Научная статья
УДК 34.03
NIION: 2022-0089-4/25-362
MOSURED: 77/27-031-2025-04-362
EDN: https://elibrary.ru/UYVAZM

Защита персональных данных в цифровом пространстве: современные правовые вызовы и пути их решения

Алена Владимировна Степаржевская[1], Елена Евгеньевна Томилина[2]
[1,2] Государственный университет управления, Москва, Россия
[1] linaavs@yandex.ru
[2] eetomilina@mail.ru

Аннотация. Анализируются существующие правовые нормы, регулирующие защиту персональных данных пользователей в Интернете. Выявляются пробелы и противоречия в современном российском законодательстве. Рассматриваются проблемы несанкционированного доступа, утечек данных и способов повышения эффективности правовых механизмов для обеспечения конфиденциальности личности в условиях быстрого развития технологий.
Ключевые слова: цифровое пространство, персональные данные, кибербезопасность, угрозы личной безопасности, правовые основы защиты информации
Для цитирования: Степаржевская А. В., Томилина Е. Е. Защита персональных данных в цифровом пространстве: современные правовые вызовы и пути их решения // Судебная экспертиза и исследования. 2025. № 4. С. 202–206.

Original article

Personal data protection in the digital space: modern legal challenges and solutions

Alena V. Steparzhevskaya[1], Elena E. Tomilina[2]
[1,2] State University of Management, Moscow, Russia
[1] linaavs@yandex.ru
[2] eetomilina@mail.ru

Abstract. The existing legal norms governing the protection of users' personal data on the Internet are analyzed. The gaps and contradictions in modern Russian legislation are revealed. The problems of unauthorized access, data leaks and ways to increase the effectiveness of legal mechanisms to ensure personal confidentiality in the context of rapid technology development are considered.
Keywords: digital space, personal data, cybersecurity, threats to personal security, legal framework for information protection
For citation: Steparzhevskaya A. V., Tomilina E. E. Personal data protection in the digital space: modern legal challenges and solutions. Forensic science and research. 2025;(4):202–206. (In Russ.).

Введение. Развитие цифрового пространства в современных условиях формирует большую доступность информации и возможность получения услуг и сервисов в онлайн-режиме. Использование данного инструмента активизируется ежегодно, пользователями сети Интернет по всему миру на сентябрь 2025 г. являлось 5,65 млрд человек, что на 200 млн больше, чем годом ранее [1]. Расширение доступности информации при всех его социальных и экономических преимуществах обладает рядом угроз, связанных с нарушением ограниченности доступа к личным данным пользователей, которые могут быть использованы мошенниками для совершения преступлений. В таких условиях защита персональных данных в цифровом пространстве становится одной из приоритетных задач для государств и бизнеса, поскольку стремительное развитие технологий и растущие объемы обрабатываемой информации создают новые вызовы для правового регулирования.

Особенно актуально это в условиях ужесточения международных санкций, нарастания киберугроз и пересмотра законодательных норм, что требует от субъектов данных гибкости и своевременного реагирования на изменения в правовом поле. Наряду с этим, усиление требований к безопасности персональных данных в 2025 г., в том числе введение новых категорий данных с особым режимом обработки и ужесточение ответственности за нарушения, свидетельствуют о новом этапе формирования цифровой правовой культуры, где баланс между защитой прав

граждан и интересами бизнеса становится гораздо более тонким и комплексным. Такой контекст диктует необходимость углубленного анализа современных правовых вызовов и поиска эффективных механизмов их преодоления, способных обеспечить как технологический прогресс, так и гарантию неприкосновенности частной жизни в цифровом обществе.

Основная часть. Определение понятия «персональные данные» представлено в научной литературе достаточно широко. Следует отметить существование нормативного закрепления термина в Федеральном законе № 152-ФЗ, где под ним понимается «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)» [2]. В соответствии с требованиями законодательства под данную категорию попадает любая информация, относящаяся к прямо или косвенно определенному физическому лицу, включая фамилию, имя, отчество, дату рождения, контакты, биометрию, IP-адреса и пр. Законом вводятся категории: общедоступные, специальные и биометрические данные, которые относятся к персональным данным и требуют обеспечения мер по и защите.

В специальных исследованиях, опубликованных отечественными учеными, персональные данные представляются в информации, позволяющей установить личность прямо или косвенно (фамилия, имя и отчество, документы, контакты, биометрия, а также данные о здоровье). В частности, в работе Д. М. Назарова и К. М. Саматова [3] под исследуемым термином поднимаются сведения, с помощью которых можно однозначно определить личность, включая как документальные, так и цифровые идентификаторы. Данный подход видится достаточно обоснованным и отражает необходимость обеспечения защиты данных как на бумажном, так и на электронном носителе. Близкую трактовку понятия «персональные данные» приводит И. Г. Шаблинский: «любая информация, напрямую или косвенно относящаяся к физическому лицу, необходимая для правовой защиты и регулирования обработки» [4]. В данном определении более детализирован правовой аспект работы с личными данными человека, которые требуют сохранности в условиях цифрового пространства.

С. Н. Тагаева и Э. М. Гатиятуллина [5] отмечают, что персональные данные — это многогранная категория, предположительно включающая традиционные идентификаторы и поведенческие характеристики, требующие усиленной охраны. Данный подход видится достаточно обоснованным и включает аспект обеспечения сохранности личной информации, которая обеспечивается нормативными требованиями.

Современные определения дополняются такими категориями, как поведенческие характеристики и данные о местоположении. Перечисленные выше авторы отмечают выраженную тенденцию расширения перечня персональных данных и усиления защиты, в то время как законотворческие изменения акцентируют внимание на необходимости точного и однозначного согласия субъекта и строгом соблюдении правил обработки данных. Обобщая вышесказанное, можно сформулировать следующее определение понятия: персональные данные — это любая информация, которая относится к конкретному физическому лицу (субъекту персональных данных), прямо или косвенно идентифицирующая этого человека или позволяющая его идентифицировать, включает имя, фамилию, дату рождения, адрес, контактные и биометрические данные, сведения о здоровье, финансовую информацию, а также любые другие аспекты, которые в совокупности или по отдельности позволяют установить личность субъекта.

Исходя из выделенного представления о содержательной части персональных данных, изучены аспекты их правового регулирования. По определению, приведенному в работе С. С. Рудика, А. Е. Антоненко, М. А. Танова и И. В. Петрова [6], защита персональных данных рассматривается как совокупность мер по охране информации, связанной с конкретным лицом, обеспечиваемая законодательством и судебной практикой. Представленный подход видится достаточно обоснованным и полноценным, поскольку включает в себя правовой и организационный аспекты. В. Г. Наборщиков [7] акцентирует внимание на необходимости оценки эффективности мер защиты персональных данных, как ключевого критерия результативности принимаемых действий. Указанный подход представляется адекватным, поскольку позволяет избежать формального использования правовых инструментов для соблюдения безопасности граждан, гарантированных Конституцией Российской Федерации, в том числе и в цифровом пространстве.

Основным нормативным актом, регулирующим защиту персональных данных, является Федеральный закон № 152-ФЗ [2], который в 2025 г. подвергся значительным изменениям, направленным на ужесточение требований к локализации данных, расширение перечня случаев обработки без согласия субъек-

та, а также к усилению контроля и отчетности операторов данных перед государственными органами. В частности, увеличены штрафные санкции, как для юридических лиц, так и для индивидуальных предпринимателей, что способствует стимулированию выработки более строгих мер информационной безопасности и минимизации рисков утечек и неправомерного использования данных. Вместе с тем законодательные нововведения предусматривают введение обязательной аккредитации операторов при работе с биометрическими данными, запрет на отказ в обслуживании при отказе предоставления таких данных, а также строгое регулирование порядка получения и оформления согласия субъектов на обработку персональной информации.

Несмотря на законодательные усилия, практика показывает, что вопросы несанкционированного доступа к персональным данным и их утечки остаются актуальной угрозой, обусловленной как техническими уязвимостями, так и недостаточной правоприменительной практикой. В частности, в исследованиях агентства РБК [8] отмечается тенденция на ужесточение мер юридической ответственности, включая новации в уголовном законодательстве за данную категорию преступлений, как следствие роста утечек данных. По материалам, опубликованным агентством «PT Security», специализирующимся на информационной безопасности, «каждая вторая успешная атака на организации в I полугодии 2024 г. привела к утечке конфиденциальных данных. При этом атаки на финансовые организации и медицинские учреждения приводили к утечке чаще всего — данные были украдены в четырех из пяти успешных атак на организации этих отраслей» [9]. Представленные данные наглядно отражают уровень угроз персональным данным, которые не могут быть решены исключительно в правовом поле и требуют технических новаций, регулируемых, в том числе и на законодательном уровне.

Несмотря на введение ужесточенных норм законодательства в 2025 г. [10, с. 184], включая значительное повышение штрафов за нарушения в области защиты персональных данных, а также расширение требований к локализации и безопасности информации, на практике сохраняются сложности с пресечением фактов несанкционированного доступа, которые часто связаны с недостаточной подготовкой операторов данных и несовершенством инфраструктуры защиты. Последствия таких инцидентов, по мнению автора статьи, могут быть катастрофическими как для самих субъектов данных, чей персональный мир подвергается риску раскрытия, так и для юридических лиц, сталкивающихся с репутационными и финансовыми потерями, что порождает необходимость всестороннего пересмотра комплексных механизмов безопасности и ответственности, на что обращают внимание в своей работе Г. В. Гарбузов и А. А. Теренин [10, с. 189].

Кроме того, ключевыми проблемами остаются несовершенство процедуры уведомления контролирующих органов о фактах утечек, из-за чего снижается оперативность реагирования и эффективность предотвращения дальнейших инцидентов, а также сложность в обеспечении баланса между необходимостью использования новых технологических решений и сохранением конфиденциальности данных, на чем акцентируют внимание в своей работе Г. Ф. Миннибаев [11]. Вследствие этого, несмотря на рост законодательных требований и усиление контроля, практика нарушения правил хранения персональных данных остается достаточно распространенной, что ставит под сомнение достаточность текущих мер и указывает на потребность в развитии как технических, так и правоприменительных инструментов. Следовательно, решение проблем несанкционированного доступа и утечек невозможно без синергии усилий государства, бизнес-сообщества и научного сообщества, направленных на создание инновационных систем защиты, совершенствование нормативной базы и повышение общей культуры информационной безопасности.

Обобщая вышесказанное, можно сделать вывод о том, что использование устаревших систем защиты, недостаток квалифицированного персонала и сложности в обеспечении непрерывного мониторинга создают благоприятные условия для злоумышленников, что вынуждает пересматривать подходы к правовому регулированию. Кроме того, выявляется проблема несвоевременного уведомления Роскомнадзора о фактах утечек, что снижает оперативность реагирования и минимизации последствий для пострадавших субъектов данных. Согласно данным ведомства, в 2024 г. оно получило 200 уведомлений об утечках, тогда как в 2023 г. их было 380, что свидетельствует о некотором улучшении ситуации; однако, вместе с этим, эксперты подчеркивают, что фактическое количество инцидентов может быть значительно выше из-за того, что многие организации не всегда своевременно уведомляют контролирующий орган, опасаясь репутационных или финансовых последствий [12].

Зафиксированное количество утечек данных в 2024 г. составило 135 случаев, в результате которых было скомпрометировано более 710 млн записей о гражданах России, что значительно превышает показатели предыдущих лет и указывает на рост масштабов проблемы несмотря на снижение количества зарегистрированных инцидентов. При этом, согласно законодательству (п. 3.1 ст. 21 Федерального закона № 152-ФЗ) компании обязаны уведомлять Роскомнадзор о произошедших утечках в течение 24 часов, в противном случае им грозят значительные штрафы, достигающие до 3 млн руб. для юридических лиц. Тем не менее, практика показывает, что несвоевременные уведомления не редки, что обусловлено не только недостатками систем внутреннего контроля компаний, но и отсутствием строгого мониторинга и эффективных механизмов принуждения к соблюдению норм. Аналитики указывают [8], что несвоевременное информирование Роскомнадзора снижает эффективность мер по минимизации ущерба, поскольку усложняет проведение расследований и ограничивает возможности вовлечения правоохранительных органов на ранних стадиях инцидентов. В итоге, данная проблема создает негативное воздействие как на правообладателей персональных данных, так и на рынок информационной безопасности в целом, подчеркивая необходимость не только усиления контроля и наказаний, но и развития превентивных механизмов, направленных на повышение ответственности и прозрачности операторов персональных данных, а также формирования у них культуры своевременного и полного выполнения обязательств по уведомлению регулятора.

Для адекватного противодействия современным угрозам предлагается внедрение комплексного подхода, включающего как технологические, так и нормативные меры. В частности, необходимо усиление требований к сертификации систем защиты информации, развитие института государственного контроля и аудита операторов персональных данных, а также совершенствование механизмов взаимодействия между правоохранительными органами и бизнес-сообществом. Важным аспектом является повышение правовой грамотности как специалистов, так и обычных пользователей, внедрение обязательного обучения работников, контактирующих с персональными данными. Помимо этого, рекомендуется расширение сферы применения методов анонимизации и обезличивания данных, что позволит снизить риски нарушения конфиденциальности при обработке больших массивов информации.

Заключение. Таким образом, несмотря на существенное развитие правового регулирования в области защиты персональных данных в России, остаются значительные вызовы, связанные с обеспечением полноценной конфиденциальности в цифровом пространстве, что негативно сказывается на обеспечении безопасности личной информации. Решение данных проблем требует системного подхода, объединяющего законодательные инициативы, технологические инновации и повышение общественного сознания, что позволит добиться сбалансированного взаимодействия между развитием цифровых сервисов и защитой прав граждан на неприкосновенность личной информации.

Список источников

1. 22 Internet Usage Statistics 2025 [Worldwide Data] // URL: https://www.demandsage.com/internet-user-statistics/

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ (в ред. от 7 июля 2025 г. № 200-ФЗ) «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 3. Ч. 1. Ст. 3451.

3. Назаров Д. М., Саматов К. М. Основы обеспечения безопасности персональных данных в организации: учеб. пособие. Екатеринбург, 2019.

4. Шаблинский И. Г. Правовое регулирование информационных отношений в сфере обработки персональных данных: учеб. пособие. М., 2023.

5. Тагаева С. Н., Гатиятуллина Э. М. Большие данные и персональные данные: правовая природа и вопросы регулирования // Digital law journal. 2024. Т. 5. № 2.

6. Рудик С. С., Антоненко А. Е., Танов М. А., Петров И. В. Защита персональных данных в гражданско-правовых отношениях // Журнал прикладных исследований. 2025. № 5. С. 152–159.

7. Наборщиков В. Г. Обзор подходов к проведению оценки эффективности принимаемых мер защиты персональных данных // Вестник науки. 2025. Т. 2. № 6 (87). С. 2681–2685.

8. Персональные данные: новая уязвимость в условиях цифровой экономики // URL: https://companies.rbc.ru/news/dj7lXAJwVh/personalnyie-dannyie-novaya-uyazvimost-v-usloviyah-tsifrovoj-ekonomiki/?ysclid=mf5587tp5r48709087

9. Утечки конфиденциальных данных из организаций — 1-е полугодие 2024 // URL: https://www.ptsecu-

rity.com/ru-ru/research/analytics/utechki-dannyh-aktualnye-ugrozy-pervogo-polugodiya-2024-dlya-organizaczij/#id1

10. Гарбузов Г. В., Теренин А. А. Проблемы дефиниций и постановки целей защиты от утечек информации ограниченного доступа // International Journal of Open Information Technologies. 2024. № 5. Т. 12. С. 184–191.

11. 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.

12. РКН: в 2024 г. большинство утечек произошло в сфере торговли и услуг // URL: https://tass.ru/obschestvo/23065521

References

1. 22 Internet Usage Statistics 2025 [Worldwide Data] // URL: https://www.demandsage.com/internet-user-statistics/

2. Federal Law No. 152-FZ of July 27, 2006 (as amended dated July 7, 2025, No. 200-FZ) «On Personal Data» // Collection of Legislation of the Russian Federation. 2006. No. 3. P. 1. Art. 3451.

3. Nazarov D. M., Samatov K. M. Fundamentals of personal data security in the organization: textbook. Yekaterinburg, 2019.

4. Shablinsky I. G. Legal regulation of information relations in the field of personal data processing: textbook. M., 2023.

5. Tagaeva S. N., Gatiyatullina E. M. Big data and personal data: legal nature and regulatory issues // Digital law journal. 2024. Vol. 5. No. 2.

6. Rudik S. S., Antonenko A. E., Tanov M. A., Petrov I. V. Protection of personal data in civil law relations // Journal of Applied Research. 2025. No. 5. P. 152–159.

7. Naborshchikov V. G. Review of approaches to assessing the effectiveness of measures taken to protect personal data // Bulletin of Science. 2025. No. 6 (87). Vol. 2. P. 2681–2685.

8. Personal data: a new vulnerability in the digital economy // URL: https://companies.rbc.ru/news/dj7lXAJwVh/personalnyie-dannyie-novaya-uyazvimost-v-usloviyah-tsifrovoj-ekonomiki/?ysclid=mf5587tp5r48709087

9. Confidential data leaks from organizations — 1st half of 2024 // URL: https://www.ptsecurity.com/ru-ru/research/analytics/utechki-dannyh-aktualnye-ugrozy-pervogo-polugodiya-2024-dlya-organizaczij/#id1

10. Garbuzov G. V., Terenin A. A. Problems of definitions and setting goals for protection against leaks of limited access information // International Journal of Open Information Technologies. 2024. Vol. 12. No. 5. P. 184–191.

11. Minnebaev G. F. Key problems and challenges in the implementation of the digital footprint in the modern digital environment // Bulletin of Economics, Law and Sociology. 2025. No. 2. P. 68–75.

12. RKN: in 2024, the majority of leaks occurred in the field of trade and services // URL: https://tass.ru/obschestvo/23065521

Информация об авторах

А. В. Степаржевская — магистрант Института государственного управления и права Государственного университета управления;

Е. Е. Томилина — доцент кафедры частного права Государственного университета управления, кандидат юридических наук, доцент.

Information about the authors

A. V. Steparzhevskaya — Master's Student of the Institute of Public Administration and Law of the State University of Management;

E. E. Tomilina — Associate Professor of the Department of Private Law of the State University of Management, Candidate of Legal Sciences, Associate Professor.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 30.09.2025; одобрена после рецензирования 07.10.2025; принята к публикации 14.10.2025.
The article was submitted 30.09.2025; approved after reviewing 07.10.2025; accepted for publication 14.10.2025.