УДК 32:004
DOI: 10.26456/vtfilol/2026.1.173

ФОРМИРОВАНИЕ ЦИФРОВОГО ПРОФИЛЯ ГРАЖДАНИНА В ИНФОРМАЦИОННОМ ПОЛЕ РФ

А. В. Штырлина

Коммуникационное агентство «Практика», г. Москва

В статье исследуются правовые, технологические и экономические предпосылки формирования цифрового профиля (ЦП) гражданина в контексте курса Российской Федерации на технологическую автономию. Анализируются сущность, структура и функции ЦП, нормативно-правовая база его регулирования, ключевые угрозы кибербезопасности, а также роль национального мессенджера *MAX* в построении безопасной цифровой экосистемы. Обосновано, что ЦП выступает не только инструментом повышения эффективности госуслуг и цифровых сервисов, но и важнейшим элементом защиты информационного суверенитета страны.

Ключевые слова: *технологический суверенитет, медиабезопасность, информационная безопасность, цифровое пространство, цифровой профиль, нормативно-правовое регулирование, защита данных, цифровая трансформация.*

В эпоху цифровой трансформации экономики и общества в условиях интенсификации трансграничных информационных потоков защита цифрового профиля физического лица приобретает первостепенное значение. С одной стороны, повсеместное внедрение цифровых сервисов требует раскрытия значительного объёма персональных данных; с другой – неуклонно растут угрозы киберпреступности, способные нанести серьёзный урон репутации, финансовой стабильности и даже личной безопасности граждан. В этих условиях формирование и защита цифрового профиля становятся ключевыми элементами обеспечения национальной безопасности и технологического суверенитета Российской Федерации.

Актуальность проблемы подтверждается статистическими данными: по информации Министерства внутренних дел РФ, преступления с использованием информационно-телекоммуникационных технологий в 2024 г. составили 40 % от общего числа зарегистрированных в России преступлений, что является максимумом от общего числа преступлений, начиная с 2020 года [3]. А общий ущерб от них превысил 170 млрд рублей [4]. За тот же период Федеральной службой безопасности было зафиксировано свыше 640 тыс. случаев дистанционного мошенничества [Там же]. Эти цифры наглядно демонстрируют необходимость выстраивания

© Штырлина А. В., 2026

надёжной системы защиты цифрового профиля как базового элемента информационной безопасности личности и государства.

Цель данного исследования – проанализировать правовые, технологические и экономические предпосылки формирования цифрового профиля физического лица в контексте курса РФ на технологическую автономию. Для её достижения необходимо решить следующие задачи: определить структуру и компоненты цифрового профиля; выявить ключевые угрозы медиа- и кибербезопасности; проанализировать нормативно-правовую базу защиты персональных данных; оценить роль национального мессенджера *MAX* в формировании безопасной цифровой экосистемы.

Цифровой профиль (ЦП) представляет собой динамическую совокупность данных о гражданине, хранящихся в государственных (ЕСИА, ЕГРН, ФНС), коммерческих (банки, страховые компании) информационных системах, а также в Единой биометрической системе (ЕБС). Его ключевая особенность – способность трансформироваться и дополняться на протяжении всей жизни человека: уже в период обучения ЦП формируется за счёт данных из образовательных платформ, сервисов стажировок, социальных сетей и профессиональных сообществ [1]. Это делает крайне важным раннее осознание структуры профиля для эффективного управления цифровой репутацией и информационной гигиеной.

Функционально цифровой профиль реализует три базовых принципа: централизацию и автоматизацию данных (объединение информации из ПФР, ФНС, МВД, Росреестра в единую платформу); проактивность и бесконтактность (управление доступом к данным через механизмы согласия/отзыва); интеграцию с технологическими решениями (взаимодействие с ЕСИА, СМЭВ, Открытыми API).

Правовое регулирование ЦП базируется на многоуровневой системе нормативных актов. Согласно Указу Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации», документ определяет информационную безопасность как стратегический приоритет, а защиту информационного пространства – как условие суверенитета. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» устанавливает требования к устойчивости информационных систем и порядок блокировки запрещённого контента. Принцип локализации данных закреплён в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных», что минимизирует риски утечки информации за рубеж.

Федеральный закон от 30.12.2020 № 538-ФЗ вводит повышенные санкции за клевету и оскорбление в публичном пространстве, включая интернет-ресурсы (ст. 5.61 КоАП РФ). Федеральный закон от 08.08.2024 № 303-ФЗ устанавливает обязанность регистрации блогеров с аудиторией свыше 10 тысяч подписчиков в Роскомнадзоре, что позволяет контроли-

ровать распространение информации. Федеральный закон от 14.07.2022 № 255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием» предусматривает создание реестра иностранных агентов и ограничения на их деятельность в медиапространстве. Федеральный закон от 02.07.2021 № 347-ФЗ «О рекламе» вводит обязательную маркировку интернет-рекламы и передачу данных в Единый реестр интернет-рекламы (ЕРИР). Федеральный закон от 11.03.2024 № 42-ФЗ запрещает рекламу ресурсов иностранных агентов, усиливая контроль за финансированием деструктивных медиапроектов. Федеральный закон от 22.04.2024 г. № 93-ФЗ О внесении изменения в Федеральный закон «О государственном языке Российской Федерации» устанавливает русский язык как государственный на всей территории страны и обязывает использовать его в определённых сферах, включая СМИ, образование, делопроизводство и взаимодействие с органами власти, в том числе наружной рекламе, – до 1 марта 2026 года вывески требуется привести их в соответствие с языковыми нормами.

Эти нормативно-правовые акты формируют комплексную систему защиты, сочетающую технические меры по локализации данных и отечественному ПО; правовые ограничения по блокировке ресурсов и ответственности за фейки в связке с экономическими механизмами по маркировке интернет-рекламы и госзаказу на цифровые решения.

Ввиду регуляторных нововведений меняется весь коммуникационный ландшафт страны. А это совокупность коммуникационных процессов, каналов, технологий и участников, определяющих взаимодействие в обществе. К последним относятся: *государственные органы*, которые формируют и используют цифровые профили, регулируют медиапространство; *коммерческие организации* (банки, страховые компании, IT-компании), интегрирующие цифровые профили в свои бизнес-процессы; *СМИ и медиакомпании*, адаптирующие контент под новые форматы и каналы распространения; *блогеры и инфлюенсеры*, выступающие в роли самостоятельных медиааакторов; *граждане*, которые одновременно являются потребителями информации и источниками данных в цифровых профилях; *технологические платформы* (соцсети, мессенджеры), выступающие каналами распространения контента и инструментами коммуникации.

Традиционные СМИ адаптируются к цифровой среде: развивают онлайн-платформы, мобильные приложения, переходят на принцип *digital-first* (контент сначала публикуется в цифровом виде). Возникают новые игроки – блогеры, инфлюенсеры, создатели контента в соцсетях, которые формируют альтернативные каналы распространения информации. Медиапотребление кастомизируется за счёт выбора аудиторией контента в соответствии со своими интересами, что приводит к формированию «информационных пузырей», что опасно поляризацией общества и искажением действительности [6].

Таким образом, цифровой профиль становится катализатором изменений в коммуникациях и медиасреде, способствуя переходу к более цифровым, автоматизированным и персонализированным формам взаимодействия. Это трансформирует не только способы обработки данных, но и саму структуру информационного пространства в России, выявляя ряд системных рисков. Во-первых, зависимость от иностранных технологий. Несмотря на развитие отечественных платформ (*VK*, *Rutube*, Яндекс), значительная часть интернет-трафика проходит через зарубежные сервисы, создавая уязвимости: блокировку доступа к критически важным ресурсам, риски утечки данных, ограничения в распространении государственной повестки. Во-вторых, киберугрозы критической инфраструктуры. За 2025 год 73 % всех утечек данных из российских организаций пришлись на госсектор. Было слито более 105 млн строк данных с записями о пользователях и компаниях [5]. И наконец, деструктивный контент. Фейки, манипулятивные технологии и пропаганда чуждых ценностей подрывают социокультурную идентичность и доверие к официальным источникам.

Для нейтрализации угроз реализуется комплекс мер по формированию независимой цифровой экосистемы. Среди них – локализация данных, согласно ст. 18 ФЗ № 152-ФЗ; импортозамещение благодаря разработке отечественных операционных систем «Аврора» и *Astra Linux* и телекоммуникационного оборудования [2]; регулирование контента посредством блокировки запрещённых ресурсов по ст. 15.1–15.6 ФЗ № 149-ФЗ, контроль маркировки интернет-рекламы и просветительская работа через популяризацию программ по цифровой грамотности и медиабезопасности.

Особую роль в этом процессе играет национальный мессенджер MAX, разработанный компанией VK при поддержке Минцифры и «Ростеха». В 2025 году он получил статус многофункциональной платформы с функцией цифровой верификации личности согласно Федеральному от 24.06.2025 № 156-ФЗ «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации». Этот закон заложил основу для замены бумажных документов электронными аналогами, запретил использование иностранных мессенджеров в госсекторе, сделал *MAX* обязательным каналом взаимодействия в сфере ЖКХ, с ноября 2025 года ограничил доступ к платформе «Сферум» только через *MAX*.

Поправки к ФЗ № 152-ФЗ от 30.05.2025 усилили требования к обработке данных и ответственность за утечки, фактически переведя ЦП в разряд юридически значимых элементов повседневной жизни.

Вместе с тем интеграция *MAX* в инфраструктуру идентификации актуализировала ряд проблем в сфере медиабезопасности. Прежде всего,

цифровизация официального подтверждения личности повысила риски, связанные с неполнотой, устареванием или искажением данных в цифровом профиле, что может приводить к отказам в предоставлении услуг или ошибкам в госуслугах. Централизация данных в рамках единой платформы создала потенциальную «точку уязвимости». А значит, любая компрометация аккаунта *MAX* способна открыть доступ ко всему комплексу персональных сведений пользователя.

Для повышения доверия к *MAX* необходимы прозрачное информирование о составе данных и целях их обработки, инструменты контроля (отзыв согласия, история запросов, оповещения), технические меры защиты (многофакторная аутентификация, биометрия) и программы цифровой грамотности для пользователей.

Таким образом, формирование цифрового профиля гражданина – ключевой элемент стратегии медиабезопасности РФ в условиях технологической автономии. ЦП повышает эффективность госуслуг и коммерческих сервисов и защищает суверенитет через локализацию персональных данных, снижая зависимость от иностранных платформ и создавая доверенную цифровую среду.

Для успешной реализации этой стратегии критически важно соблюдать баланс между функциональностью, удобством и защитой прав пользователей. Только при условии прозрачности, надёжных механизмах контроля и повышения цифровой грамотности граждан цифровой профиль сможет стать эффективным инструментом взаимодействия государства, бизнеса и общества в цифровом пространстве.

Список литературы

1. В России намерены создать цифровой профиль молодого человека [текст: электронный] // Известия. 18.07.2025. URL: https://iz.ru/1922784/2025-07-18/v-rossii-namereny-sozdat-tcifrovoi-profil-molodogo-cheloveka (дата обращения: 22.01.2026).
2. Драгун, Я., Аляутдин, Р. ОС «Аврора» 5 поколения в 2026 году: что нужно знать об изменениях [текст: электронный] // Hi-Tech. URL: https://hi-tech.mail.ru/review/124270-os-avrora-5-0/ (дата обращения: 22.01.2026).
3. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2024 года [текст: электронный] // Министерство внутренних дел Российской Федерации: [сайт]. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/?year=2025&month=3&day=20 (дата обращения: 22.01.2026).
4. О противодействии мошеннической деятельности. 07.05.2025 [текст: электронный] // Федеральная служба безопасности Российской Федерации URL: http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10440275%40fsbMessage.html (дата обращения: 22.01.2026).

5. Полонская, В., Жабин, А. Хакеры власть не признают [текст: электронный]// Коммерсантъ. 22.12.2025. URL: https://www.kommersant.ru/doc/8313330 (дата обращения: 22.01.2026).
6. Традиционные печатные СМИ в России: трансформации в цифровую эпоху [текст: электронный] // Ведомости. 20.08.2025. URL: https://www.vedomosti.ru/press_releases/2025/08/20/traditsionnie-pechatnie-smi-v-rossii-transformatsii-v-tsifrovuyu-epohu (дата обращения: 22.01.2026).

FORMATION OF A CITIZEN'S DIGITAL PROFILE IN THE INFORMATION FIELD OF THE RUSSIAN FEDERATION

A. V. Shtyrlina

Communication agency "Praktika", Moscow

The article examines the legal, technological and economic prerequisites for the formation of a citizen's digital profile (DP) in the context of the Russian Federation's course towards technological autonomy. It analyzes the essence, structure, and functions of the DP, the legal framework governing it, key cybersecurity threats, and the role of the national messenger MAX in building a secure digital ecosystem. It is substantiated that the DP acts not only as a tool for improving the efficiency of public and digital services, but also as an essential element in protecting the country's information sovereignty.
Keywords: *technological sovereignty, media security, information security, digital space, digital profile, regulatory framework, data protection, digital transformation.*

Об авторе:

ШТЫРЛИНА Анна Викторовна – основатель коммуникационного агентства «Практика», журналист, член Московского регионального отделения Общероссийской общественной организации «Союз журналистов России», e-mail: anna@pr-practice.ru.

About the author:

SHTYRLINA Anna Viktorovna – founder of the communication agency "Practice", journalist, member of the Moscow regional branch of the All-Russian public organization "Union of Journalists of Russia", e-mail: anna@pr-practice.ru.

Дата поступления рукописи в редакцию: 02.02.2026 г.
Дата подписания в печать: 13.03.2026 г.