Научная статья
УДК 343.3/.7
DOI: 10.47475/2311-696X-2026-50-3-47-51

С. 47–51

ЗНАЧЕНИЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Надежда Дмитриевна Муратова

Казанский инновационный университет имени В. Г. Тимирясова,
г. Казань, Россия
ndmuratova@mail.ru

Аннотация. Статья посвящена исследованию теоретико-правовых оснований, позволяющих рассматривать безопасность биометрических персональных данных в качестве самостоятельного элемента системы национальной безопасности Российской Федерации. Раскрывается содержание понятия биометрических персональных данных, их правовая природа и структурная неоднородность, обусловленная делением на статические и динамические идентификаторы личности. Особое внимание уделяется выявлению угроз, связанных с оборотом биометрических данных таких как централизации биометрических профилей граждан в рамках государственных информационных систем, использованию технологий искусственного интеллекта для синтеза поддельных биометрических артефактов, а также фрагментарности правового регулирования.

На основе изученных доктринальных источников автор обосновывает вывод о двойственной роли биометрии — как инструмента обеспечения безопасности и как самостоятельного объекта угроз, — а также формулирует предложения по совершенствованию законодательства, включая введение категории «критическая биометрическая инфраструктура» и требования об обязательном детектировании синтезированной биометрии.

Делается вывод о необходимости формирования комплексного межотраслевого механизма защиты биометрических данных, объединяющего технические, административные и уголовно-правовые меры.

Ключевые слова: биометрические персональные данные; национальная безопасность; информационная безопасность; Единая биометрическая система; цифровой профиль; критическая информационная инфраструктура; искусственный интеллект; синтезированная биометрия; дипфейк; защита персональных данных

Для цитирования: Муратова Н. Д. Значение обеспечения безопасности биометрических персональных данных для национальной безопасности Российской Федерации // Правопорядок: история, теория, практика. 2026. № 3 (50). С. 47–51. DOI: 10.47475/2311-696X-2026-50-3-47-51

Research article

THE IMPORTANCE OF ENSURING THE SECURITY OF BIOMETRIC PERSONAL DATA FOR THE NATIONAL SECURITY OF THE RUSSIAN FEDERATION

Nadezhda D. Muratova

Kazan Innovative University named after V. G. Timiryasov, Kazan, Russia
ndmuratova@mail.ru

Abstract. The article is devoted to the study of the theoretical and legal foundations that allow us to consider the security of biometric personal data as an independent element of the national security system of the Russian Federation. The content of the concept of biometric personal data, its legal nature and structural heterogeneity, обусловленная the division into static and dynamic identifiers of a person, are revealed. Special attention is paid to identifying threats associated with the circulation of biometric data: the centralization of citizens' biometric profiles within state information systems, the use of artificial intelligence technologies to synthesize fake biometric artifacts, as well as the fragmentation of legal regulation.

© Муратова Н. Д.

Based on the studied doctrinal sources, the author substantiates the conclusion about the dual role of biometrics — as a tool for ensuring security and as an independent target of threats — and formulates proposals for improving legislation, including the introduction of the category "critical biometric infrastructure" and requirements for mandatory detection of synthesized biometrics.

The conclusion is drawn that it is necessary to form a comprehensive intersectoral mechanism for protecting biometric data, combining technical, administrative, and criminallegal measures.

Keywords. biometric personal data; national security; information security; Unified Biometric System; digital profile; critical information infrastructure; artificial intelligence; synthesized biometrics; deepfake; protection of personal data

For citation: Muratova ND. The Importance of Ensuring the Security of Biometric Personal Data for the National Security of the Russian Federation. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2026;(3):47-51. (In Russ.). DOI: 10.47475/2311-696X-2026-50-3-47-51

Введение

Стремительное развитие цифровых технологий идентификации личности закономерно ставит перед юридической наукой вопрос о том, каким образом категория биометрических персональных данных соотносится с системой национальной безопасности государства. Прежде чем перейти к рассмотрению данного вопроса, необходимо подчеркнуть, что биометрические данные — изображение лица, отпечатки пальцев, голос, рисунок сетчатки глаза — представляют собой не просто разновидность персональных данных, но уникальный, неизменяемый и практически невосполнимый идентификатор личности, утрата контроля над которым порождает риски, выходящие далеко за пределы частноправовой сферы. Актуальность обращения к данной проблематике определяется тем, что в Российской Федерации создана и функционирует Единая биометрическая система, объединяющая биометрические профили граждан для целей удаленной идентификации в банковской, государственной и коммерческой сферах [6, с. 134–149]. Следует отметить, что подобная централизация данных, обладающая очевидными технологическими преимуществами, одновременно формирует новый объект посягательства — крупный массив уникальных идентификаторов личности, компрометация которого способна повлечь последствия, сопоставимые с угрозами информационной, экономической и даже оборонной безопасности страны.

Целью настоящей статьи является выявление теоретико-правовых оснований, позволяющих отнести безопасность биометрических персональных данных к числу самостоятельных элементов национальной безопасности Российской Федерации, а также формулирование предложений по совершенствованию правового механизма их защиты.

Для достижения указанной цели необходимо решить следующие задачи:

— раскрыть содержание понятия биометрических персональных данных и их правовой природы;

— охарактеризовать основные угрозы, связанные с оборотом такого рода данных;

— проанализировать соотношение доктрины национальной безопасности и института защиты биометрических данных;

— предложить выводы относительно направлений развития законодательства в исследуемой области.

Материал и методы

Основу исследования составили общенаучные и частнонаучные методы научного познания, используемые для исследования теоретической основы и формирования собственных умозаключений.

В представленной публикации использованы и проанализированы источники норм информационного законодательства, регулирующим сбор, обработку и защиту биометрических данных в России, а также специальная литература по тематике исследования.

Описание исследования

Понятие биометрических персональных данных и их правовая природа

Обратимся к содержанию понятия биометрических персональных данных, ориентируясь на законодательство и доктрину. Согласно действующему законодательству[1] и устоявшемуся в литературе подходу, биометрические персональные данные представляют собой сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для этой цели [7, с. 171–178; 14, с. 129]. Как отмечают В. Е. Степенко и А. Д. Богдановская, к числу таких данных традиционно относят изображение лица, отпечатки пальцев, папиллярный узор, особенности голоса и походки, а также рисунок кровеносных сосудов — то есть признаки, обладающие свойствами уникальности, устойчивости во времени и практической неизменяемости [11, с. 16]. Указанные свойства отличают биометрические данные от иных категорий персональных данных, например, пароль или номер документа можно заменить в случае компрометации, то отпечаток пальца или геометрию лица заменить

[1] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 26.07.2026) «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 31 (ч. I). Ст. 3451.

© Муратова Н. Д.

невозможно, что и обусловливает повышенную степень их правовой охраны.

Важно обратить внимание на то, что в специальной литературе выделяется структурная неоднородность биометрических данных. И. О. Копенкин, ссылаясь на действующие государственные стандарты, указывает, что к биометрическим персональным данным относятся изображение отпечатка пальца, изображение лица, данные геометрии контура кисти, а также динамические характеристики — голос, подпись, походка [9, с. 60]. Данная классификация позволяет условно разделить биометрические идентификаторы на статические (морфологические) и динамические (поведенческие), что имеет существенное значение для оценки степени риска при их незаконном обороте, похищение статического идентификатора создает угрозу пожизненной компрометации личности, поскольку восстановление утраченного признака в биологическом смысле невозможно.

Прежде чем перейти к выявлению угроз, связанных с оборотом биометрических данных, целесообразно обозначить их правовую природу. С. М. Коновалов справедливо указывает, что специфика правового режима биометрических данных заключается в двойственности их природы, с одной стороны, они являются информацией и подчиняются общему режиму охраны персональных данных, а с другой — неразрывно связаны с телесной, биологической сущностью личности, что приближает их к объектам, охраняемым в рамках права на неприкосновенность частной жизни и физическую целостность [8, с. 899]. Данное обстоятельство, на наш взгляд, служит основанием для вывода *о необходимости выделения биометрических данных в особую категорию объектов правовой охраны с повышенным уровнем защиты, отличным от общего режима персональных данных.*

Биометрические персональные данные как объект угроз национальной безопасности

Рассмотрим подробнее, каким образом оборот биометрических данных сопрягается с угрозами национальной безопасности. Согласно позиции А. С. Артемьевой, биометрические персональные данные образуют самостоятельный элемент системы обеспечения криминологической безопасности личности, общества и государства, поскольку неконтролируемое распространение такого рода сведений создает условия для совершения широкого спектра преступлений — от хищения денежных средств с использованием подделанных биометрических идентификаторов до создания синтетических цифровых личностей [3, с. 48–50]. Следует подчеркнуть, что данный вывод коррелирует с общемировой тенденцией, как отмечается в исследовании, посвященном сравнительно-правовому анализу технологий распознавания лиц, масштабное внедрение биометрической идентификации в государственное управление и коммерческий оборот объективно расширяет поверхность атаки для противоправных действий и требует выработки специализированных правовых механизмов защиты, учитывающих трансграничный характер соответствующих угроз [1, p. 826–838].

Особое значение в данном контексте приобретает угроза использования технологий искусственного интеллекта для создания поддельных биометрических артефактов. М. А. Желудков и А. Н. Варыгин обращают внимание на то, что современные программы искусственного интеллекта способны воссоздать голос и изображение человека на основании единичного попадания его образа в объектив камеры или микрофон, что открывает возможности для совершения корыстных преступлений с использованием синтезированной биометрии — так называемых дипфейков [7, с. 173]. Как справедливо указывается в исследовании Н. А. Стефановой и О. О. Андиряковой, стремительное внедрение биометрических технологий сопровождается объективным отставанием механизмов оценки рисков от темпов технологического развития, что порождает разрыв между декларируемой экономической эффективностью биометрической идентификации и фактическим уровнем защищенности персональных данных граждан [12, с. 39–40].

Необходимо остановиться также на угрозах, связанных с централизацией биометрических данных в рамках государственных информационных систем. О. И. Долганова, Е. В. Васильева и Д. А. Рябов отмечают то, что Единая биометрическая система, выступая инструментом доступа к цифровому профилю гражданина, объективно формирует единую точку сосредоточения критически значимой информации, компрометация которой способна затронуть неограниченный круг субъектов одновременно [5, с. 1535–1537]. В свою очередь А. Н. Мочалов, изучая риски цифровизации идентификационных процедур для конституционных прав человека, указывает, что правовая неопределенность режима обработки цифрового профиля создает почву для нарушения права на неприкосновенность частной жизни, права на защиту персональных данных, а в отдельных случаях — и права на равенство перед законом при автоматизированном принятии решений [10, с. 94].

Приведенные данные позволяют заключить, что угрозы, связанные с оборотом биометрических данных, носят системный характер и затрагивают не только частные интересы отдельных граждан, но и публичные интересы государства в сфере обеспечения устойчивости информационной инфраструктуры.

Соотношение защиты биометрических данных с доктриной национальной безопасности

Для более глубокого понимания рассматриваемой проблемы обратимся к вопросу о теоретическом обосновании включения защиты биометрических данных в структуру национальной безопасности. Г. Н. Чурилин и Е. А. Максимова отмечают, что биометрические системы идентификации являются одновременно инструментом обеспечения информационной безопасности и потенциальным источником угроз для нее, поскольку

© Муратова Н. Д.

компрометация биометрической базы данных способна парализовать функционирование целых сегментов критической информационной инфраструктуры, включая банковский сектор, системы государственного управления и объекты транспортной безопасности [13, с. 32–34]. Данное наблюдение представляется весьма значимым поскольку оно демонстрирует двойственную роль биометрии — как средства защиты и как объекта защиты одновременно, что требует дифференцированного подхода при формировании правового регулирования.

С этой точки зрения следует согласиться с позицией авторов, полагающих то, что действующее правовое регулирование защиты биометрических персональных данных в Российской Федерации характеризуется фрагментарностью и недостаточной согласованностью норм гражданского, административного и информационного законодательства, что снижает эффективность реагирования на масштабные утечки данных [4, с. 277–279]. Данный вывод подтверждается и результатами зарубежных исследований. Как показано в работе, посвященной уголовно-правовым проблемам противодействия преступности в цифровой среде, эффективное обеспечение безопасности цифровых идентификаторов личности требует не только совершенствования технических средств защиты, но и формирования согласованной системы уголовно-правовых, административных и превентивных мер, объединенных единой концепцией цифровой безопасности личности [2, p. 195–196].

Таким образом, изложенное позволяет сделать вывод о том, что безопасность биометрических персональных данных обоснованно может рассматриваться в качестве самостоятельного элемента национальной безопасности Российской Федерации по следующим основаниям.

Во-первых, компрометация биометрических данных затрагивает не отдельного гражданина, а потенциально неограниченный круг субъектов, что придает соответствующим угрозам массовый, системный характер, сопоставимый с угрозами критической информационной инфраструктуре.

Во-вторых, невозможность замены скомпрометированного биометрического идентификатора делает последствия соответствующих правонарушений необратимыми, что принципиально отличает данную категорию угроз от большинства иных информационных рисков.

В-третьих, централизация биометрических данных в государственных информационных системах формирует единую точку критической зависимости, разрушение которой способно повлечь дестабилизацию системы государственного управления и финансового сектора.

Наконец, развитие технологий синтеза биометрических артефактов размывает границу между подлинной и поддельной идентификацией личности, что создает угрозу самому институту идентификации как основе правового регулирования общественных отношений.

Заключение и выводы

Резюмируя изложенное, необходимо подчеркнуть, что вопрос обеспечения безопасности биометрических персональных данных вышел за пределы частноправовой проблематики защиты информации и приобрел характер задачи, имеющей самостоятельное значение для системы национальной безопасности Российской Федерации.

По результатам проведенного исследования представляется возможным сформулировать следующие выводы.

Во-первых, биометрические персональные данные обладают уникальным правовым статусом, обусловленным неразрывной связью информационной и телесной составляющих личности, что требует закрепления в законодательстве специального режима охраны, в том числе с помощью уголовно-правовых средств, отличного от общего режима персональных данных, включая установление отдельных, более строгих составов ответственности за незаконный оборот биометрических сведений.

Во-вторых, представляется целесообразным законодательно закрепить категорию «критическая биометрическая инфраструктура» применительно к государственным информационным системам, аккумулирующим биометрические данные граждан в значительном объеме, распространив на них требования, аналогичные требованиям к объектам критической информационной инфраструктуры, с установлением обязательного государственного контроля за уровнем их защищенности.

В-третьих, ввиду стремительного развития технологий синтеза биометрических артефактов автор полагает необходимым дополнить систему мер безопасности требованием об обязательном внедрении технологий детектирования синтезированной биометрии на уровне операторов государственных и кредитно-финансовых информационных систем, поскольку существующие меры защиты ориентированы преимущественно на предотвращение утечек, но не на выявление подделки данных.

В-четвертых, эффективная защита биометрических данных не может быть обеспечена исключительно средствами информационного, гражданского или уголовного законодательства и требует формирования комплексного, межотраслевого механизма, объединяющего технические, административные и уголовно-правовые меры в единую систему обеспечения цифровой безопасности личности как составной части национальной безопасности государства в целом.

© Муратова Н. Д.

Список источников

1. Utegen D., Rakhmetov B. Zh. Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models. Journal of Digital Technologies and Law. 2023;1(3):825-844. DOI: 10.21202/jdtl.2023.36.

2. Efremova M. A., Russkevich E. A. Criminal-Legal Issues of Countering Crime in the Metaverse: Current State and Prospects of Development. Journal of Digital Technologies and Law. 2025. 3(2):187–202. DOI: 10.21202/jdtl.2025.8. EDN: ypsxqo

3. Артемьева А. С. Биометрические персональные данные как элемент системы обеспечения криминологической безопасности, требующий уголовно-правовой защиты // Проблемы правоохранительной деятельности, 2024. № 4. С. 42–51.

4. Бурлака С. Н., Бельдина О. Г. Защита биометрических персональных данных: проблемы правового регулирования // Право и государство: теория и практика. 2023. № . 10 (226). С. 277–279. DOI: 10.47643/1815-1337_2023_10_277

5. Долганова О. И., Васильева Е. В., Рябов Д. А. Цифровой профиль гражданина: необходимый и достаточный набор персональных данных // Вопросы инновационной экономики. 2022. Т. 12, № 3. С. 1523–1540. DOI: 10.24412/2070-1381-2022-93-134-149

6. Долганова О. И., Чистякова Д. А. Варианты использования Единой биометрической системы как инструмента доступа к цифровому профилю гражданина // Государственное управление. Электронный вестник. 2022. № 93. С. 134–149. DOI: 10.24412/2070-1381-2022-93-134-149

7. Желудков М.А, Варыгин А. Н. Безопасное использование биометрических персональных данных личности как средство борьбы с корыстной цифровой преступностью // Вестник Саратовской государственной юридической академии. 2024, № 4 (159). С. 170–178. DOI: 10.24412/2227-7315-2024-4-170-178

8. Коновалов С. М. Обеспечение безопасности биометрических персональных данных на законодательном уровне: общие принципы и российская практика // Вестник науки. 2023. Т. 1, № 6 (63). С. 895–901.

9. Копенкин И. О. Биометрические персональные данные несовершеннолетних нуждаются в уголовно-правовой охране // Образование и право. 2024. № 9. С. 59–65. DOI: 10.24412/2076-1503-2024-9-59-65

10. Мочалов А. Н. Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности // Lex Russica. 2021. № 9 (178). С. 88–101. DOI: 10.17803/1729-5920.2021.178.9.088-101

11. Степенко В. Е., Богдановская А. Д. Биометрические персональные данные // Евразийский Союз Ученых. 2020. № 4–10 (73). С. 15–19.

12. Стефанова Н. А., Андирякова О. О. Риски и экономическая эффективность от использования технологии биометрии // Журнал прикладных исследований. 2024. № 3. С. 36–41. DOI: 10.47576/2949-1878.2024.3.3.00

13. Чурилин Г. Н., Максимова Е. А. Биометрия в информационной безопасности // NBI-technologies. 2019. Т. 13, № 4. С. 30–36. DOI: 10.15688/NBIT.jvolsu.2019.4.4

14. Шутова А. А., Бегишев И. Р., Волкова А. В. Уголовно-правовая охрана персональных данных в условиях экономики данных // Правоприменение. 2026. Т. 10, № 2. С. 127–136. DOI: 10.52468/2542-1514.2026.10(2).127-136.

СВЕДЕНИЯ ОБ АВТОРЕ

Муратова Надежда Дмитриевна

Кандидат юридических наук, заслуженный юрист Республики Татарстан, старший научный сотрудник Научно-исследовательского института цифровых технологий и права, Казанский инновационный университет имени В. Г. Тимирясова (г. Казань, Россия).
E-mail: ndmuratova@mail.ru

INFORMATION ABOUT THE AUTHOR

Nadezhda D. Muratova

Candidate of Legal Sciences, Honored Lawyer of the Republic of Tatarstan, Senior Researcher at the Scientific Research Institute of Digital Technologies and Law, Kazan Innovative University named after V. G. Timiryasov (Kazan, Russia).
E-mail: ndmuratova@mail.ru

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 13.08.2026.
Дата рецензирования статьи / Revised: 16.08.2026.
Дата принятия статьи к публикации / Accepted: 20.08.2026.

© Муратова Н. Д.