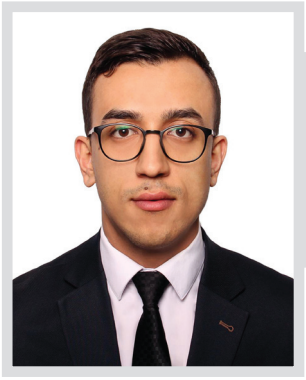
УДК 378.147.88
DOI: 10.24412/1998-5533-2025-2-68-75

Ключевые проблемы и вызовы при внедрении цифрового следа в современной цифровой среде



Миннебаев Г.Ф.
Аспирант Центра перспективных экономических исследований Академии наук Республики Татарстан (Казань)

Стремительный рост объёмов данных, создаваемых пользователями и организациями, ускоряет совершенствование бизнес-процессов и персонализацию сервисов, но обостряет риски безопасности, конфиденциальности и нормативного регулирования. Массовые утечки, манипуляции алгоритмами и непрозрачность обработки данных подчёркивают необходимость внедрять комплексные стратегии управления цифровыми следами.

Цель исследования – выявить основные проблемы и вызовы, возникающие при использовании цифровых следов, а также предложить рекомендации, обеспечивающие их безопасное и эффективное применение в бизнесе и государственных структурах.

Задача исследования включает изучение ключевых рисков, связанных с обработкой данных, в том числе утечек информации, киберугроз, вопросов конфиденциальности и этических аспектов, а также анализ их влияния на цифровую среду.

Научная и практическая значимость исследования определяется выявлением актуальных угроз, связанных с цифровыми следами и разработкой методов их защиты, что способствует снижению потенциальных рисков и укреплению доверия к цифровым технологиям. Достигнутые результаты могут быть применены для усовершенствования механизмов управления данными в организациях, формирования нормативных актов и повышения уровня осведомлённости пользователей о защите личной информации.

Ключевые слова: *цифровые следы, безопасность данных, конфиденциальность, правовое регулирование, утечки информации, кибер-угрозы, искусственный интеллект, Big Data*

Для цитирования: *Миннебаев Г.Ф. Ключевые проблемы и вызовы при внедрении цифрового следа в современной цифровой среде // Вестник экономики, права и социологии. 2025. № 2. С. 68–75. DOI: 10.24412/1998-5533-2025-2-68-75.*

Рост объёмов информации делает цифровые следы ключевым инструментом для оптимизации бизнес-процессов и управленческих решений. Организации активно используют данные пользователей и устройств для создания продуктов и услуг, адаптированных под индивидуальные запросы. Источниками информации становятся социальные медиа, логи, метаданные транзакций и данные IoT-устройств. Однако накопление больших данных и применение аналитических алгоритмов порождают риски, связанные с безопасностью, конфиденциальностью и влиянием на поведение пользователей.

Проблематика цифровых следов широко исследуется зарубежными учёными. Дж. Хайндс и А. Джоинсон рассматривают, как данные, оставляемые в сети, используются людьми и алгоритмами для прогнозирования личностных характеристик [1]. В. Арья, Д. Сети и Дж. Пол изучают влияние

цифровых следов, зафиксированных мобильными приложениями брендов, на пользовательский опыт и привязанность к компании [2]. Д.С. Гхош, П.Ч. Мишра и Т. Прадхан анализируют сложности удаления цифровых следов в контексте нормативного регулирования [3].

Этические аспекты обработки данных детально рассматриваются в работах Г.Э. Ориахи и А. Бухари. Исследователи подчеркивают важность защиты конфиденциальности, безопасности и ответственности при обработке данных. Они изучают цифровые следы, формируемые в результате онлайн-активности, включая взаимодействие в социальных сетях, историю посещений, финансовые транзакции и работу *IoT*-устройств, для персонализации сервисов и таргетированной рекламы, акцентируя внимание на прозрачности, согласии пользователей и корпоративной этике [4].

Среди российских исследований, посвящённых цифровому следу, выделяется работа В.В. Мантуленко, в которой рассматриваются перспективы его использования в сфере высшего образования. Автор анализирует вопросы преемственности между уровнями обучения, организацией и управлением учебным процессом, а также путей совершенствования образовательной системы [5].

Конституционно-правовые аспекты защиты частной жизни в контексте сбора, хранения и обработки данных изучает А.Н. Мочалов. В своём исследовании он рассматривает нормативно-правовые механизмы регулирования данной области и возможные риски, связанные с конфиденциальностью персональной информации [6]. Весомый вклад в изучение цифрового профиля внесли Е.В. Виноградова, Т.А. Полякова и А.В. Минбалеева. Их работы посвящены анализу механизмов формирования цифрового профиля, особенностям его правового регулирования и социальным вызовам, возникающим на фоне стремительного развития цифровых технологий [7].

Методологические подходы к выявлению, фиксации и изъятию цифровых следов преступлений, оставленных в социальных сетях и мессенджерах, рассматриваются в исследовании Е.Р. Россинской и Т.А. Саакова. В центре внимания находится разработка эффективных методов обработки цифровых доказательств, имеющих важное значение в борьбе с киберпреступностью [8].

Каждое взаимодействие пользователя или компании с онлайн-сервисами, мобильными приложениями, умными устройствами и другими технологическими решениями приводит к формированию цифрового следа [9]. В современном мире этот поток данных становится ценным источником информации о клиентском поведении, особенностях спроса, логистических процессах, финансовых операциях и многих других аспектах.

Наряду с этим возникают серьёзные вызовы, связанные с безопасностью, конфиденциальностью, правовым регулированием, качеством обработки и этическими аспектами использования данных. Компании стремятся максимально эффективно применять собранные сведения, однако увеличение числа кибератак и масштабных утечек подтверждает необходимость ответственного и комплексного подхода к сбору и хранению цифровых следов. Практические примеры, иллюстрирующие уязвимости, позволяют оценить масштаб возникающих проблем, представленных в таблице 1.

В начале 2024 г. произошла утечка персональных данных клиентов «*Ticketmaster*», вызвавшая широкий общественный резонанс: в открытый доступ попало 500 млн записей, содержащих имена, *e-mail* адреса, почтовые адреса, телефоны и частичные данные банковских карт; это стало крупнейшим подобным инцидентом на тот момент [12]. Особенно уязвимым остаётся онлайн-ритейл, где хранится обширный массив данных о клиентах: контактные сведения, история покупок, адреса доставки и платёжная информация. Попав в руки злоумышленников, такие сведения могут использоваться для фишинговых атак, мошенничества или перепродажи в теневых сегментах интернета. За последние годы утечки затронули пользователей многих популярных сервисов, включая поставщиков готовой еды и маркетплейсы. Широкий общественный отклик вызвали случаи несанкционированного доступа к данным клиентов служб доставки. Некоторые компании предпочитают не раскрывать факт кибератаки, однако практика показывает, что подобные инциденты неизбежно становятся известны, нанося ущерб репутации и финансовому положению бизнеса.

Серьёзные угрозы наблюдаются и в медицинском секторе. Информация о пациентах, включая диагнозы и назначения, может представлять интерес не только для мошенников, но и для тех, кто использует её в целях шантажа или дискредитации. Несколько крупных лабораторий и медицинских сервисов уже столкнулись с утечками, в результате которых миллионы записей оказались в открытом доступе. Хакеры проникают в базы данных через уязвимости в программном обеспечении, прибегают к методам социальной инженерии для обмана сотрудников или намеренно блокируют доступ к медицинским данным, требуя выкуп. Подобные атаки особенно опасны, поскольку в сфере здравоохранения задержка в доступе к информации может повлечь за собой критические последствия для жизни пациентов [13].

Человеческий фактор остаётся одним из наиболее уязвимых звеньев. Массовая рассылка писем и сообщений, внешне выглядящих как уведомления от службы безопасности различных сервисов, часто приводит к тому, что сотрудники сами передают злоумышленникам свои учетные данные. Методы

Таблица 1

Утечки персональных данных: масштабные инциденты 2019–2025 гг. [10; 11]

Дата	Название утечки	Объем данных	Описание
Октябрь 2019 г.	Сбербанк	60 млн кредитных карт	Продажа базы клиентов с кредитными картами, утечка через инсайдера
Май 2020 г.	СДЭК	466 млн + 822 млн. строк	Несколько крупных утечек базы клиентов и заказов курьерской службы
Январь 2022 г.	Госуслуги (*COVID*-19)	48 млн записей о вакцинации	Утекли данные вакцинации россиян, полученные через уязвимость *API*
Февраль 2022 г.	Яндекс.Еда	58000 клиентов	Данные клиентов сервиса доставки (телефоны, адреса, заказы)
Осень 2022 г.	Citymobil	3,9 млн клиентов, 80 тыс. водителей	Утечка клиентской базы агрегатора такси
Май 2022 г.	Гемотест	31 млн записей пациентов	Компрометация медицинских данных клиентов лаборатории
2023 г.	СберСпасибо, Спортмастер и др.	52,5 млн. записей	Серии взломов баз данных крупных компаний
Сентябрь 2023 г.	МТС Банк	1 млн клиентов	Компрометация клиентов банка, включая ИНН и частично маскированные карты
Весна 2023 г.	Kassy.ru, СОГАЗ, Золото 585	22,7 млн записей	Утечки клиентских данных из разных сфер торговли и услуг
Лето-осень 2023 г.	Ашан, Leroy Merlin, ТВОЕ и др.	Много миллионов (не раскрыто)	Широкая волна утечек в ритейле и интернет-торговле
Начало 2024 г.	Неизвестная база (500 млн. записей)	500 млн записей	Крупнейшая утечка в истории России – 500 млн записей
Начало 2024 г.	Достаевский	3 млн записей	Утекли данные клиентов и сотрудников сервиса доставки
Март 2024 г.	*DNS*	Несколько млн записей	Компрометация базы клиентов *DNS*
Январь 2025 г.	Ростелеком	154 тыс. *e-mail*, 101 тыс. телефонов	Компрометация данных клиентов из-за подрядчика
Январь 2025 г.	Альфа-Страхование-Жизнь	500 тыс. клиентов	Хакеры украли данные страховой компании, включая телефоны и *e-mail*

социальной инженерии стремительно развиваются: одним из распространённых способов мошенничества является так называемая схема «фейкового босса», при которой взламывается или имитируется аккаунт руководителя. Уверенные в подлинности обращения, подчинённые выполняют запросы, связанные с разглашением конфиденциальных сведений или сомнительными финансовыми операциями. Даже при наличии многоуровневых механизмов аутентификации люди нередко становятся жертвами тщательно продуманных атак, использующих поддельные, но визуально достоверные сообщения.

Сбор избыточного объёма данных без чёткого уведомления пользователей ставит под угрозу конфиденциальность и приватность. В результате многие не осознают, насколько детальная информация о них сохраняется, включая историю перемещений или переписки в чатах технической поддержки. Если такие сведения становятся достоянием общественности, правовые и репутационные последствия оказываются серьёзными: люди обнаруживают, что их личные данные доступны на подпольных платформах. В ряде случаев выясняется, что компании хранили информацию гораздо дольше установленного срока, а меры по её своевременному удалению или анонимизации не предпринимались [14].

В 2019 г. Ассоциация больших данных при поддержке Института развития интернета инициировала разработку и подписание «Кодекса этики использования данных». К нему присоединились крупнейшие представители *IT*-отрасли, банковского сектора и телекоммуникаций, включая «Яндекс», Сбербанк, МТС, «Ростелеком» и *VK*. Документ закрепляет ключевые принципы обработки информации: законность сбора, уважение прав личности, обеспечение защиты данных и предотвращение злоупотреблений. Компании, подписавшие кодекс, обязуются не использовать персональные сведения во вред гражданам, не собирать ненужную информацию и поддерживать прозрачность политики конфиденциальности [15].

Вопросы безопасности особенно значимы для финансового сектора, однако статистика показывает, что доля утечек, затрагивающих банковскую сферу, остаётся относительно невысокой. Несмотря на это, в 2023 г. объём компрометированных персональных данных в мире увеличился вдвое, достигнув 47,24 млрд записей [16]. Даже единичный случай взлома клиентской базы приводит к серьёзным репутационным потерям, что иллюстрирует рисунок 1.

Когда информация об уязвимостях банка становится достоянием общественности, клиенты начинают сомневаться в безопасности своих средств. Взломы могут происходить не только из-за технических проблем, но и вследствие организационных

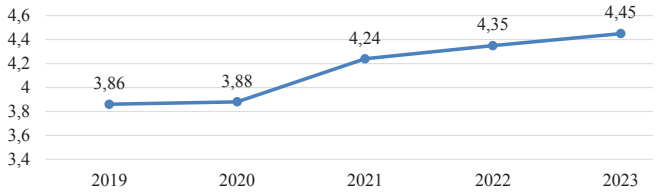


Рис. 1. Динамика роста средней стоимости утечек данных в мире, 2019–2023 гг., млн долл. [17–20]

ошибок: неправильной настройки хранилищ, использования слабых паролей, недостаточной сегментации сетевой инфраструктуры [21]. Современные методы шифрования позволяют значительно повысить уровень защиты, однако без регулярного аудита безопасности, особенно среди подрядчиков и контрагентов, риск утечек возрастает в самых неожиданных местах.

Обсуждение этических аспектов обработки данных приобретает всё большую актуальность. В одном из случаев алгоритм, обученный на исторических резюме, начал проявлять дискриминацию при найме сотрудников: мужские кандидатуры получали приоритет, в то время как женские занизились в рейтинге [22]. Закреплённые в исходных данных предубеждения автоматически перенеслись в систему. Подобные ошибки возможны и при кредитном скоринге или страховых оценках, если алгоритм использует некорректные параметры или искажённые выборки. В результате отдельные люди получают отказы в услугах без чёткого объяснения причин, а компания оказывается в центре скандала, вынужденно опровергая обвинения в предвзятости.

Широкое внедрение систем распознавания лиц вызывает серьёзные опасения, поскольку они формируют масштабные базы биометрических данных. Один из стартапов оказался в центре скандала, когда выяснилось, что в его распоряжении находится до 50 млрд изображений пользователей, собранных без их согласия. Данный случай продемонстрировал, что подобные практики могут привести к обвинениям в нарушении права на частную жизнь [23]. В отдельных странах регуляторы признали такие действия незаконными и наложили значительные штрафы, однако сам принцип создания глобальных баз лиц остаётся предметом споров, затрагивающих вопросы возможной слежки и риска дискриминации, как узаконенной, так и несанкционированной.

Ещё одной проблемой остаётся качество данных, используемых в аналитических системах, и вероятность ложных сигналов. В корпоративных базах нередко встречаются дубликаты, устаревшие записи и некорректно заполненные поля. Если алгоритмы обучаются на таких наборах, возрастает риск ошибочных прогнозов и решений, основанных на случайных корреляциях. Один из примеров – система, предназначенная для предсказания вспышек гриппа на основе поисковых запросов. Со временем её точность снизилась из-за «переобучения». Отсутствие регулярной проверки информации и понимания принципов работы алгоритмов может привести к тому, что компании выстраивают маркетинговые стратегии или принимают управленческие решения, опираясь на ошибки машинного обучения.

Быстрый рост цифровых следов делает традиционные методы хранения и анализа данных малоэффективными. Современные технологии, такие как распределённые файловые системы, *NoSQL*-базы, кластеры *Hadoop* и *Spark*, а также облачные платформы, уже стали стандартом для крупных компаний. Однако малый и средний бизнес не всегда имеет возможность внедрять такие решения. В результате формируется технологический разрыв: одни организации получают конкурентные преимущества за счёт развитой аналитики, в то время как другие остаются на периферии цифровой трансформации [24].

Важную роль играет и культурный аспект. Даже при наличии современных технологий, таких как системы *Big Data* и модули искусственного интеллекта, отсутствие доверия к аналитическим данным со стороны руководства или сотрудников может свести эффективность их использования к нулю [24]. Если управленцы продолжают опираться на привычные схемы работы, игнорируя алгоритмические рекомендации, инвестиции в цифровые решения оказываются неэффективными. Скептицизм некоторых менеджеров, считающих, что алгоритмы «не учитывают специфики бизнеса», приводит к тому, что решения по-прежнему принимаются интуитивно, а потенциал сложных аналитических инструментов остаётся нереализованным.

Сфера правового регулирования также сталкивается с трудностями из-за стремительного развития цифровых технологий [25]. Во многих странах механизмы аудита алгоритмов остаются недостаточно проработанными, отсутствуют детализированные стандарты анонимизации и псевдонимизации, а реализация пользовательских прав, таких как право на забвение или получение копии персональных данных, оказывается затруднительной. Тем не менее судебные разбирательства и наложенные штрафы свидетельствуют о том, что законодательные органы всё чаще принимают жёсткие меры в отношении компаний, нарушающих принципы конфиденциальности или допустивших утечки большого масштаба.

Вопрос «двойного использования» данных становится всё более актуальным, когда информация, собранная с одной целью, например для улучшения сервисов, применяется в других областях, таких как кредитный скоринг или маркетинговые кампании. Часто пользователи не осознают, что их цифровая активность способна повлиять на принятие решений о предоставлении займа. Если согласие на такие действия не получено заранее, а политика об-

работки остаётся непрозрачной, подобная практика может восприниматься как введение клиентов в заблуждение, что создаёт репутационные риски и вероятность судебных разбирательств.

Разобщённость внутри компании также становится причиной снижения эффективности работы с данными. Использование разнородных баз и различных форматов хранения в разных подразделениях усложняет выполнение обязательств перед клиентами, например, полное удаление информации по запросу. В результате один и тот же пользователь может оказаться зарегистрированным в нескольких системах, а попытки унифицировать данные сопровождаются техническими и организационными сложностями. Отсутствие единой платформы затрудняет контроль за тем, какая информация хранится о каждом человеке, какие меры защиты применяются, кто имеет доступ к определённым сегментам [26].

Феномен «*data overload*» (с англ. перегрузка данными) характеризуется тем, что предприятия сталкиваются с таким объёмом информации, что теряют способность эффективно выделять ключевые сигналы. В условиях, когда аналитики вынуждены тратить значительное время на очистку и подготовку данных, дорогостоящие технологии машинного обучения не дают ожидаемых результатов. Что усиливает потребность в квалифицированных специалистах – инженерах данных, аналитиках, экспертах по информационной безопасности [27]. Высокий спрос на такие кадры существенно превышает предложение, что приводит к росту их рыночной стоимости.

Этические вопросы обработки цифровых следов становятся предметом активных дискуссий, особенно в контексте баланса между «полезной персонализацией» и скрытым манипулированием. Маркетинговые алгоритмы могут использовать уязвимости пользователей, такие как склонность к азартным играм или зависимость от кредитных продуктов, для показа таргетированной рекламы. Когда подобные стратегии становятся достоянием общественности, это вызывает негативную реакцию. Некоторые крупные компании создают внутренние комитеты по этике искусственного интеллекта, которые проводят аудит алгоритмов, оценивая их на предмет дискриминации и вторжения в личное пространство.

В основе многих рисков лежит корпоративная культура. Сопротивление изменениям, отказ от прозрачного управления данными и практика сокрытия утечек значительно усложняют внедрение ответственного подхода к использованию цифровых следов. Однако примеры передовых организаций подтверждают, что компании, ориентированные на защиту интересов пользователей, извлекают из данных максимальную ценность. Что способствует укреплению доверия клиентов и партнёров, снижает вероятность судебных разбирательств и минимизирует возможные репутационные потери в случае инцидента [28]. В целом проблемы и вызовы, возникающие при внедрении цифровых следов в современной среде, можно свести к нескольким основным категориям, таблица 2.

Таким образом, внедрение цифровых следов в деятельность современных организаций предо-

Таблица 2

Основные проблемы и вызовы применения «цифровых следов» в экономике организаций

Категория проблемы	Описание проблемы	Возможные последствия	Возможные решения
Юридические и нормативные риски	Размытые законодательные нормы, противоречия в регулировании обработки цифровых следов	Нарушение законов о защите персональных данных, штрафы, судебные иски	Разработка и внедрение чётких стандартов обработки данных; соблюдение *Regulation (EU)* 2016/679 от 27.04.2016 г. «*On the protection of natural persons with regard to the processing of personal data…» (GDPR*) и Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»
Конфиденциальность и приватность	Использование данных клиентов, сотрудников без их ведома. Возможность слежки и контроля	Репутационные потери, недоверие со стороны клиентов и персонала, возможные иски	Введение прозрачной политики конфиденциальности, сбор согласий на обработку данных
Безопасность данных	Высокий риск утечек, взломов, кибератак, компрометация цифровых следов	Финансовые потери, утрата конкурентных преимуществ, возможные штрафы от регуляторов	Инвестирование в кибербезопасность, регулярные аудиты ИБ, мониторинг аномальной активности
Этические аспекты	Возможность дискриминации на основе цифровых следов, манипуляция поведением клиентов	Нарушение прав пользователей, снижение доверия, репутационные скандалы	Внедрение этических стандартов работы с данными, независимые аудиты алгоритмов
Качество данных	Некорректные, устаревшие, неполные цифровые следы, ошибки в алгоритмах	Ошибочные бизнес-решения, снижение эффективности маркетинговых стратегий	Развитие системы валидации данных, внедрение AI-алгоритмов для очистки данных

Продолжение таблицы 2

Категория проблемы	Описание проблемы	Возможные последствия	Возможные решения
Персонализация vs Интрузивность	Баланс между удобством персонализации услуг и чрезмерным вторжением в частную жизнь клиентов	Отток клиентов, негативные отзывы, снижение лояльности	Оптимизация алгоритмов персонализации, прозрачное управление пользовательскими настройками
Доступность технологий	Высокая стоимость внедрения и поддержки технологий работы с цифровыми следами	Недоступность для малого и среднего бизнеса, технологическое неравенство	Развитие облачных решений, субсидии и гранты на цифровизацию бизнеса
Человеческий фактор	Ошибки персонала, недостаточная подготовка к работе с цифровыми следами	Утечки информации, неправильное использование данных, репутационные риски	Тренинги, программы повышения цифровой грамотности сотрудников
Двойное использование данных	Цифровые следы, собранные для одной цели (например, маркетинга), могут быть использованы для другой (например, кредитного скоринга) без ведома пользователей	Юридические риски, потеря доверия клиентов, возможные судебные иски	Разработка строгих политик управления данными, прозрачное информирование клиентов
Отсутствие стандартизации	Разные компании используют цифровые следы по-разному, отсутствуют единые форматы хранения и обработки данных	Трудности интеграции данных между системами, несовместимость платформ, замедление цифровизации	Разработка отраслевых стандартов работы с цифровыми следами, унификация форматов данных
Перегрузка данных («data overload»)	Из-за огромного объема цифровых следов сложно выделить полезную информацию	Снижение эффективности аналитики, потери в бизнес-решениях, рост затрат на обработку данных	Внедрение систем Big Data, AI-аналитики, фильтрации и агрегации данных
Цифровой разрыв (Digital Divide)	Разные организации и регионы имеют разный уровень доступа к технологиям анализа цифровых следов	Рост неравенства между крупными и малыми бизнесами, отставание в цифровой трансформации	Государственные программы поддержки цифровизации, доступ к облачным технологиям
Недостаточная прозрачность алгоритмов	Компании используют цифровые следы в системах AI и Big Data, но не раскрывают принципы работы алгоритмов	Потеря доверия, риск необоснованных решений, например, отказ в кредите из-за непрозрачного скоринга	Внедрение этических принципов AI, аудит и объяснимость алгоритмов
Фрагментация данных	Цифровые следы могут храниться в разных системах, без единого централизованного хранилища	Потеря данных, сложности в управлении, снижение эффективности работы с клиентами	Создание унифицированных дата-центров, интеграция систем
Риск монополизации данных	Крупные компании (Google, Meta, Amazon) обладают доступом к огромному количеству цифровых следов, что создает дисбаланс	Ограничение конкуренции, рост зависимости бизнеса от крупных платформ.	Государственное регулирование, развитие национальных платформ для работы с данными
Цифровая идентификация и подмена личности	Использование цифровых следов для создания фальшивых идентичностей, мошеннических действий	Рост киберпреступности, финансовые и репутационные риски	Развитие биометрической идентификации, многофакторная аутентификация
Эрозия анонимности	Все больше данных пользователей отслеживается, уменьшается возможность сохранять конфиденциальность в сети	Социальные протесты, возможные законодательные запреты на отслеживание	Разработка этических принципов использования данных, внедрение технологий приватности (Zero-Knowledge Proof)

Источник: составлено автором.

ставляет широчайшие возможности: от точного прогнозирования продаж и оптимизации логистики до качественной персонализации сервисов. Однако эти возможности идут рука об руку с множеством проблем и вызовов. Масштабные утечки данных, рост стоимости киберинцидентов, отсутствие единых правовых норм, этические дилеммы, нехватка квалифицированного персонала и технологические ограничения – все эти факторы формируют сложный ландшафт, в котором бизнесу приходится адаптироваться.

Литература:

1. Hinds J., Joinson A. Human and computer personality prediction from digital footprints // Current Directions in Psychological Science. 2019. Т. 28. № 2. P. 204–211. DOI: 10.1177/096372141982784.
2. Arya V., Sethi D., Paul J. Does digital footprint act as a digital asset? – Enhancing brand experience through remarketing // International Journal of Information Management. 2019. Т. 49. P. 142–156. DOI: 10.1016/j.ijinfomgt.2019.03.013.
3. Sarkar Ghosh D., Mishra P. C., Pradhan T. The conundrum of erasing digital footprints: A regulatory challenge // Jindal Global Law Review. 2024. Т. 15. № 1. P. 25–59. DOI: 10.1007/s41020-024-00223-5.
4. Oriakhi H.E., Buhari A. Ethical Implications of Digital Footprinting: Privacy, Security, and Accountability // Digital Adaptability and Crisis Management for Sustainable Development: Conference Proceedings. 2024. P. 25–59.
5. Мантуленко В.В. Перспективы использования цифрового следа в высшем образовании // Преподаватель XXI век. 2020. № 3–1. С. 32–42. DOI: 10.31862/2073-9613-2020-3-32-42.
6. Мочалов А.Н. Цифровые следы человека и неприкосновенность частной жизни // Антиномии. 2024. Т. 24. № 4. С. 164–189. DOI: 10.17506/26867206_2024_24_4_164.
7. Виноградова Е.В., Полякова Т.А., Минбалеев А.В. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации // Правоприменение. 2021. Т. 5. № 4. С. 5–19. DOI: 10.52468/2542-1514.2021.5(4).5-19.
8 Россинская Е.Р., Сааков Т.А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 106–123. DOI: 10.24411/2587-9820-2020-10060.
9. Гайдаш О.В. Феномен цифрового следа в современном обществе // Вестник магистратуры. 2020. № 6 (105). С. 10–12.
10. Неманова В.И., Вакурин И.С., Маклачкова В.В., Гадасин Д.В. Определение экономической эффективности затрат предприятия на защиту персональных данных // DSPA: Вопросы применения цифровой обработки сигналов. 2024. № 3. С. 37–45.
11. Белова А.А., Щербинина У.Е. О способе предотвращения хищения данных клиентов в электронной коммерции // Advances in Science and Technology. 2022. С. 139–141.
12. Norman G. Most recent data breaches in 2024: updated stats. URL: https://preyproject.com/blog/worst-data-security-breaches (дата обращения: 10.02.2025).
13. Seh A.H., Zarour M., Alenezi M., Sarkar A.K., Agrawal A., Kumar R., Ahmad Khan R. Healthcare data breaches: insights and implications // Healthcare. MDPI, 2020. Т. 8. № 2. P. 2–18. DOI: 10.3390/healthcare8020133.
14. Деев С.А. Цифровые следы и их защита // XLVIII межд. науч. конф. «Исследования молодых ученых». Казань, ноябрь 2022. С. 1–7. URL: https://moluch.ru/conf/stud/archive/466/17564.
15. Крупнейшие российские компании подписали Кодекс этики использования данных. URL: https://www.sostav.ru/publication/krupnejshie-rossijskie-kompanii-podpisali-kodeks-etiki-ispolzovaniya-dannykh-40927.html#:~:text= (дата обращения: 10.02.2025).
16. Утечки данных. URL: https://www.tadviser.ru/index.php/Статья:Утечки_данных (дата обращения: 10.02.2025).
17. Потери от утечек данных. URL: https://www.tadviser.ru/index.php/Статья:Потери_от_утечек_данных (дата обращения: 10.02.2025).
18. В отчете IBM Security говорится, что утечка данных обходится компаниям дороже, чем прежде. URL: https://dsmedia.pro/analytics/v-otchete-ibm-security-govoritsja-chto-utechka-dannyh-obhoditsja-kompanijam-dorozhe-chem-prezhde (дата обращения: 10.02.2025).
19. Отчёт IBM: личная информация клиентов и сотрудников – главные жертвы утечек. URL: https://www.securitylab.ru/news/540308.php (дата обращения: 10.02.2025).
20. IBM: средняя стоимость взлома достигла рекордных $ 4,88 миллионов в 2024 году. URL: https://10guards.com/ru/blog/2024/07/31/ibm-average-breach-costs-hit-record-4-88m-in-2024-up-10-from-last-year/ (дата обращения: 10.02.2025).
21. Jimmy F.N.U. Cybersecurity Threats and Vulnerabilities in Online Banking Systems // International Journal of Scientific Research and Management (IJSRM). 2024. № 12(10). P. 1631–1646. DOI: 10.18535/ijsrm/v12i10.ec10.
22. Dastin J. Insight – Amazon scraps secret AI recruiting tool that showed bias against women. URL: https://www.reuters.com/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG (дата обращения: 17.04.2025).
23. Фирма Clearview собрала в соцсетях миллиарды фото лиц. Полиция в США обращалась к её базе миллион раз. URL: https://informburo.kz/stati/firma-clearview-sobrala-v-socsetyax-milliardy-foto-lic-policiya-v-ssa-obrashhalas-k-eyo-baze-million-raz (дата обращения: 11.02.2025).
24. Maroufkhani P., Wan Ismail W.K., Ghobakhloo M. Big data analytics adoption model for small and medium enterprises // Journal of Science and Technology Policy Management. 2020. Т. 11. № 4. P. 483–513.
25. Трусов Н.А., Елисеева В.С. Правовое регулирование и опыт реализации цифровых проектов в регионах Российской Федерации // Труды Академии управления МВД России. 2022. № 4 (64). С. 42–51. DOI: 10.24412/2072-9391-2022-464-42-51.

26. Kumar S. Data Silos: A Roadblock for aiops // arXiv preprint arXiv:2312.10039. 2023. 2024 IJRTI. T. 9. № 1. P. 33–39.
27. Лягошина Т.В. Большие языковые модели: влияние на публичный дискурс и общество в целом // Вестник Московского университета. Серия 10. Журналистика. 2024. Т. 79. № 1. С. 15–25. DOI: 10.30547/vestnik.journ.1.2024.1525.
28. Tabaghdehi S.A.H. Ethical Governance of Digital Footprint Data: A Journey Towards a Responsible Society // Business Strategies and Ethical Challenges in the Digital Ecosystem. Emerald Publishing Limited, 2024. P. 369–379.

Key Issues and Challenges Associated With Implementing a Digital Footprint in Today's Digital Environment

Minnebaev G.F.
Academy of Sciences of the Republic of Tatarstan (Kazan)

The rapid expansion of data produced by users and organizations is accelerating business process optimization and service personalization, yet it heightens risks to security, privacy, and regulatory compliance. Widespread breaches, algorithmic manipulation, and opaque processing underscore the need for comprehensive strategies to manage digital footprints.

The aim of the study is to identify the main issues and challenges arising from the use of digital footprints and to propose recommendations to ensure their safe and effective application in business and government.

The research objective includes examining the key risks associated with data processing, including information leaks, cyber threats, privacy issues and ethical aspects, as well as analyzing their impact on the digital environment.

The scientific and practical significance of the research is determined by the identification of current threats associated with digital footprints and the development of methods to protect them, which helps to reduce potential risks and strengthen trust in digital technologies. The results achieved can be applied to improve data governance mechanisms in organizations, shape regulations, and increase user awareness of personal information protection.

Keywords: digital footprints, data security, confidentiality, legal regulation, data breaches, cyber threats, artificial intelligence, Big Data