Т. 12. №2 2026
https://doi.org/10.33619/2414-2948/123

УДК 343.9 https://doi.org/10.33619/2414-2948/123/60

ОСОБЕННОСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА РЕЖИМНЫХ ОБЪЕКТАХ РФ

*©**Доровских К. Ю**., ORCID: 0009-0005-2189-4562, Томский государственный университет, г. Новосибирск, Россия, rusheshnikovak@mail.ru*

PERSONAL DATA PROTECTION IN RESTRICTED ACCESS FACILITIES IN THE RUSSIAN FEDERATION

*©**Dorovskikh K**., ORCID: 0009-0005-2189-4562, Tomsk State University, Novosibirsk, Russia, rusheshnikovak@mail.ru*

Аннотация. Исследуются правовые, организационные и технические особенности защиты персональных данных на режимных объектах Российской Федерации. Рассмотрены базовые нормы Федерального закона № 152-ФЗ «О персональных данных», особенности обработки данных сотрудников силовых органов, требования пропускной системы, применение биометрии и журнального учёта. Проанализированы судебные решения и проблемы взаимодействия закона о персональных данных и законодательных актов о гостайне. Сделаны предложения по гармонизации правовых норм в целях усиления защиты и минимизации правовых коллизий.

Abstract. The article examines the legal, organizational, and technical features of personal data protection at facilities operating under a special security regime within the Russian Federation. It reviews the foundational norms of Federal Law No. 152-FZ on personal data, the specifics of processing data of security personnel, access control system requirements, the use of biometrics, and log-keeping practices. Court decisions are analyzed, and the interplay between personal data law and state secrecy legislation is investigated. Proposals for harmonizing legal norms to strengthen protection and reduce legal conflicts are offered.

Ключевые слова: режимные объекты, персональные данные, защита, биометрия, пропускной режим, государственная тайна

Keywords: special security facilities, personal data, protection, biometrics, access control, state secrecy

Режимные объекты (объекты с усиленным режимом доступа) определены Указом Президента РФ как те, «на которых ведутся работы с использованием сведений, составляющих государственную тайну» [1]. Обработка персональных данных на таких объектах сопровождается повышенными рисками: наряду с обычной ответственностью по закону о персональных данных (152-ФЗ) могут действовать нормы об охране государственной тайны, нормативные акты ФСБ и спецслужб, внутренние инструкции. Цель настоящего исследования — выявить юридические вызовы и особенности, которые необходимо учитывать при защите персональных данных именно в контексте режимных объектов, и предложить пути минимизации правовых противоречий.

Задачи статьи: проанализировать нормы 152-ФЗ, имеющие особое значение для режимных объектов; рассмотреть организационные и технические меры, применяемые на

Т. 12. №2 2026
https://doi.org/10.33619/2414-2948/123

таких объектах; проанализировать судебную практику по защите персональных данных (особенно в контексте силовых структур); выработать предложения по гармонизации нормативной базы.

В исследовании был выполнен нормативно-правовой анализ — исследование положений 152-ФЗ, смежных законов, указов и постановлений. Источники включают законодательство, официальные акты, материалы судебной практики (в т.ч. решения ВС и разъяснения), публикации в юридической науке.

1. Законодательные особенности обработки персональных данных для режимных объектов.

Ст. 6 152-ФЗ, ч. 1.1, предусматривает, что обработка данных объектов государственной охраны и лиц, подлежащих защите, осуществляется с учётом особенностей, предусмотренных законом о государственной охране [2]. Это положение прямо относит часть персональных данных, обрабатываемых на режимных объектах, к особой категории и требует дополнительной нормативной базы.

Закон №152-ФЗ допускает случаи обработки без согласия субъекта (ч. 3 ст. 6), если это предусмотрено федеральным законом или необходимостью исполнения задач безопасности, что часто применяется к сотрудникам силовых органов и персоналу закрытых объектов [3].

В 2022 г принят ФЗ №572-ФЗ «Об обязательной биометрической идентификации в Единой биометрической системе», что усиливает контроль при входе на территорию режимных объектов через биометрические данные. Во многих нормативных актах ФСБ, ФСТЭК, служба безопасности предприятиях вводят дополнительные требования к шифрованию, разграничению прав доступа, журналам посещений, системы видеонаблюдения и т.д.

2. Организационные и технические меры защиты.

Системы контроля доступа и биометрия. На режимных объектах применяют биометрические системы (отпечаток пальца, скан лица, радужная оболочка) для входа, что снижает риск использования чужих пропусков. Журналы пропуска: ведутся бумажные или электронные журналы, с записью ФИО, цели визита, времени входа/выхода, ответственного лица. Журналы хранятся в охране и подлежат строгому хранению по регламенту.

Сегментация информационных систем и криптографическая защита. Информационные системы персональных данных (ИСПДн), используемые на таких объектах, должны соответствовать классу защиты «особо важный» или «критический», с многоуровневой авторизацией, шифрованием, аудитом доступа.

Правила разграничения доступа: доступ к персональным данным предоставляется только тем сотрудникам, чья должность этого требует (принцип необходимости).

Контроль и аудит. Периодические проверки, внутренние аудиты безопасности, система реагирования на инциденты (утечки, попытки несанкционированного доступа).

3. Судебная практика и правовые споры.

Верховный Суд РФ разъяснил, что Роскомнадзор вправе выступать истцом от имени неопределённого круга лиц в спорах о защите персональных данных, что позволяет контролирующему органу защищать ПД даже без индивидуального иска [4].

В ряде дел суды признавали незаконной обработку персональных данных при размещении ФИО и адресов без согласия (например, публикация задолженностей по коммуналке) [5].

Некоторые решения отклонили требования об автоматическом признании контактов (номер телефона, e-mail) персональными данными, если они не связаны с идентификацией лица (без ФИО) [6].

Т. 12. №2 2026
https://doi.org/10.33619/2414-2948/123

В судебной практике встречаются случаи, когда режимная защита данных допускается как ограничение, необходимое государственным интересам, но суды тщательно проверяют обоснованность таких ограничений [7-9].

Проблемы и правовые коллизии.

Конфликт норм 152-ФЗ и законодательства о гостайне. В некоторых случаях режимные объекты обрабатывают персональные данные, которые одновременно относятся к информации с грифом «секретно». Возникают вопросы: насколько нормы о защите ПД применимы, если данные уже защищены как гостайна?

Неоднозначность правового основания обработки без согласия. Закон допускает обработку без согласия в определённых случаях, но на практике возникают споры, суды проверяют, соответствует ли подобное исключение законодательству и задачам безопасности.

Прозрачность и информирование субъектов. Субъекты ПД (сотрудники, посетители) должны быть информированы о целях и способах обработки, даже если объект закрытый, что создает риск разглашения внутренней структуры безопасности.

Риски утечек и инцидентов. На режимных объектах последствия утечки персональных данных особенно серьёзны. Необходимы механизмы реагирования и ответственности, учитывающие повышенный риск.

Рекомендации

Разработать специальные поправки к 152-ФЗ для режимных объектов — юридически чёткие основания обработки без согласия, с обязательным контролем.

Ввести обязательную сертификацию ИСПДн для объектов с режимом особого доступа и единые стандарты по криптографической защите.

Уточнить обязанности по информированию субъектов ПД на закрытых объектах — возможно, посредством внутреннего соглашения, разграничивая, какие сведения могут сообщаться.

Усилить ответственность за нарушения (в том числе дисциплинарную, административную) — с учётом специфики режимных объектов.

Проводить обучение персонала, аудит безопасности и план реагирования на инциденты, адаптированный для режимных условий.

Заключение

Защита персональных данных на режимных объектах РФ — задача особой сложности. Здесь сталкиваются нормы 152-ФЗ и законодательство о гостайне, требования к безопасности и право граждан на защиту их данных. Практика показывает, что усиление контроля (биометрия, контроль доступа) эффективно, но необходимо юридически чёткое закрепление оснований обработки, прозрачные механизмы информирования и строгий надзор. Дальнейшие исследования могут быть направлены на детализацию стандарта защиты данных для объектов с грифом «секретно» и выработку унифицированной методики оценки рисков в подобных режимах.

Нормативные правовые акты:

(1). Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) (в ред. от 1 июля 2020 г.) // Российская газета. 2020. 4 июля.

(2). Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных» (в ред. от 24 июня 2025 г.) // Собрание законодательства РФ. 2006. №31. Ст. 3451.

Т. 12. №2 2026
https://doi.org/10.33619/2414-2948/123

(3). Федеральный закон от 21 июля 1993 г. №5485-1 «О государственной тайне» (в ред. от 29 декабря 2023 г.) // Российская газета. 2024. 10 янв.

(4). Федеральный закон от 29 декабря 2022 г. №572-ФЗ «Об осуществлении идентификации и аутентификации физических лиц с использованием биометрических персональных данных» // Собрание законодательства РФ. 2023. №1. Ст. 41.

(5). Федеральный закон от 8 августа 2024 г. №249-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части обработки персональных данных Федеральной службой безопасности Российской Федерации» // Российская газета. 2024. 13 авг.

(6). Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесённых к государственной тайне» (в ред. от 24 июня 2025 г.) // Собрание законодательства РФ. 1995. №49. Ст. 4775.

(7). Постановление Правительства РФ от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных без использования средств автоматизации» // Собрание законодательства РФ. 2008. №38. Ст. 4326.

(8). Постановление Пленума Верховного Суда РФ от 9 ноября 2020 г. №АКПИ20-171 «О судебной защите прав субъектов персональных данных» // Российская газета. 2020. 12 нояб.

Список литературы:

1. Бачило И. Л. Право и информационные технологии: проблемы соотношения // Журнал российского права. 2021. №6. С. 45-53.

2. Гаврилов Э. П. Правовое регулирование персональных данных: комментарий к Федеральному закону №152-ФЗ. М.: Юрайт, 2023. 240 с.

3. Гончаренко Л. А. Персональные данные: проблемы защиты и ответственность за их нарушение. СПб.: Питер, 2022. 198 с.

4. Михайлова О. С. Режимные объекты как элемент системы национальной безопасности // Государственная власть и местное самоуправление. 2024. №5. С. 77-83.

5. Савельев А. И. Персональные данные и кибербезопасность. М.: Статут, 2023. 356 с.

6. Тихомиров Ю. А. Информационное право России. М.: Норма, 2020. 416 с.

7. Чернышева Е. Н. Государственная тайна и режим ограниченного доступа. М.: Инфра-М, 2021. 304 с.

8. General Data Protection Regulation (GDPR). Official Journal of the European Union. 2016. L 119. pp. 1–88.

9. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD, 2013. 32 p.

References:

1. Bachilo, I. L. (2021). Pravo i informatsionnye tekhnologii: problemy sootnosheniya. *Zhurnal rossiiskogo prava,* (6), 45-53. (in Russian).

2. Gavrilov, E. P. (2023). Pravovoe regulirovanie personal'nykh dannykh: kommentarii k Federal'nomu zakonu №152-FZ. Moscow. (in Russian).

3. Goncharenko, L. A. (2022). Personal'nye dannye: problemy zashchity i otvetstvennost' za ikh narushenie. St. Petersburg. (in Russian).

4. Mikhailova, O. S. (2024). Rezhimnye ob"ekty kak element sistemy natsional'noi bezopasnosti. *Gosudarstvennaya vlast' i mestnoe samoupravlenie,* (5), 77-83. (in Russian).

5. Savel'ev, A. I. (2023). Personal'nye dannye i kiberbezopasnost'. Moscow. (in Russian).

6. Tikhomirov, Yu. A. (2020). Informatsionnoe pravo Rossii. Moscow. (in Russian).

7. Chernysheva, E. N. (2021). Gosudarstvennaya taina i rezhim ogranichennogo dostupa. Moscow. (in Russian).

8. General Data Protection Regulation (GDPR) (2016). *Official Journal of the European Union,* 119, 1–88.

9. OECD (2013). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECDp.

Поступила в редакцию
11.12.2025 г.

Принята к публикации
23.12.2025 г.

Ссылка для цитирования:

Доровских К. Ю. Особенности защиты персональных данных на режимных объектах РФ // Бюллетень науки и практики. 2026. Т. 12. №2. С. 543-547. https://doi.org/10.33619/2414-2948/123/60

Cite as (APA):

Dorovskikh, K. (2026). Personal Data Protection in Restricted Access Facilities in the Russian Federation. *Bulletin of Science and Practice, 12*(2), 543-547. (in Russian). https://doi.org/10.33619/2414-2948/123/60