БЕЛЯЕВ Д. А.

ЦИФРОВЫЕ СЛЕДЫ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА: НАЧАЛЬНЫЕ ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ФОРМИРОВАНИЯ, ВЗАИМОДЕЙСТВИЯ И БЕЗОПАСНОСТИ

УДК 004.42, ГРНТИ 20.01.04

Статья поступила в редакцию 20.05.2026

Цифровые следы личности, общества, государства: начальные теоретические аспекты формирования, взаимодействия и безопасности

Digital traces of personality, society, state: initial theoretical aspects of formation, interaction and security

Д. А. Беляев

Сыктывкарский государственный университет; г. Сыктывкар

D. A. Belyaev

Syktyvkar State University, Syktyvkar

Описаны теоретические аспекты цифровых следов личности, общества, государства. Дан начальный контекст особенностей информационной безопасности личности, общества, государства в части защиты цифрового следа.

The theoretical aspects of digital traces of the individual, society, and state are described. The initial context of the information security features of the individual, society, and state in terms of protecting the digital footprint is given.

Ключевые слова: *цифровой след, безопасность, личность, общество, государство*

Keywords: *digital footprint, security, personality, society, state*

Введение

Понятие цифрового следа введено основателем сервиса Reputation.com Майклом Фертиком в 2017 году. Во второй четверти XXI века актуальность вопросов анализа появления, сохранения и затухания цифровых следов постоянно повышается. Вопросы, связанные с цифровыми следами, в последние годы активно обсуждаются как в научных статьях (например, [1], [2], [3]), так и в беллетристике, в суждениях общественных и государственных институтов и деятелей. Вместе с тем в настоящее время отсутствуют единые стандартные научные подходы к формулированию и обоснованию тех или иных аспектов существования и развития цифровых следов личности, общества и государства, их безопасности.

Под личностью мы понимаем совокупность относительно устойчивых психологических характеристик, определяющих индивидуальность человека и его место в обществе [4]. Другими словами, это комплексное понятие, обозначающее уникальный набор психологических характеристик,

определяющих поведение человека в обществе. Каждая личность в современном обществе имеет уникальный цифровой портрет и, затем, след.

Общество в контексте рассматриваемого вопроса — это человеческая общность, специфику которой представляют отношения людей между собой, их формы взаимодействия и объединения, прежде всего, с точки зрения цифрового взаимодействия отдельных личностей, также – их горизонтального цифрового влияния друг на друга.

Следуя одному из традиционных определений, государство есть социальный институт, обеспечивающий поддержание порядка в отношениях между членами общества, опирающегося на традиции и законы. Заметим, что в рамках настоящей статьи традиции и законы предполагаем цифровыми, как и далее – след государства тоже цифровым.

Цифровой след личности – термин, который означает совокупность данных, которые человек оставляет в процессе использования цифровых технологий, преимущественно – в интернете. Это могут быть цифровые данные и сведения, как предоставленные самим пользователем – активный цифровой след, так и собранные автоматически – пассивный цифровой след [5].

Цифровые следы общества – влияние совокупностей данных и информации, представленных в различных цифровых формах и используемых для удовлетворения информационных потребностей пользователей – личностей (субъектов общества). Также цифровые ресурсы — это оцифрованные знания, подготовленные личностями для социального использования в обществе и зафиксированные на материальном (независимом, замкнутом или облачном) носителе.

Цифровые следы государства – влияние цифровой информации, содержащейся в государственных информационных системах, а также иных имеющихся в распоряжении государственных органов сведений и документов.

Формирование цифровых следов личности и общества, и далее их влияние происходит индуктивно – от частного к общему. Наоборот, влияние цифрового следа государства происходит преимущественно дедуктивно, то есть от общего к частному. Индукция в контексте цифровых следов означает, что общая картина складывается постепенно из множества отдельных цифровых элементов отдельных субъектов. Дедукция здесь означает, что государство создаёт в цифровом пространстве общие правила и структуры, которые затем применяются к частным случаям, в том числе при необходимости ограничения формирования и существования цифровых следов личностей и общества.

Безопасность личности, общества и государства, в том числе информационная и, конкретно, цифровая заключается в состоянии защищённости жизненно важных информационных интересов соответственно личности, общества и государства от внутренних и внешних угроз. Жизненно важные интересы — совокупность потребностей, удовлетворение которых надёжно обеспечивает существование и возможности прогрессивного развития личности, общества и государства [6]. Касательно цифровой безопасности личности можем вспомнить необходимость защиты оцифрованных

персональных данных граждан, которые представляют собой цифровые слепки реальных документальных, физических и биометрических данных.

Одна из традиционных классификаций аспектов безопасности может быть сформулирована следующим образом. Для личности – это психическая, психологическая, психиатрическая безопасность; физическая, физиологическая, медицинская безопасность; экономическая, финансовая, материальная безопасность. Для общества и государства – это духовная, цивилизационная безопасность; демографическая безопасность, воспроизводство народонаселения; экологическая, биосферная безопасность [7].

Особенности информационной безопасности личности в части защиты цифрового следа связаны с необходимостью контролировать данные, которые пользователь оставляет в интернете, и минимизировать риски, связанные с этим следом.

Основные риски, связанные с цифровым следом:

- Кража личных данных — мошенники могут использовать открытую информацию для подмен оригинальных аккаунтов, социальной инженерии или создания ложных аккаунтов;
- Утечки данных — базы с персональными данными, украденные у организаций или государственных структур, могут попасть в закрытые сегмента интернета (так называемый даркнет), затем продаваться злоумышленникам;
- Репутационные потери — старые посты (сообщения) или фото могут быть использованы для шантажа или повлиять на трудоустройство. Таргетированные (целевые) атаки — детали цифрового следа помогают создавать персонализированные ложные письма;
- Профилирование и дискриминация — организации или государственные структуры могут использовать данные для принятия локальных персонализированных решений (например, при выдаче кредитов физическим лицам);
- Нарушение приватности (частной жизни) — осуществляемый сбор данных без согласия пользователя (через отслеживание активности, специализированные приложения) может приводить к потере контроля над личной информацией.

Особенности информационной безопасности общества в части защиты цифрового следа — это комплексная задача, которая решается через сочетание законодательных мер, массовых технологий защиты и типовых рекомендаций для пользователей. Разберём каждый элемент подробнее.

1. Законодательные меры:

Законы и нормативные акты создают правовую основу для защиты персональных данных и цифрового следа граждан. Ключевые направления:

- Закрепление прав граждан: право на доступ к своим данным, их исправление и удаление («право на забвение»), отзыв согласия на обработку;

- Обязанности организаций: требования к операторам данных по обеспечению безопасности, уведомлению о утечках, локализации баз данных;
- Ответственность за нарушения: административная и уголовная ответственность за неправомерный сбор, использование и распространение персональных данных;
- Регулирование трансграничной передачи данных: ограничения на передачу данных в другие страны без гарантий защиты.

Примером соответствующих законов в России являются Федеральный закон № 152-ФЗ «О персональных данных» [8] — основной закон о защите персональных данных, а также Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [9] — он регулирует вопросы информационной безопасности в целом. Есть пример такого закона в других странах, например, GDPR (General Data Protection Regulation) в Европейском Союзе— один из самых строгих регламентов по защите данных в мире.

В качестве механизмов реализации можно привести следующее: создание регуляторов (в России — Роскомнадзор); проведение проверок и аудитов; рассмотрение жалоб граждан; блокировка ресурсов, нарушающих требования.

2. Массовые защитные технологии:

Технологические решения позволяют снизить риски на уровне инфраструктуры и сервисов.

Основные категории:

- Шифрование данных: сквозное шифрование в мессенджерах (Signal, Telegram); защищенный протокол HTTPS для веб-сайтов; шифрование баз данных;
- Средства аутентификации: двухфакторная аутентификация (2FA) для аккаунтов; биометрическая аутентификация (отпечатки пальцев, распознавание лица);
- Системы обнаружения и предотвращения вторжений (IDS/IPS): мониторинг сетевой активности для выявления подозрительных действий;
- Антивирусное и антифишинговое ПО: защита от вредоносных программ и мошеннических сайтов;
- Инструменты приватности: VPN-сервисы для маскировки IP-адреса; браузеры и расширения с усиленной защитой приватности (Firefox, Brave, uBlock Origin); анонимные сети (Tor);
- Технологии обезличивания данных: анонимизация и псевдонимизация данных перед их использованием для аналитики или машинного обучения;
- Централизованные системы мониторинга утечек: сервисы, отслеживающие появление персональных данных в даркнете и уведомляющие пользователей.

Особенности информационной безопасности государства в части защиты цифрового следа требуют комплексного подхода, который объединяет:

- Законодательные нормативно-регламентные меры — создают правовую основу и устанавливают ответственность;
- Технические средства — обеспечивают автоматизированную защиту инфраструктуры и данных;
- Организационные меры — координируют действия внутри страны и на международной арене.

В частности, отметим, что государство, в том числе, создаёт правовую базу для защиты цифрового следа граждан и организаций. Ключевые направления этого аспекта включают:

- Закрепление прав граждан: право на доступ к своим данным; право на их исправление и удаление («право на забвение»); право на отзыв согласия на обработку данных.
- Регулирование деятельности операторов данных: требования к обеспечению безопасности хранения и передачи данных; обязанность уведомлять о случаях утечек; локализация баз данных (хранение на территории страны).
- Ответственность за нарушения: административная и уголовная ответственность за неправомерный сбор, использование и распространение персональных данных; штрафы за несоблюдение требований к защите данных.
- Стандартизация: разработка национальных стандартов в области информационной безопасности (например, ГОСТ Р ИСО/МЭК); утверждение регламентов по защите критической информационной инфраструктуры.

Такой подход позволяет минимизировать риски компрометации данных, защитить критическую инфраструктуру, обеспечить безопасность граждан и укрепить суверенитет государства в цифровом пространстве.

Цифровые следы формируют идентичность и субъектность каждой личности. Каждый такой цифровой след является индивидуальным и неповторимым. Защита и безопасность цифрового следа личности должна строится на нивелировании угроз и отражении возможных атак на след с точки зрения защиты самого следа, а также с учетом необходимости защищенности цифровых следов других личностей. Цифровые следы личностей могут влиять друг на друга, в том числе с точки зрения взаимной синергии отдельных следовых эффектов, с одной стороны, и, потенциального ослабления либо разрушения таковых – с другой.

Цифровые следы общества могут быть классифицированы, исходя из поколенческих либо социально-экономических и информационно-технологических особенностей и закономерностей развития в конкретный период времени. Цифровые следы личностей в совокупности влияют или даже формируют цифровой след общества. Обратно, тренды, порожденные и сформированные обществом путем объединения (смешения, упорядочивания,

интеграции) цифровых следов существующих личностей, их составляющих, имеют линейно (по времени) отложенный зеркальный, но почти наверняка преломленный импульс. Последний влияет на формирование каркасов цифровых следов новых личностей.

Цифровые следы государства имеют накопительный и постоянно расширяющийся положительный баланс цифровых ресурсов отдельных направлений развития общества и даже отдельных личностей. Так, современный известный блогер (или писатель, или научный работник и др.) может формировать новые тренды, существенно влияющие на формирование цифровых следов многих личностей, затем общества и впоследствии государства. Множество цифровых следов личностей является вложенным, но не в единой плоскости, в цифровой след общества.

При этом цифровые следы общества и государства не являются тождественными или вложенными друг в друга. Цифровые следы государства являются консервативными по составу. Также – они всегда регламентированы.

Они не тождественны по следующим причинам:

1. Цифровой след общества складывается из действий миллионов отдельных пользователей: публикации в социальных сетях, поисковые запросы, онлайн-покупки, перемещения с включённой геолокацией, использование мобильных приложений и т.д.

2. Цифровой след государства формируется за счёт деятельности госорганов, государственных информационных систем (ГИС), официальных порталов (например, «Госуслуги»), ведомственных баз данных, систем электронного документооборота и т.п.

Также отличаются цели создания:

1. В обществе цифровые следы образуются стихийно, как побочный результат повседневной активности людей. Их основная цель — коммуникация, развлечение, решение бытовых задач.

2. Цифровые следы государства создаются целенаправленно для выполнения функций управления, учёта, контроля и предоставления государственных услуг. Они служат инструментом реализации государственной политики.

Отличия есть и по составу и структуре:

1. Цифровой след общества крайне разнороден: включает личные данные, мнения, эмоции, поведенческие паттерны, неформальные коммуникации. Он динамичен и постоянно пополняется новыми фрагментами.

2. Цифровой след государства структурирован и формализован: это реестры, базы данных, официальные документы, отчёты, статистика, нормативные акты. Его структура задаётся регламентами и стандартами.

По уровню доступности:

1. След общества может быть как открытым (публичные посты и сообщения), так и закрытым (личные переписки). Значительная часть данных доступна третьим лицам (соцсети, маркетплейсы и т.д.).

2. След государства делится на категории доступа: открытый (официальные публикации), ограниченного доступа (служебная информация) и секретный (гостайна). Доступ строго регламентирован.

Консервативность означает, что состав и структура государственных цифровых следов определяются заранее и меняются только в установленном порядке. Это проявляется, к примру, в нормативном закреплении, ограниченным кругом источников, долгосрочным хранением и постоянным контролем изменений.

Заключение

Таким образом, цифровые следы общества и государства принципиально различаются по природе, целям и механизмам формирования. След общества стихиен, многообразен и динамичен, тогда как цифровой след государства — структурирован, консервативен и жёстко регламентирован. Эта разница отражает их роли: первый — отражение частной жизни граждан, второй — инструмент государственного управления и контроля. Понимание этих различий критически важно для разработки политик информационной безопасности, защиты персональных данных и эффективного взаимодействия общества и государства в цифровой среде, в том числе при анализе (защите) цифровых следов.

Изучение проблематики инициации, сопровождения и затухания цифровых следов личности, общества, государства представляется важной современной научной задачей. Вопросы безопасности при этом занимают значительное актуальное место и требуют дополнительного содержательного анализа и подхода к определению эффективных механизмов – и прямой безопасности цифровых следов, и защиты от негативного и деструктивного влияния от некоторых из них.

Список использованных источников и литературы

1. Нестеров С.А., Смолина Е.М. Понятие цифрового следа и анализ цифрового следа в образовании // Системный анализ в проектировании и управлении. сборник научных трудов XXVI Международной научно-практической конференции. В 3 ч.. Санкт-Петербург, 2023. С. 309-314.

2. Кизима С.В., Кидалов Ф.В., Пальцин Д.А. Телекоммуникационная среда и проблематика данных цифрового следа субъектов цифрового общества // Электросвязь. 2021. № 12. С. 33-37.

3. Мазлов Н.Е., Садыков А.М. Утилизация цифровых следов как элемент корпоративной социальной ответственности (КСО) и инструмент формирования цифрового доверия // В сборнике: Цифровые технологии в развитии современных экономических систем. Материалы I Всероссийской научно-

практической конференции с международным участием. Липецк, 2026. С. 676-680.

4. Лебедев А.В. Личность и ее свойства: Учеб. пособие. СПб.: СПбГУНиПТ, 2001. – 212 с.

5. Фомичева Т.Л. Цифровой след и цифровая гигиена. // Самоуправление. 2023. № 6 (139). С. 361-363.

6. Закон РФ от 05.03.1992 N 2446-1 (ред. от 26.06.2008) – утратил силу на основании Федерального закона от 28.12.2010 №390-ФЗ.

7. Маслов А., Хает Л. Структура системной безопасности жизнедеятельности // “Станкоинструмент”. 2016. № 3 (4). С. 36-40.

8. Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ.

9. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ.

List of references

1. Nesterov S.A., Smolina E.M. The concept of digital footprint and analysis of digital footprint in education // System analysis in design and management. collection of scientific papers of the XXVI International Scientific and Practical Conference. At 3 o'clock. St. Petersburg, 2023. pp. 309-314.

2. Kizima S.V., Kidalov F.V., Paltsin D.A. Telecommunication environment and problems of digital footprint data of subjects of digital society // Electrosvyaz. 2021. No. 12. pp. 33-37.

3. Mazlov N.E., Sadykov A.M. Recycling digital traces as an element of corporate social responsibility (CSR) and a tool for building digital trust // In the collection: Digital technologies in the development of modern economic systems. Materials of the I All-Russian scientific and practical conference with international participation. Lipetsk, 2026. pp. 676-680.

4. Lebedev A.V. Personality and its properties: Proc. allowance. St. Petersburg: SPbGUNIPT, 2001. – 212 p.

5. Fomicheva T.L. Digital footprint and digital hygiene. // Self-government. 2023. No. 6 (139). pp. 361-363.

6. Law of the Russian Federation dated 03/05/1992 N 2446-1 (as amended on 06/26/2008) – lost force on the basis of Federal Law dated 12/28/2010 No. 390-FZ.

7. Maslov A., Khaet L. Structure of systemic life safety // “Stankoinstrument”. 2016. No. 3 (4). pp. 36-40.

8. Federal Law “On Personal Data” dated July 27, 2006 No. 152-FZ.

9. Federal Law “On Information, Information Technologies and Information Protection” dated July 27, 2006 No. 149-FZ.