Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.738.5:004.056:342.738:316.472.4

ЦИФРОВОЙ СЛЕД И РЕПУТАЦИЯ: ЧТО НУЖНО ЗНАТЬ ПОЛЬЗОВАТЕЛЮ О ПРИВАТНОСТИ В СЕТИ

Марчуков Андрей Дмитриевич,
студент, МГТУ имени Н.Э. Баумана, 105005, г. Москва, ул. Бауманская 2-я, д. 5, стр. 1; Marchukovv904@mail.ru

Хисматулин Тимур Дамирович,
студент, МГТУ имени Н.Э. Баумана, 105005, г. Москва, ул. Бауманская 2-я, д. 5, стр. 1; timurkh2004@yandex.ru

Суфиянов Тимур Ренатович,
студент, МГТУ имени Н.Э. Баумана, 105005, г. Москва, ул. Бауманская 2-я, д. 5, стр. 1; fa-luke16@mail.ru

Ермолаев Иван Владимирович,
студент, МГТУ имени Н.Э. Баумана, 105005, г. Москва, ул. Бауманская 2-я, д. 5, стр. 1; vaneeji@mail.ru

Аннотация

Статья посвящена анализу цифрового следа как фактора, одновременно влияющего на приватность пользователя, его социальную репутацию, устойчивость к экономическим рискам. Актуальность темы аргументируется тем, что повседневная коммуникация, потребление digital-сервисов, профессиональная самопрезентация все в большей степени переносятся в сетевую среду. А масштабы утечек персональных данных и практики проверки онлайн-профилей со стороны работодателей продолжают расширяться. Именно здесь возникает существенное противоречие: пользователь формально включен в цифровую среду добровольно, но фактически лишен полного контроля над тем, какие сведения о нем накапливаются, как долго они хранятся, в каких контекстах затем интерпретируются. Не менее значимо и другое расхождение: с одной стороны, digital-активность рассматривается как условие профессиональной и социальной видимости; с другой – тот же самый массив данных способен стать источником репутационных потерь, дискриминационных решений. Цель состоит в том, чтобы показать, каким образом цифровой след преобразуется из совокупности разрозненных сетевых действий в устойчивый репутационный и поведенческий профиль, а также определить практические меры пользовательской самозащиты. В статье разграничены активный и пассивный цифровые следы, раскрыт механизм их влияния на репутацию, приватность. Также проанализированы риски, которые возникают на пересечении социальных платформ, алгоритмической обработки данных, кадровых практик. Резюмировано, что ключевая угроза заключается не в самой публичности как таковой, а в кумулятивном эффекте, когда фрагментарные сведения объединяются в профиль, пригодный для оценки, прогнозирования, манипуляции.

Ключевые слова: виртуальная идентичность, защита персональных данных, информационная безопасность, приватность, репутация, социальные сети, цифровой след

DIGITAL FOOTPRINT AND REPUTATION: WHAT A USER NEEDS TO KNOW ABOUT ONLINE PRIVACY

Marchukov Andrey Dmitrievich,
Student, Bauman Moscow State Technical University, 2nd Baumanskaya str., 5, bldg. 1, Moscow, 105005; Marchukovv904@mail.ru

Khismatulin Timur Damirovich,
Student, Bauman Moscow State Technical University, 2nd Baumanskaya str., 5, bldg. 1, Moscow, 105005; timurkh2004@yandex.ru

Sufiyanov Timur Renatovich,
Student, Bauman Moscow State Technical University, 2nd Baumanskaya str., 5, bldg. 1, Moscow, 105005; fa-luke16@mail.ru

Ermolaev Ivan Vladimirovich,
Student, Bauman Moscow State Technical University, 2nd Baumanskaya str., 5, bldg. 1, Moscow, 105005; vaneeji@mail.ru

ABSTRACT

The article is devoted to the analysis of the digital footprint as a factor that simultaneously affects user privacy, social reputation, and resilience to economic risks. The relevance of the topic is argued by the fact that everyday communication, the consumption of digital services, and professional self-presentation are increasingly moving into the network environment. Furthermore, the scale of personal data leaks and the practice of online profile screening by employers continue to expand. It is here that a significant contradiction arises: the user is formally included in the digital environment voluntarily, but is effectively deprived of full control over what information about them is accumulated, how long it is stored, and in what contexts it is subsequently interpreted. Equally significant is another discrepancy: on one hand, digital activity is viewed as a prerequisite for professional and social visibility; on the other, the same data set can become a source of reputational losses and discriminatory decisions. The goal is to demonstrate how a digital footprint is transformed from a collection of fragmented network actions into a stable reputational and behavioral profile, and to determine practical measures for user self-protection. The article distinguishes between active and passive digital footprints, revealing the mechanism of their influence on reputation and privacy. Risks arising at the intersection of social platforms, algorithmic data processing, and HR practices are also analyzed. It is summarized that the key threat lies not in publicity itself, but in the cumulative effect, where fragmentary information is combined into a profile suitable for evaluation, forecasting, and manipulation.

Keywords: virtual identity, personal data protection, information security, privacy, reputation, social networks, digital footprint.

В эпоху масштабной интеграции информационно-коммуникационных технологий во все сферы общественной жизни концепция личной приватности претерпевает существенные системные преобразования. По существу, каждое действие индивида в виртуальном пространстве (будь то отправка электронного письма или авторизация на государственном портале) оставляет специфический электронный «маркер». Их совокупность формирует так называемый цифровой след.

Как представляется, рассматриваемый виртуальный «отпечаток» давно перестал быть сугубо технической категорией, которая интересует лишь отраслевых специалистов. Он органично перешел в разряд значимых социально-экономических факторов, в значительной степени определяющих статус человека в современном социуме. Впрочем, осведомленность рядовых граждан о механизмах сбора, хранения, последующего анализа их сетевой активности до сих пор остается на недостаточно высоком уровне [4, 9]. Вследствие этого отметим, что проблема управления персональной информацией требует академического осмысления и междисциплинарного подхода.

По-видимому, современный субъект информационных отношений не в полной мере осознает долгосрочные последствия необдуманного размещения сведений о себе. Между тем, сформированный годами электронный профиль напрямую влияет на карьерные перспективы, уровень финансовой безопасности, общую репутацию в обществе.

В академическом дискурсе и корпоративной практике принято разделять рассматриваемый феномен на две ключевые категории: активную и пассивную [4, 5, 9, 10].

Первая составляющая генерируется осознанно, когда субъект целенаправленно публикует тексты, фотографии, видеоматериалы и т. д. на различных медиаплатформах, добровольно заполняет анкеты, участвует в публичных дискуссиях.

В отличие от предыдущих подходов, которые были сфокусированы, в основном, на анализе открытых публикаций, современные исследователи уделяют повышенное внимание именно пассивной компоненте. Она формируется без прямого, осознанного участия человека (посредством агрегации файлов cookie, фиксации IP-адресов, сбора телеметрии, отслеживания геолокации, сохранения истории поисковых запросов браузера.

Примечательно, что скрыто собираемые массивы метаданных сегодня представляют наибольшую угрозу для безопасности личности, поскольку их структура, алгоритмы обработки, сроки хранения практически не контролируются самим субъектом. В сопоставлении с более ранними подходами к оценке рисков, в настоящий момент акцент смещается в сторону защиты непреднамеренно оставляемых индикаторов. Крупные корпорации и агрегаторы задействуют сложные математические модели с целью построения предиктивных профилей потребителей. И это на практике ведет к частичной или полной утрате анонимности.

Цифровая репутация стала очень важным элементом при оценивании профессиональных качеств кандидатов на вакантные должности. Грань между частной жизнью и рабочей сферой в условиях транспарентности интернета фактически стерлась [6]. По статистическим сводкам из социологического опроса Русской школы управления, 75% отечественных компаний осуществляют регулярную проверку аккаунтов потенциальных сотрудников в социальных медиа. При этом половина работодателей скрупулезно анализирует профили претендентов на руководящие позиции, а четверть организаций применяет сплошной мониторинг абсолютно всех соискателей [7].

На основании отмеченного подчеркнем: кадровые решения все чаще базируются не только на профессиональных компетенциях, но и на сетевом имидже. Около 80% нанимателей прямо заявляют о готовности отказать специалисту в трудоустройстве, если обнаруженный на его страницах контент вступает в диссонанс с корпоративной этикой.

Видимо, старые публикации, экспрессивные высказывания в комментариях, специфический визуальный материал способны оказать пролонгированное деструктивное воздействие на развитие карьеры. Известны множественные практические кейсы, когда педагогические работники были вынуждены покинуть свои должности из-за размещения личных фотоснимков в открытом доступе, а гражданские активисты сталкивались с юридическими преследованиями из-за архивных цитат многолетней давности. В увязке с обозначенным отметим, что сетевой образ требует столь же взвешенного и тщательного конструирования, как и традиционное профессиональное портфолио [2, 7].

Одновременно с этим, помимо репутационных издержек, небрежное отношение к собственной приватности влечет за собой прямые экономические угрозы. Статистика инцидентов информационной безопасности в Российской Федерации отражает выраженную негативную динамику. Согласно аналитическим данным центра Solar Aura, за первые восемь месяцев 2025 года в глобальную сеть попало порядка 13 миллиардов строк персональных данных россиян. Указанный показатель почти в четыре раза превышает суммарный объем скомпрометированной информации за весь 2024 год, когда было зафиксировано 3,5 миллиарда утекших записей [12].

В свою очередь, экспертно-аналитический центр ГК InfoWatch также фиксирует усугубление ситуации. Так, по их оценкам, из отечественных корпоративных и государственных баз за 2025 год утекло 1,581 миллиарда записей. Это отражает прирост более, чем на 30% относительно прошлогодних значений. Подразделение киберразведки F6 отмечает, что масштаб компрометации информации существенно увеличился. И основная тяжесть инцидентов пришлась на государственные платформы и коммерческий сектор. Хотя методологии подсчета у различных институтов могут варьироваться, общий эмпирический тренд не вызывает сомнений: значительные массивы личной информации систематически оказываются в распоряжении криминальных структур [1, 3, 11, 13].

Следствием подобных утечек становится закономерный всплеск мошеннических манипуляций. Преступники активно используют агрегированные профили жертв, методично объединяя разрозненные фрагменты сведений из разных открытых и теневых источников. Зная номера телефонов и родственные связи, злоумышленники реализуют многоуровневые схемы социальной инженерии, целевого фишинга. Так, по официальным сведениям Центрального банка РФ, только в первом квартале 2025 года была зафиксирована 296 591 несанкционированная финансовая операция. Доля денежных средств, которые удалось успешно возместить пострадавшим клиентам банков, снизилась до 7,6% в сопоставлении с 9,9% годом ранее [2, 8]. Разумно предположить, что в реалиях столь масштабной компрометации баз данных классические методы защиты периметра корпоративных сетей стремительно теряют свою изначальную эффективность.

С целью более детализированного понимания структуры возникающих угроз уместно рассмотреть сопоставление элементов виртуального присутствия. В приведенной ниже таблице 1 систематизированы основные параметры двух типов сетевых следов.

Таблица 1 – Сравнительная характеристика видов цифрового следа и ассоциированных рисков (составлено на основе [4, 5, 9, 10])

Параметр	Цифровой след	
	Активный	Пассивный
Способ формирования	Добровольная и осознанная публикация контента (посты, фотографии, отзывы)	Скрытый автоматизированный сбор (cookie, IP-адреса, геолокация, история поиска)

Уровень контроля субъектом	Высокий (человек может удалить или отредактировать собственные материалы)	Крайне низкий (сведения хранятся на серверах третьих лиц и аналитических корпораций)
Ключевые источники	Социальные медиа, блоги, профессиональные форумы, видеохостинги	Браузеры, мобильные приложения, интернет-магазины, smart-устройства (IoT)
Основной вектор угроз	Репутационные потери (отказ в найме, общественное осуждение, дисциплинарные взыскания)	Экономические потери (кража личности, мошенничество, ценовая дискриминация)
Методы минимизации	Самоцензура, аудит старых публикаций, строгие настройки видимости аккаунтов	Использование VPN, блокировщиков трекеров, очистка кэша, отказ от сбора геоданных

Перед тем как подвести итоги, необходимо сформулировать ряд прикладных авторских рекомендаций. Предлагаемые ниже меры призваны решить проблему фрагментарности и непоследовательности действий рядовых пользователей, обеспечивая системную защиту личного бренда. Их новизна состоит в переходе от рефлексивной модели поведения (экстренное удаление информации после инцидента) к проактивной «архитектуре» превентивного управления.

Во-первых, рекомендуется искусственно разделить виртуальное присутствие на строго профессиональный и сугубо личный сегменты. Для каждого вектора должны использоваться изолированные адреса электронной почты, разные псевдонимы, непересекающиеся контактные номера. Это решает проблему несанкционированного смешения рабочих компетенций и частной жизни в глазах потенциальных работодателей.

Во-вторых, следует не только свести к минимуму объем публикуемых достоверных фактов, но и применять методы «информационного шума». Осознанное внесение незначительных искажений в анкетные данные на развлекательных ресурсах снижает ценность собираемого профиля для дата-брокеров. Данное предложение защищает от автоматизированного скоринга и снижает эффективность социальной инженерии.

В-третьих, регулярная инвентаризация имеющихся аккаунтов, в том числе, выявление и удаление «заброшенных» профилей. Как только становится известно об утечке в сервисе, которым пользовался индивид, необходимо превентивно менять аутентификационные параметры на всех смежных площадках.

Подводя итоги, резюмируем, что феномен цифрового следа превратился в мощный инструмент влияния на судьбу и благополучие современного человека. Проанализированные статистические данные, которые касаются кратного роста объемов компрометации персональной информации и ужесточения требований работодателей к сетевому облику соискателей, доказывают: приватность больше не является естественной данностью. Она требует ежедневной, целенаправленной защиты.

Полученные в ходе работы результаты обладают научным и прикладным значением. Они демонстрируют, что технологическая эволюция заметно опережает развитие правовых механизмов обеспечения информационной безопасности и общий уровень грамотности населения. Внедрение предложенных в статье рекомендаций в корпоративные стандарты и повседневную практику поможет значительно снизить уязвимость граждан перед лицом киберугроз. В дальнейшем изучении данной проблематики представляется целесообразным сфокусироваться на анализе правовых аспектов реализации «права на забвение» и разработке алгоритмических систем оценки персональных рисков.

Список литературы:

1. Антонова, В. Объем «слитых» данных россиян в 2025 году вырос почти на 70% / В. Антонова, Е. Шокурова // URL: https://www.rbc.ru/rbcfreenews/6980d4c89a794781848ce080 (дата обращения: 11.04.2026).
2. Бондаренко, Е. Цифровой след: что это, как формируется и чем опасен / Е. Бондаренко, М. Вихрева, А. Павлова // URL: https://practicum.yandex.ru/blog/chto-takoe-cifrovoy-sled-v-internete/ (дата обращения: 11.04.2026).
3. Денисенко, А. Число утечек данных россиян за год выросло на 70%, хотя количество ИТ-инцидентов снизилось / А. Денисенко // URL: https://www.cnews.ru/news/top/2026-02-03_kolichestvo_utechek_dannyh (дата обращения: 11.04.2026).
4. Евсюков, В.В. Цифровой след пользователя – его ментальная ДНК / В.В. Евсюков, М.А. Плинская, Д.А. Евсюков // Вестник Тульского филиала Финуниверситета. – 2023. – № 1. – С. 364-368.
5. Ефимова, Л.Г. Цифровая личность как способ присутствия субъекта права в киберпространстве / Л.Г. Ефимова // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2025. – № 4 (128). – С. 32-41.
6. Ефремов, В.А. Цифровая репутация: гид для тех, кто в сети / В.А. Ефремов // Magister. – 2022. – № 1. – С. 46-54.
7. Как отдел кадров изучает профили сотрудников и кандидатов в интернете // URL: https://www.kommersant.ru/doc/7214795 (дата обращения: 11.04.2026).
8. Логинов, П. Цифровая приватность мертва: цифровой след лишает нас контроля над личными данными / П. Логинов // URL: https://blogs.forbes.ru/2025/07/17/cifrovaja-privatnost-mertva-cifrovoj-sled-lishaet-nas-kontrolja-nad-lichnymi-dannymi/ (дата обращения: 11.04.2026).
9. Миронов, В.Л. Анализ сетевой активности пользователей с использованием открытых источников сети Интернет / В.Л. Миронов // Парадигма. – 2025. – № 12-2. – С. 56-61.
10. Паутов, И.А. Цифровые следы пользователей как источник данных для предиктивной аналитики / И.А. Паутов // Интернаука. – 2025. – № 44-1 (408). – С. 54-56.
11. Утечки данных в России: 1,581 млрд скомпрометированных записей // URL: https://belinfonalog.ru/company/news/aktualnoe/utechki-dannykh-v-rossii-1-581-mlrd-skomprometirovannykh-zapisey/ (дата обращения: 11.04.2026).
12. Шокурова, Е. Объем слитых данных россиян вырос вчетверо, до 13 млрд строк / Е. Шокурова // URL: https://www.rbc.ru/society/23/09/2025/68d24e309a7947c037bff93e (дата обращения: 11.04.2026).
13. Шпунт, Я. Объемы утечек данных из российских сервисов выросли в 1,5 раза / Я. Шпунт // URL: https://www.anti-malware.ru/news/2026-02-02-121598/48889 (дата обращения: 11.04.2026).

References:

1. Antonova V., Shokurova E. The volume of "leaked" data of Russians in 2025 increased by almost 70% // URL: https://www.rbc.ru/rbcfreenews/6980d4c89a794781848ce080 (accessed: 11.04.2026).
2. Bondarenko E., Vikhreva M., Pavlova A. Digital footprint: what it is, how it is formed and why it is dangerous // URL: https://practicum.yandex.ru/blog/chto-takoe-cifrovoy-sled-v-internete/ (accessed: 11.04.2026).
3. Denisenko A. The number of data leaks of Russians for the year increased by 70%, although the number of IT incidents decreased // URL: https://www.cnews.ru/news/top/2026-02-03_kolichestvo_utechek_dannyh (accessed: 11.04.2026).
4. Evsyukov V.V., Plinskaya M.A., Evsyukov D.A. Digital footprint of a user – their mental DNA // Bulletin of the Tula branch of the Financial University. – 2023. – No. 1. – P. 364-368.
5. Efimova L.G. Digital identity as a way of presence of a subject of law in cyberspace // Courier of Kutafin Moscow State Law University (MSAL). – 2025. – No. 4 (128). – P. 32-41.
6. Efremov V.A. Digital reputation: a guide for those online // Magister. – 2022. – No. 1. – P. 46-54.
7. How the HR department studies the profiles of employees and candidates on the Internet // URL: https://www.kommersant.ru/doc/7214795 (accessed: 11.04.2026).
8. Loginov P. Digital privacy is dead: digital footprint deprives us of control over personal data // URL: https://blogs.forbes.ru/2025/07/17/cifrovaja-privatnost-mertva-cifrovoj-sled-lishaet-nas-kontrolja-nad-lichnymi-dannymi/ (accessed: 11.04.2026).
9. Mironov V.L. Analysis of user network activity using open sources of the Internet // Paradigm. – 2025. – No. 12-2. – P. 56-61.
10. Pautov I.A. Digital footprints of users as a data source for predictive analytics // Internauka. – 2025. – No. 44-1 (408). – P. 54-56.
11. Data leaks in Russia: 1.581 billion compromised records // URL: https://belinfonalog.ru/company/news/aktualnoe/utechki-dannykh-v-rossii-1-581-mlrd-skomprometirovannykh-zapisey/ (accessed: 11.04.2026).
12. Shokurova E. The volume of leaked data of Russians increased fourfold, up to 13 billion rows // URL: https://www.rbc.ru/society/23/09/2025/68d24e309a7947c037bff93e (accessed: 11.04.2026).
13. Shpunt Ya. Volumes of data leaks from Russian services increased 1.5 times // URL: https://www.anti-malware.ru/news/2026-02-02-121598/48889 (accessed: 11.04.2026).