenarii_ispolzovaniya_czp_fl_v1_47.pdf.

² Распоряжение Правительства РФ от 20.05.2023 г. № 1315-р «Об утверждении Концепции технологического развития на период до 2030 года» (вместе с «Концепцией технологического развития на период до 2030 года») // СЗ РФ. 2023. № 22. Ст. 3964.

³ Как дела у ИТ-бизнеса в России // <https://habr.com/ru/companies/datanomica/articles/745636/> (дата обращения: 24.12.2025).

Крупнейшие ИТ-компании в России по выручке за 2024 год (в млрд рублей)



1. Включены показатели компаний Росэл, Автоматика, Швабе, КРЭТ и др.
2. Выручка от цифровых сервисов
3. Глобальная выручка

Ил. 2. Топ-10 рейтинга 500 крупнейших компаний, работающих на российском ИТ-рынке

вперёд, и запрете на поставку программного обеспечения таких производителей, как Autodesk (включая AutoCAD), SolidWorks, SAP, Oracle и Microsoft.

Для обеспечения собственной технологической независимости Российская Федерация пошла по пути импортозамещения, который подразумевает переход на использование программного обеспечения отечественного производства. Хотя этот подход представляет собой один из наиболее сложных, но в то же время наиболее перспективных методов обеспечения безопасности граждан и суверенитета в среднесрочной и долгосрочной перспективе.

За последние три года в Российской Федерации происходит существенная трансформация в структуре рынка, характеризующаяся замещением компаний, прекративших свою деятельность на территории страны, отечественными предприятиями. Например, в 2024 г. в соответствии со статистикой, представленной социальной сетью «Авито», Windows не вошла даже в топ-4 по продажам в России. Эти позиции в рейтинге заняли наши производители: Astra Linux, «Ред ОС», «Ред Софт», «Базальт СПО», а также платформа Uncom OS¹.

По итогам исследования, проведённого аналитическим агентством «TAdviser» в 2025 г., составлен рейтинг 500 крупней-

¹ Санкции_и_ограничения_в_области_высоких_технологий_против_России // https://www.tadviser.ru/index.php/Статья:Санкции_и_ограничения_в_области_высоких_технологий_против_России# (дата обращения: 24.12.2025).

ших компаний, работающих на российском ИТ-рынке, он представлен на ил. 2¹.

Для обеспечения основ государственной власти в технологической сфере в конце 2024 г. был принят Федеральный закон «О технологической политике»², в котором технологический суверенитет закреплён как элемент национальной безопасности. В том же году подписан Указ Президента РФ «О Стратегии научно-технологического развития Российской Федерации»³, в котором определены понятие технологического суверенитета и принципы государственной политики в области научно-технологического развития.

Технологический суверенитет является вектором развития технологического и социально-экономического укладов государства. Но для реализации этого вектора развития государством должна быть предварительно создана система взаимосвязанных нормативных правовых и технических условий развития всех возможных технологий.

Так, в соответствии с Постановлением Правительства РФ от 16.12.2020 г. № 2136⁴ для оценки уровня технологического суверенитета исследуются «технические характеристики продукции, результаты интеллектуальной деятельности, применение отечественных решений в составе продукции комплексного проекта, наличие у организации научно-технического и технологического задела и его значимость для реализации комплексного проекта».

Таким образом, технологический суверенитет Российской Федерации определяется верховенством государственной власти в области развития собственных тех-

нологий и инноваций, исследовательских центров, конструкторских бюро, а также требованиями к принципам разработки собственных продукции и технологий, к инвестициям в научные исследования.

Заключение

В контексте обеспечения цифрового суверенитета государство сталкивается с многогранной дилеммой, которая не может быть решена исключительно технологическими методами. С одной стороны, необходимо осуществлять контроль над информационной инфраструктурой, персональными данными граждан и обеспечивать безопасность информации. С другой стороны, наблюдается увеличение запросов со стороны граждан относительно защиты их персональных данных и обеспечения автономии в цифровом пространстве. В этих условиях ЦП гражданина становится инструментом государственного управления, который способствует повышению эффективности государственного администрирования, но и порождает ряд противоречий. Поскольку ЦП гражданина представляет собой сложную систему, в которой пересекаются разнообразные интересы и потребности.

Понятие ЦП следует рассматривать в широком контексте как комплексную и многоуровневую структуру, которая формируется на основе анализа данных, интегрированных из всех существующих ИС и информационно-телекоммуникационных сетей. Причём технологическая инфраструктура, обеспечивающая функционирование ЦП на территории России, должна находиться под контролем отечественных компаний.

¹ TAdviser500: Крупнейшие ИТ-компании в России // https://www.tadviser.ru/index.php/Статья:Ранкинг_TAdviser500:_Крупнейшие_ИТ-компании_в_России_2025. (дата обращения: 24.12.2025).

² Федеральный закон от 28.12.2024 г. № 523-ФЗ «О технологической политике в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2024. № 53 (Ч. I). Ст. 8533.

³ Указ Президента РФ от 28.02.2024 г. № 145 «О Стратегии научно-технологического развития Российской Федерации» // СЗ РФ. 2024. № 10. Ст. 1373.

⁴ Постановление Правительства РФ от 16.12.2020 г. № 2136. «Об утверждении Правил предоставления в 2023 году из федерального бюджета субсидий российским организациям на финансовое обеспечение мероприятий по проведению научно-исследовательских и опытно-конструкторских работ в области средств производства электроники» // СЗ РФ. 2020. № 52 (Ч. I). Ст. 8823.

Решая проблему обеспечения цифрового суверенитета в условиях санкций, Российская Федерация в период с 2022 по 2025 г. осуществила значительные институциональные изменения в сфере технологической политики. В 2024 г. концепция технологического суверенитета была законодательно закреплена в Федеральном законе «О технологической политике» и Стратегии научно-технологического развития Российской Федерации. Такие изменения свидетельствуют о трансформации вопроса

из технико-экономической плоскости в политико-правовую сферу. Наша страна последовательно усиливает свои технологические возможности в рамках стратегии импортозамещения, что позволит обеспечить технологический суверенитет и, следовательно, безопасность.

Под воздействием внешних санкций и политического давления происходит постепенная трансформация российской государственной политики в сторону строительства суверенной цифровой экосистемы.

ЛИТЕРАТУРА

1. Провалинский Д.И. Правовое обеспечение суверенитета в цифровом пространстве // Правосудие. 2024. Т. 6. № 2. С. 98–108. DOI: 10.37399/2686-9241.2024.2.98–108.
2. Степанов П.В. Подходы к пониманию цифрового суверенитета России // Журнал российского права. 2024. Т. 28. № 4. С. 37–51. DOI: 10.61205/jrp.2024.4.1.
3. Жарова А.К. Обеспечение информационного суверенитета Российской Федерации // Юрист. 2021. № 11. С. 28–33. DOI: 10.18572/1812-3929-2021-11-28-33.
4. Мартиросян А.Ж. Реалии цифрового суверенитета в современном мире // Международная жизнь. 2021. № 3. С. 28–35.
5. Жарова А.К. Множественность понятия «суверенитет Российской Федерации в информационной сфере» / А.К. Жарова, В.В. Елина // Правопорядок: история, теория, практика. 2024. № 4 (43). С. 51–55. DOI: 10.47475/2311-696X-2024-43-4-51-55.
6. Елин В.М. Цифровое пространство доверия как инструмент построения цифрового суверенитета / В.М. Елин, А.В. Царегородцев // Юридическая наука. 2025. № 4. С. 481–484.
7. Карев Д.А. Цифровой суверенитет / Д.А. Карев, Ю.В. Чертыковцев // Право и государство: теория и практика. 2025. № 4. С. 80–83. DOI: 10.47643/1815-1337_2025_4_80.
8. Жарова А.К. Анализ размещаемых в сети открытых данных в целях получения информации о криминогенной обстановке / А.К. Жарова, В.М. Елин, И.В. Атласов // Вопросы кибербезопасности. 2025. № 4 (68). С. 152–159. DOI: 10.21681/2311-3456-2025-4-152-159.
9. Жарова А.К. Вопросы обеспечения безопасности цифрового профиля человека // Юрист. 2020. № 3. С. 55–61.

Security of Citizens' Digital Profiles as Key Element of the State's Digital Sovereignty

Zharova Anna Konstantinovna — Doctor of Law, a leading researcher at the Institute of State and Law of the Russian Academy of Sciences.
E-mail: anna_jarova@mail.ru

The author examines the relationship between the state's digital sovereignty and the digital profiles of its citizens, which requires special attention. In this context, the state has an obligation to ensure security in the information domain. State control serves as a tool for countering threats

to national security in the information space. The state, while ensuring safety against internal and external threats in the information domain, must guarantee transparency, limited scope, accountability, and legal regulation of the methods for creating and using citizens' digital profiles.

The article confirms the hypothesis that a necessary and sufficient condition for protecting digital profiles is the achievement of technological sovereignty, expressed in state control over digital profiling technologies. Ensuring technological sovereignty contributes to the achievement of digital sovereignty.

While addressing the problem of ensuring digital sovereignty under sanctions, the Russian Federation carried out significant institutional changes in the field of technology policy between 2022 and 2025.

Keywords: digital sovereignty, technological sovereignty, information sphere, information sovereignty, sanctions, digital profile, law, legal regulation, security, state policy

REFERENCES

1. Provalinskii D.I. Pravovoe obespechenie suvereniteta v tsifrovom prostranstve // Pravosudie. 2024. T. 6. № 2. S. 98–108. DOI: 10.37399/2686-9241.2024.2.98–108 (in Russian).
2. Stepanov P.V. Podkhody k ponimaniyu tsifrovogo suvereniteta Rossii // Zhurnal rossiiskogo prava. 2024. T. 28. № 4. S. 37–51. DOI: 10.61205/jrp.2024.4.1 (in Russian).
3. Zharova A.K. Obespechenie informatsionnogo suvereniteta Rossiiskoi Federatsii // Yurist. 2021. № 11. S. 28–33. DOI: 10.18572/1812-3929-2021-11-28-33 (in Russian).
4. Martirosyan A.Zh. Realii tsifrovogo suvereniteta v sovremennom mire // Mezhdunarodnaya zhizn'. 2021. № 3. S. 28–35 (in Russian).
5. Zharova A.K. Mnozhestvennost' ponyatiya «suverenitet Rossiiskoi Federatsii v informatsionnoi sfere» / A.K. Zharova, V.V. Elina // Pravoporyadok: istoriya, teoriya, praktika. 2024. № 4 (43). S. 51–55. DOI: 10.47475/2311-696X-2024-43-4-51-55 (in Russian).
6. Elin V.M. Tsifrovoe prostranstvo doveriya kak instrument postroeniya tsifrovogo suvereniteta / V.M. Elin, A.V. Tsaregorodtsev // Yuridicheskaya nauka. 2025. № 4. S. 481–484 (in Russian).
7. Karev D.A. Tsifrovoy suverenitet / D.A. Karev, Yu.V. Chertykovtsev // Pravo i gosudarstvo: teoriya i praktika. 2025. № 4. S. 80–83. DOI: 10.47643/1815-1337_2025_4_80 (in Russian).
8. Zharova A.K. Analiz razmeshchaemykh v seti otkrytykh dannykh v tselyakh polucheniya informatsii o kriminogennoi obstanovke / A.K. Zharova, V.M. Elin, I.V. Atlasov // Voprosy kiberbezopasnosti. 2025. № 4 (68). S. 152–159. DOI: 10.21681/2311-3456-2025-4-152-159 (in Russian).
9. Zharova A.K. Voprosy obespecheniya bezopasnosti tsifrovogo profilya cheloveka // Yurist. 2020. № 3. S. 55–61 (in Russian).