УДК 004.35:342.7

ЦИФРОВЫЕ СЛЕДЫ В ИНТЕРНЕТЕ: УГРОЗЫ И СПОСОБЫ УПРАВЛЕНИЯ ЛИЧНЫМИ ДАННЫМИ

Субаева А.К., доктор экономических наук, доцент,
subaeva.ak@mail.ru
Цветлюк Д.А., магистрант, reintaru@yandex.ru
ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ»
Александрова Н.Р., кандидат экономических наук, доцент,
anr73@mail.ru
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *цифровой след, персональные данные, приватность, кибербезопасность, цифровая идентификация, правовое регулирование, сокрытие данных.*

Представлены результаты системного анализа цифровых следов как уникальных идентификационных паттернов, создаваемых на основе данных об устройстве, браузере и поведенческих характеристиках пользователя. Исследование базируется на типологии приватно-ориентированного поведения и концепции «сокрытия» цифровых следов, позволяющей блокировать нежелательные логические выводы о персональных характеристиках. Выявлены правовые проблемы, связанные с неопределённостью статуса цифровых следов в РФ и отсутствием пропорционального регулирования. Предложена четырёхуровневая модель управления цифровыми следами с учётом компромисса между приватностью и персонализацией.

Введение. Каждый пользователь интернета оставляет цифровые следы – совокупность данных, фиксируемых при взаимодействии с веб-ресурсами, приложениями и IoT-устройствами. Эти данные формируют детализированный цифровой профиль личности [1, 2]. Согласно определению А.Н. Мочалова (2024), цифровой след – это «зафиксированная с помощью цифровых устройств информация о

взаимодействии индивида с компьютерной системой», практически всегда содержащая сведения о частной жизни [2, с. 165].

В зарубежной науке ключевые исследования посвящены цифровой идентификации (Musa et al., 2025) [1], концепции сокрытия следов (Goethals et al., 2025) [6, 7] и типологии приватно-ориентированного поведения (Muhammad et al., 2024) [5]. В российской науке проблематика разрабатывается преимущественно в русле конституционного и информационного права [2, 3, 8].

Цель исследования – системный анализ угроз, связанных с цифровыми следами, и разработка научно-обоснованных рекомендаций по управлению персональными данными.

Материалы и методы исследования. Теоретическая база включает: концепцию цифровых отпечатков (Musa et al., 2025) об эволюции трекинга от простых браузерных куков до сложных методов цифрового отпечатывания, использующих машинное обучение [1]; концепцию сокрытия (Goethals et al., 2025) о фундаментальном компромиссе между приватностью и персонализацией [6, 7]; типологию пользовательского поведения (Muhammad et al., 2024) [5]; правовой анализ цифровых следов (Мочалов, 2024 [2]; Соловкин, 2025 [8]).

Методы: контент-анализ научной литературы, сравнительно-правовой анализ, систематизация методов защиты, моделирование.

Результаты исследований и их обсуждение.

Цифровые следы классифицируются по способу формирования: активные (осознанные действия пользователя) и пассивные («цифровая тень», сбор данных без участия человека). Пассивные следы представляют наибольшую угрозу, поскольку пользователь часто не подозревает об их сборе [8, с. 452].

Систематизация основных источников (на основе [1, 5, 9]) представлена в таблице 1.

На основе анализа источников выделены следующие категории угроз, связанных с цифровыми следами:

1. Цифровая идентификация и слежка без согласия. Современные методы цифрового отпечатывания позволяют отслеживать пользователей на разных платформах без их ведома. «Цифровые отпечатки создают значительные риски для приватности» [1, p. 1].

2. Социальная инженерия и таргетированный фишинг. На основе цифровых следов можно предсказывать личностные характеристики, что используется для вредоносных действий [6, p. 152].

3. Предиктивное профилирование и дискриминация. По данным Goethals et al. (2025), по цифровым следам (лайки, транзакции, записи смартфона) с высокой точностью выводятся политические взгляды, религиозные убеждения [6, p. 350].

4. Финансовое мошенничество и кража идентичности. Злоумышленники создают «цифрового двойника» для оформления кредитов и доступа к счетам [9].

Таблица 1 – Основные источники цифровых следов

Источник	Тип следа	Ключевые риски
Социальные сети	Активный/пассивный	Профилирование, таргетирование, социальная инженерия
Поисковые системы	Пассивный	Профиль интересов, таргетированная реклама
Мобильные приложения	Пассивный	Несанкционированный доступ к приватным данным
IoT-устройства	Пассивный	Взлом, шпионаж, сбор данных о бытовых привычках

На основе обобщения данных из источников проведён сравнительный анализ эффективности различных методов защиты. Результаты представлены в таблице 2.

Ключевой вывод Goethals et al. (2025): существует фундаментальный компромисс между приватностью и персонализацией – чем эффективнее защита от нежелательных выводов, тем сильнее снижается точность желательной персонализации [6, p. 358].

Анализ [2, 8] выявляет следующие правовые проблемы, связанные с цифровыми следами в РФ:

1. Неопределённость правового статуса – законодательство о персональных данных (№ 152-ФЗ) не регулирует сбор цифровых следов.

2. Отсутствие презумпции приватности – необходимо закрепить, что цифровой след всегда содержит информацию о частной жизни [2, с. 165].

3. Массовое цифровое слежение – «непропорциональное ограничение права на неприкосновенность частной жизни» [2, с. 178].

4. Предлагаемые решения: право запрещать автоматизированное предоставление сведений; право отказа от рекомендательных технологий; законодательные гарантии недопустимости массового слежения [2, с. 179–180]; расширение понятия «цифровой след физического лица» [8, с. 453].

Таблица 2 − Эффективность методов защиты цифровых следов

Метод защиты	Эффективность (по шкале 0–100%)	Основные ограничения
Настройка приватности в соцсетях	40–50%	Защищает только от других пользователей; платформа сохраняет доступ к данным
Режим инкогнито в браузере	15–20%	Не скрывает геолокацию, не блокирует трекеры, не защищает от fingerprinting
Блокировщики рекламы и трекеров	70–80%	Требуют регулярного обновления; неэффективны против продвинутого fingerprinting
Использование VPN	60–70%	Скрывает IP, но не предотвращает сбор поведенческих данных на уровне приложений
Регулярная чистка старых аккаунтов	65–75%	Трудоёмкий процесс; данные могут сохраняться в архивах и кэше поисковых систем
Сокрытие цифровых следов (cloaking)	50–80% (снижается со временем)	Требует технической сложности; снижает качество персонализации

На основе синтеза подходов [1, 2, 5–7] предложена четырёхуровневая модель:

1. Аудит – инвентаризация аккаунтов, проверка утечек.

2. Очистка и ограничение – удаление неиспользуемых аккаунтов, настройка приватности.

3. Техническая защита – блокировщики трекеров, приватные поисковики, VPN.

4. Цифровая гигиена – минимизация публикуемых данных, критическое отношение к доступам, регулярное обучение [6, p. 152].

Заключение. Цифровые следы – многомерный феномен, позволяющий с высокой точностью выводить интимные характеристики личности, что создаёт риски дискриминации и слежки. Существует фундаментальный компромисс между приватностью и

персонализацией: сокрытие нежелательных выводов препятствует желательным. Правовое регулирование цифровых следов в РФ находится в стадии формирования; необходимо закрепление специального правового режима, включая презумпцию принадлежности к сфере частной жизни. Эффективная защита требует комплексного подхода – сочетания технических средств, поведенческих практик и правовой осведомлённости. Перспективное направление – разработка автоматизированных систем сокрытия, особенно на основе «мета-признаков».

Библиографический список:

1. Musa, A., Vishi, K., Martiri, E., Rexha, B. Our Digital Traces in Cybersecurity: Bridging the Gap Between Anonymity and Identification // IEEE Access. – 2025. – Vol. 13. – P. 46909–46924. DOI: 10.1109/ACCESS.2025.3553690.

2. Мочалов, А.Н. Цифровые следы человека и неприкосновенность частной жизни / А.Н. Мочалов // Антиномии. – 2024. – Т. 24, вып. 4. – С. 164–189. DOI: 10.17506/26867206_2024_24_4_164.

3. Серова, А.А. Цифровой след как объект правовой охраны: правовые и этические аспекты / А.А. Серова // Молодой учёный. – 2026. – № 4 (607). – С. 357–359.

4. Muhammad, S.S., Dey, B.L., Bala, H., Alwi, S.F., Asaad, Y. A Typology and Model of Privacy- and Security-Concerned Users‘ Attitudes Towards Digital Footprints // Journal of the Association for Information Systems. – 2024. – Vol. 25, Iss. 5. – P. 1240–1273. DOI: 10.17705/1jais.00893.

5. Goethals, S., Matz, S., Provost, F., Martens, D., Ramon, Y. The Impact of Cloaking Digital Footprints on User Privacy and Personalization // Big Data. – 2025. – Vol. 13, No. 5. – P. 345–363. DOI: 10.1089/big.2024.0036.

6. Ketipov, R., Schnalle, R., Doukovska, L., Dehez, D. Managing Cybersecurity: Digital Footprint Threats // Cybernetics and Information Technologies. – 2024. – Vol. 24, No. 3. – P. 151–162. DOI: 10.2478/cait-2024-0030.

7. Соловкин, С.В. Цифровые следы в эпоху киберфизических систем / С.В. Соловкин // Цифровые технологии в системе публично-правовых отношений. - 2025. - С. 451-459.

8. Баишев, Д. А. Особенности расследования кибермошенничества / Д. А. Баишев // Молодой ученый. - 2025. - № 20 (571). - С. 375-378

DIGITAL TRACES ON THE INTERNET: THREATS AND METHODS OF PERSONAL DATA MANAGEMENT

Subaeva A.K., Tsvetlyuk D.A.
Kazan National Research Technical University named after A.N. Tupolev – KAI
Alexandrova N.R.
FSBEI HE Ulyanovsk SAU

Keywords: *digital trace, personal data, privacy, cybersecurity, digital identification, legal regulation, data concealment.*

This article presents the results of a systemic analysis of digital traces as unique identification patterns created based on device, browser, and user behavioral data. The study is based on the typology of privacy-oriented behavior and the concept of "concealing" digital traces, which allows blocking unwanted logical inferences about personal characteristics. Legal issues related to the ambiguity of the status of digital traces in the Russian Federation and the lack of proportionate regulation are identified. A four-tier model for managing digital traces is proposed, taking into account the trade-off between privacy and personalization.