

Федеральное государственное казенное образовательное учреждение  
высшего образования «Белгородский юридический институт  
Министерства внутренних дел Российской Федерации  
имени И.Д. Путилина»

*На правах рукописи*

**Карпушина Анна Викторовна**

**АДМИНИСТРАТИВНО-ПРАВОВАЯ ЗАЩИТА  
БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Специальность 5.1.2. Публично-правовые (государственно-правовые) науки

**ДИССЕРТАЦИЯ**  
на соискание ученой степени  
кандидата юридических наук

Научный руководитель:  
доктор юридических наук, профессор  
**Дизер Олег Александрович**

Белгород – 2026

## ОГЛАВЛЕНИЕ

|                                                                                                                                                             |            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>Введение .....</b>                                                                                                                                       | <b>3</b>   |
| <b>Глава 1. Административно-правовые основы защиты биометрических персональных данных.....</b>                                                              | <b>19</b>  |
| § 1. Биометрические персональные данные как объект правовой защиты .....                                                                                    | 19         |
| § 2. Административно-правовое регулирование защиты биометрических персональных данных .....                                                                 | 55         |
| § 3. Особенности административной ответственности за правонарушения, связанные с обработкой биометрических персональных данных .....                        | 78         |
| <b>Глава 2. Организационно-правовые основы защиты биометрических персональных данных.....</b>                                                               | <b>107</b> |
| § 1. Система органов публичной власти, осуществляющих защиту биометрических персональных данных.....                                                        | 107        |
| § 2. Меры административно-правовой защиты биометрических персональных данных .....                                                                          | 140        |
| § 3. Совершенствование деятельности органов внутренних дел Российской Федерации по административно-правовой защите биометрических персональных данных ..... | 169        |
| <b>Заключение .....</b>                                                                                                                                     | <b>194</b> |
| <b>Список литературы .....</b>                                                                                                                              | <b>202</b> |
| <b>Приложение 1 .....</b>                                                                                                                                   | <b>242</b> |
| <b>Приложение 2 .....</b>                                                                                                                                   | <b>246</b> |
| <b>Приложение 3 .....</b>                                                                                                                                   | <b>247</b> |
| <b>Приложение 4 .....</b>                                                                                                                                   | <b>248</b> |
| <b>Приложение 5 .....</b>                                                                                                                                   | <b>249</b> |

## ВВЕДЕНИЕ

**Актуальность темы исследования.** Использование искусственного интеллекта, автоматизированных систем идентификации личности, разработка цифрового профиля человека повлияли на популяризацию использования биометрических персональных данных физического лица. Автоматизированная идентификация по биометрическим характеристикам гарантирует высокую эффективность, обеспечивая скорость обработки и точность результатов при сопоставлении идентификаторов. Это позволяет в кратчайшие сроки установить личность человека и реализовать цели идентификации и (или) аутентификации.

Президент Российской Федерации В.В. Путин на конференции по искусственному интеллекту и анализу данных Artificial Intelligence Journey 2021 подчеркнул, что биометрические персональные данные как информация, имеющая критическое значение для безопасности граждан и являющаяся предельно личной, должна храниться в единой государственной системе биометрической идентификации и государство должно взять на себя ответственность за ее хранение<sup>1</sup>.

Особенность биометрических персональных данных как правовой категории заключается в их особом статусе среди персональных данных ввиду природы их происхождения и целей использования. В отличие от классических персональных данных (паспортные данные, ИНН, СНИЛС и т.д.) биометрические характеристики являются неизменными. В случае, если биометрические персональные данные перестают быть конфиденциальными, то использование таких данных для идентификации становится невозможным.

Общественные отношения, связанные с оборотом биометрических персональных данных, активно развиваются, и это требует от государства принятия релевантных мер административно-правовой защиты. Именно

---

<sup>1</sup> Информация с официального сайта Президента России [Электронный ресурс]. – URL: <http://www.kremlin.ru/events/president/transcripts/speeches/67099> (дата обращения: 17.11.2022).

государство выступает гарантом безопасности использования биометрических характеристик физического лица.

В 2024 году в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации (далее – Роскомнадзор) поступило 68 748 обращений с жалобами на неправомерное использование их персональных данных, что на 7,4% больше, чем в 2023 году<sup>1</sup>. Аналогично прирост отмечается в сведениях, отражающих количество рассмотренных дел об административных правонарушениях в области сбора, хранения, использования или распространения персональных данных. Так, в 2024 году рассмотрено 1086 дел, в 2023 – 916, в 2022 – 617<sup>2</sup>. В Российской Федерации отсутствуют данные официальной статистики, касающейся административных правонарушений в области обработки биометрических персональных данных. Эти сведения отражаются в общей совокупности статистической информации о количестве административных правонарушений в сфере защиты персональных данных.

Данное обстоятельство обуславливает специфику правового регулирования в области защиты биометрических характеристик граждан. Особенностью является тот факт, что фундаментальной основой для правового регулирования биометрических персональных данных выступает законодательство, регламентирующее обработку персональных данных. Однако, принятие новых нормативных правовых актов свидетельствует о формировании тенденции к разработке отдельных норм специального законодательства в области защиты биометрических персональных данных.

В условиях активной интеграции технологических инноваций в общественные отношения требуется формирование необходимого уровня доверия к вопросам правовой защиты в области информационной безопасности.

---

<sup>1</sup> Итоги работы с обращениями граждан в Роскомнадзоре в 2024 году / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://rkn.gov.ru/treatments/p436/> (дата обращения: 25.05.2025).

<sup>2</sup> Административные правонарушения в области связи и информации / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://stat.api-пресс.пф/stats/adm/t/31/s/73> (дата обращения: 13.04.2025).

В связи с чем очевидна необходимость совершенствования правового регулирования по сбору, обработке и хранению биометрических персональных данных и их обособление в отдельную правовую категорию, что позволит обеспечить более высокий уровень государственной защиты в исследуемой области.

С развитием компьютерных технологий появились новые способы совершения правонарушений в отношении биометрических персональных данных – дипфейк (deepfake) и спуфинг (spoofing). За три месяца 2025 года в России был выявлен 61 уникальный дипфейк и 2,3 тыс. копий, что в 2,6 раза превышает весь объем дипфейков, зафиксированный в 2023 году<sup>1</sup>. При этом проблема правового регулирования в отношении данного явления остается нерешенной. Законодательно понятие дипфейка не закреплено и, соответственно, не предусмотрено мер ответственности за подмену биометрических персональных данных с помощью искусственного интеллекта. В связи с чем требуется разработка эффективной системы привлечения к административной ответственности за правонарушения в области сбора, обработки и хранения биометрических персональных данных. Правовое регулирование в данной области должно быть прогрессивным и работать на упреждение возникающих рисков.

Сложность совершенствования законодательства в области биометрических персональных данных заключается в том, что перед государством стоят задачи по правовому регулированию технических условий сбора, обработки и хранения биометрических персональных данных, а также по осуществлению контроля за соблюдением установленных норм с учетом этических правил при работе с биометрией. Это обуславливает необходимость использования междисциплинарного подхода при изучении рассматриваемого феномена. Биометрические персональные данные представляют собой предмет информационного права, однако важная роль в данном случае отводится

---

<sup>1</sup> Дипфейк шагает по планете. С чем связан рост числа сообщений, сгенерированных ИИ / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://rg.ru/2025/04/08/dipfejk-shagaet-po-planete.html> (дата обращения: 03.05.2025).

административному праву, социологии, философии и техническим наукам. При этом требуется консолидация усилий как от государства, так и в целом общества.

На сегодняшний день доказана необходимость научного исследования биометрических персональных данных как юридической категории, правовой анализ административных правонарушений в области защиты биометрических характеристик, структуризация органов публичной власти, реализующих законодательство в данной сфере, а также рассмотрение роли МВД России в реализации мер, направленных на безопасность данных о физиологических и поведенческих характеристиках физических лиц.

Вышесказанное актуализирует обозначенную тему и обуславливает необходимость проведения комплексного научного исследования административно-правовой защиты биометрических персональных данных.

**Степень научной разработанности темы исследования.** Проблемы административно-правовой защиты биометрических персональных данных актуальны, так как их изучение затрагивает разнообразные области знаний. В процессе подготовки диссертации использовались научные труды ученых в области, как информационных технологий, социологии, философии, экономики и права. Изучались вопросы, связанные с понятием биометрических персональных данных, их юридической природы, были проанализированы конституционные принципы, заложенные в основу института административной ответственности, исследовались меры административно-правовой защиты биометрии.

Диссертационные работы, затрагивающие вопросы биометрических персональных данных, исследовались в различных междисциплинарных отраслях такими авторами, как М.В. Бундин<sup>1</sup>, С.А. Быстрыкова<sup>2</sup>, С.С. Волкова<sup>3</sup>,

---

<sup>1</sup> Бундин М.В. Персональные данные в системе информации ограниченного доступа: дис. ... канд. юрид. наук: 12.00.13. М., 2017.

<sup>2</sup> Быстрыкова С.А. Правовое регулирование цифрового оборота персональных данных в системе обеспечения транспортной безопасности: дис. ... канд. юрид. наук: 5.1.2. М., 2024.

<sup>3</sup> Волкова С.С. Методы повышения эффективности систем биометрической аутентификации пользователей информационных систем по изображению лица: дис. ... канд. техн. наук: 05.13.19. СПб., 2017.

С.И. Гутник<sup>1</sup>, В.В. Игумнов<sup>2</sup>, А.В. Кучеренко<sup>3</sup>, В.Б. Наумов<sup>4</sup>, М.И. Проскурякова<sup>5</sup>, С.В. Соловкин<sup>6</sup>. В представленных исследованиях осуществлялся анализ персональных данных в целом, без выделения специфических характеристик и особенностей административно-правовой защиты биометрических персональных данных. Настоящее исследование призвано в определенной мере восполнить указанные пробелы.

**Целью диссертационного исследования** является разработка и обоснование концептуальных теоретических основ административно-правовой защиты биометрических персональных данных как юридической категории, а также выработка предложений по совершенствованию административно-правового регулирования в данной сфере.

Для достижения указанной цели предполагается решение следующих **задач**:

– раскрыть сущность биометрических персональных данных как правовой категории, совершенствовать понятие, выделить признаки, определить их классификацию;

– исследовать становление отечественного законодательства в области защиты биометрических персональных данных и разработать пути оптимизации административного и информационного правового регулирования в современных условиях;

– выявить проблемы и определить приоритетные направления развития института административной ответственности в области защиты биометрических

---

<sup>1</sup> Гутник С.И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных: дис. ... канд. юрид. наук: 12.00.08. Владивосток, 2017.

<sup>2</sup> Игумнов В.В. Публично-правовое регулирование цифрового профилирования в Российской Федерации: автореф. дис. ... кан. юрид. наук: 5.1.2. М., 2024.

<sup>3</sup> Кучеренко А.В. Правовое регулирование персональных данных в Российской Федерации: дис. ... канд. юрид. наук: 12.00.14. Челябинск, 2010.

<sup>4</sup> Наумов В.Б. Институт идентификации в информационном праве: дис. ... док. юрид. наук: 12.00.13 М., 2020.

<sup>5</sup> Проскурякова М.И. Защита персональных данных в праве России и Германии: конституционно-правовой аспект: дис. ... кан. юрид. наук: 12.00.02. СПб., 2017.

<sup>6</sup> Соловкин С.В. Публично-правовое регулирование процессов автоматизированного сбора данных о человеке в условиях цифровой трансформации: дис. ... кан. юрид. наук: 5.1.2. М., 2024.

персональных данных, раскрыть особенности составов административных правонарушений в исследуемой области;

– охарактеризовать участников системы органов публичной власти, осуществляющих защиту биометрических персональных данных;

– определить меры административно-правовой защиты биометрических персональных данных, классифицировать их;

– изучить деятельность органов внутренних дел Российской Федерации по совершенствованию административно-правовой защиты биометрических персональных данных;

– сформулировать и обосновать рекомендации и предложения приоритетных направлений совершенствования деятельности полиции в исследуемой области.

**Объектом диссертационного исследования** является совокупность общественных отношений, складывающихся в области административно-правовой защиты биометрических персональных данных.

**Предметом диссертационного исследования** выступают нормы российского законодательства, регулирующие общественные отношения в сфере административно-правовой защиты биометрических персональных данных, положения теории, правоприменительная практика и теоретические исследования по данному вопросу.

**Методологической основой исследования** выступили общенаучные методы: логический (при последовательном изложении темы исследования и формулировании выводов), исторический (при рассмотрении этапов становления биометрических персональных данных), системно-структурный (при анализе мер по защите биометрических персональных данных, изучении основ правового регулирования деятельности). Использовался диалектический метод познания правовых явлений, с помощью которого удалось раскрыть вопросы защиты биометрических персональных данных в развитии и во взаимообусловленности с другими явлениями экономической, политической и этической сторон общественной жизни, а также методы конкретно-социологических исследований

(при отборе, обработке и анализе информации о сборе, обработке и хранении биометрических персональных данных, судебной практики, анкетировании, интервьюировании), в том числе статистический метод (при обобщении информации, содержащейся в публикациях и обзорах в области правового регулирования биометрических персональных данных).

Также применялись частно-научные методы: сравнительно-правовой (при анализе административно-правового статуса биометрических персональных данных) и формально-юридический (при анализе правовых актов, формулировании авторских определений и рекомендаций).

**Теоретическую основу исследований** составили труды следующих авторов: В.В. Архипова, С.В. Баженова, Ю.А. Брюхомицкого, М.В. Бундина, Е.Г. Барковской, А.Н. Варыгина, Р.Н. Данеляна, В.Е. Дивольда, М.Б. Добробабы, М.А. Желудкова, В.Х. Каримова, Н.Н. Ковалевой, Э.И. Лескиной, А.В. Минбалеева, А.А. Морозова, В.Б. Наумова, Н.И. Платоновой, Т.А. Поляковой, И.М. Рассолова, Е.В. Старанцовой, Э.В. Талапиной, Л.К. Терещенко, Н.А. Троян, С.Е. Чаннова, А.А. Чеботаревой, С.Г. Чубуковой, С.В. Яценко.

Общие проблемы административной ответственности рассматривали такие ученые, как Ю.Е. Аврутин, О.А. Дизер, А.С. Дугенец, А.А. Затолокин, С.В. Запольский, С.М. Зубарев, А.И. Каплунов, В.И. Ковшевацкий, О.А. Кожевников, П.И. Кононов, С.Ф. Мазурин, Н.В. Макарейко, Ю.И. Мигачев, К.Г. Прокофьев, А.Н. Прокопенко, Л.Л. Попов, Б.В. Россинский, В.П. Сальникова, Ю.Н. Старилов, С.А. Старостин, А.И. Стахов, М.С. Студеникина, Г.Н. Сулова, И.В. Тимошенко, Ю.А. Тихомиров, И.Д. Фиалковская и др.

Теоретические и прикладные аспекты правовой защиты биометрических персональных данных являлись предметом исследования в юридических науках, включая конституционное право (С.С. Зенин, О.А. Ижаев, Д.Л. Кутейников, В.А. Лебедев, А.Н. Мочалов), уголовное право (С.И. Гутник, А.А. Койсин, Т.В. Попова, А.Б. Сергеев), криминалистику (Р.С. Белкина, Е.Р. Россинской, Л.Г. Эджубова, З.И. Кирсанова, В.Я. Колдина, И.С. Полевого, В.А. Снеткова,

А.И. Хвыли-Олинтера и др.), а также в технических науках (А.А. Островский, Д.Н. Жариков, В.С. Лукьянов, Д.С. Попов, Ю.Н. Семенов, В.И. Кабаров, А.Р.М. Кассу, А.М. Трошков, М.А. Трошков, Д.В. Шлаев).

**Нормативную правовую основу** диссертации составили международные акты, Конституция Российской Федерации, федеральные законы, нормативные правовые акты субъектов Российской Федерации, подзаконные нормативные правовые акты, закрепляющие различные аспекты административно-правовой защиты биометрических персональных данных, а также нормы, регламентирующие вопросы их применения в рассматриваемой сфере.

**Эмпирическая основа исследования.** В рамках исследования изучены материалы 52 дел об административных правонарушениях, связанных с неправомерными действиями в отношении биометрических персональных данных, совершенных на территории Российской Федерации в 2020–2024 годах.

В качестве эмпирического материала в работе отражены отчеты о выполнении Плана и показателей деятельности Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций за 2020–2024 годы; мониторинг развития информационного общества в Российской Федерации, подготовленный Федеральной службой государственной статистики; иные материалы официальных отчетов, официальных сайтов федеральных и региональных органов государственной власти; результаты интервьюирования 375 граждан Российской Федерации и др.

**Научная новизна исследования** заключается в том, что автором проведено специализированное административно-правовое исследование теоретических основ административно-правовой защиты биометрических персональных данных, результаты которого восполняют ощутимый пробел в административно-правовой и административно-процессуальной науке.

Новизна предложенных автором суждений выражена в исследовании понятия и сущности биометрических персональных данных как юридической категории; сформулированы актуальные понятия «биометрических персональных данных», «мер административно-правовой защиты биометрических персональных

данных»; выделены признаки биометрических персональных данных; классифицированы меры административно-правовой защиты биометрических персональных данных; исследован институт административной ответственности за правонарушения в области защиты биометрических персональных данных.

В диссертации с учетом правовых и законодательных тенденций научно обоснованы положения, обладающие элементами новизны и связанные с особенностями биометрии, выделяющими ее из совокупности персональных данных. Автором предлагается обособление биометрических персональных данных, создание прозрачности и открытости при формировании статистических данных правоприменительной и судебной практик.

Диссертантом проанализирована роль органов внутренних дел в реализации мер по защите биометрических персональных данных, обоснована необходимость наделения полиции полномочиями по возбуждению и рассмотрению административных правонарушений, связанных с биометрией.

В результате анализа особенностей правового регулирования биометрических персональных данных автором сформулированы предложения, направленные на дальнейшее совершенствование административно-правового регулирования, подготовлены проекты Федерального закона Российской Федерации «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях», Федерального закона Российской Федерации «О внесении изменений в Федеральный закон «О персональных данных», Федерального закона Российской Федерации «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации».

Новизна диссертационного исследования находит свое выражение в следующих **положениях, выносимых на защиту:**

1. Обоснована необходимость совершенствования используемого в законодательстве понятия биометрических персональных данных в части

унификации качественных характеристик. Основанием для этого служит исключение из определения употребления равнозначных терминов (от общего к частному) и включение в определение используемых в правоприменительной практике поведенческих характеристик. Исходя из этого, под биометрическими персональными данными следует понимать сведения, относящиеся к физиологическим и поведенческим характеристикам физического лица, полученные в целях идентификации и (или) аутентификации в результате специальной технической обработки, в том числе с использованием автоматизированных систем.

Данная дефиниция характеризует биометрические персональные данные как юридическую категорию и позволяет четко обособить биометрические данные от иных видов персональных данных.

2. Современная парадигма регулирования административно-правовой защиты биометрических персональных данных требует формирования специального правового режима, интегрирующего технические стандарты и правовые нормы. Важным условием создания эффективной системы законодательного регулирования является разработка правовой модели, которая будет иметь прогностический потенциал и своевременно реагировать на возникающие вызовы по защите биометрических персональных данных как самостоятельного объекта правовой защиты в сфере правового регулирования информации. В свою очередь, гарантом безопасности по регулированию мер административно-правовой защиты биометрических персональных данных выступает государство, роль которого заключается в защите прав субъектов данных.

3. Всю совокупность нормативных правовых актов, регулирующих правоотношения в области административно-правовой защиты биометрических персональных данных, можно разделить на две группы:

– нормативные правовые акты, регулирующие порядок сбора, обработки и хранения биометрических персональных данных для идентификации личности в целях осуществления гражданских общественных действий;

– нормативные правовые акты, регулирующие порядок сбора, обработки и хранения отдельных видов биометрических персональных данных органами публичной власти в целях обеспечения правопорядка и государственной безопасности.

Данная классификация отражает важную особенность правового регулирования административно-правовой защиты биометрических персональных данных в Российской Федерации, выраженную в разделении нормативных правовых актов в зависимости от целей биометрической идентификации и обуславливающую отсутствие единого нормативного правового акта, регулирующего всю совокупность биометрических характеристик.

4. Разработана классификация составов административных правонарушений, предусмотренных Кодексом Российской Федерации об административных правонарушениях (далее – КоАП РФ) в области защиты биометрических персональных данных. В соответствии с выявленными специфическими характеристиками составы административных правонарушений в исследуемой области можно разделить на четыре категории:

1) характеризующиеся единством состава административных правонарушений как в отношении биометрических персональных данных, так и классических персональных данных (статья 13.11 КоАП РФ);

2) связанные с нарушением законодательных норм в области обработки биометрии в единой биометрической системе (статья 13.11.3 КоАП РФ);

3) заключающиеся в неисполнении требований органа публичной власти, уполномоченного в области обеспечения безопасности биометрических персональных данных (статья 13.46 КоАП РФ);

4) иные правонарушения, посягающие на реализацию прав граждан по вопросам сбора, обработки и хранения биометрических персональных данных (часть 2.1 статьи 5.63 КоАП РФ).

Предложенная классификация может быть использована в качестве методологической основы для систематизации и структуризации существующих составов административных правонарушений в КоАП РФ, либо может являться

теоретической основой в случае если законодателем будет принято решение о целесообразности выделения данных норм в отдельную главу КоАП РФ.

5. Аргументированы выводы о необходимости введения в КоАП РФ нормы, предусматривающей меры ответственности за создание «дипфейков» и их использования для несанкционированного доступа к закрытой информации. Данные дефиниции имеют форму общепринятых научных терминов, не нашедших в настоящее время своего отражения в юридических словарях.

В связи с чем предложено законодательно закрепить следующие понятия:

1. Ложное воссоздание биометрических персональных данных с использованием искусственного интеллекта (дипфейк) – это воссоздание биометрических характеристик человека посредством использования искусственного интеллекта в целях совершения несанкционированного доступа при идентификации личности.

2. Идентификация по ложной биометрической характеристике (спуфинг) – использование дипфейка на основе биометрических характеристик в целях совершения неправомерной идентификации личности, ведущее к несанкционированному доступу.

На основании сформулированных предложений предложено внести изменения в КоАП РФ, дополнив статью 13.11.3 пунктом 5, предусматривающим административную ответственность за создание копии биометрических персональных данных, полученных с использованием искусственного интеллекта на основе биометрических характеристик, в целях совершения неправомерной идентификации личности, ведущее к несанкционированному доступу.

6. Условия аккредитации организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, не лишены дискредитирующего характера. Это проявляется в установлении требования к наличию размера собственных средств (капитала), который на сегодняшний день должен составлять не менее 500 миллионов рублей. Данная сумма не позволяет конкурировать организациям с меньшим капиталом на рынке предоставления услуг, связанных с биометрической идентификацией. Основываясь на мнениях

ученых, собственных результатах исследования, считаем целесообразным скорректировать требование к величине собственных средств по пути их уменьшения в целях повышения доступности использования систем биометрической идентификации, таким образом снизив уровень дискриминации юридических лиц по данному признаку.

7. Предложено в качестве одной из мер по совершенствованию административно-правовой защиты биометрических персональных данных правое информирование граждан посредством портала государственных услуг Российской Федерации. Данный портал является одним из популярных сервисов<sup>1</sup>, вход в который может осуществляться в том числе и посредством биометрической идентификации. В связи с чем допустимо создание информационных материалов о правах граждан в области защиты биометрии, обязательных для ознакомления при входе на портал.

8. Анализ функций МВД России по защите биометрических персональных данных позволяет сделать вывод о двойственности полномочий. С одной стороны МВД России является оператором по сбору, обработке и хранению физиологических и поведенческих характеристик физического лица, с другой стороны уполномочен осуществлять обязательную государственную дактилоскопическую регистрацию сотрудников полиции.

При этом область применения биометрических персональных данных весьма обширна, одновременно с их использованием МВД России реализует функцию по охране общественного порядка и обеспечению общественной безопасности и в то же время осуществляет функции органа публичной власти по оказанию услуг населению (например, выдача паспортов).

9. Доказана перспективность расширения полномочий должностных лиц органов внутренних дел Российской Федерации в сфере административной юрисдикции путем наделения их правами возбуждения и рассмотрения дел об административных правонарушениях, совершаемых в области биометрических

---

<sup>1</sup> На портале «Госуслуги» зарегистрировались более 112 млн человек / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://объясняем.пф/articles/news/na-portale-gosuslugi-zaregistrirovalis-bolee-112-mln-chelovek> / (дата обращения: 20.05.2025).

персональных данных, предусмотренных ч. 2.1. ст. 5.63, ч. 17 ст. 13.11, ст. 13.11.3, ч. 8 ст. 14.8 КоАП РФ.

**Теоретическая значимость исследования** заключается в том, что полученные результаты развивают и углубляют теоретические положения административного и административно-процессуального права в вопросах, затрагивающих противоправные случаи, связанные с нарушением прав в области правовой защиты биометрических персональных данных.

Вкладом в теорию информационного права является расширение концептуальных представлений о биометрических персональных данных, их нормативно-правовом регулировании. Предложенные решения способны восполнить пробелы в административно-правовом регулировании сбора, обработки и хранения биометрических персональных данных. Полученные результаты исследования могут послужить предпосылками для дальнейших научных исследований в рассматриваемой сфере.

**Практическая значимость исследования** заключается в том, что изложенные в нем выводы, предложения и рекомендации по совершенствованию административно-правового регулирования защиты биометрических персональных данных, способны обеспечить должную защиту прав и законных субъектов биометрических характеристик.

Как свидетельствуют акты внедрения результатов диссертационного исследования, его материалы востребованы в учебном процессе образовательных организаций высшего образования МВД России при изучении дисциплин «Административное право», «Основы информационной безопасности в ОВД», «Основы кибербезопасности», при подготовке слушателями выпускных квалификационных работ, а также в системе занятий по профессиональной служебной подготовке в подразделениях ОВД РФ и образовательных организациях высшего образования системы МВД России.

**Степень достоверности и апробация результатов исследования** обусловлены выбором и применением методов исследования научной методологии, предусматривающие системное, комплексное рассмотрение

проблематики диссертации, изучение эмпирического материала. Проанализирован широкий круг теоретических и нормативных источников, правоприменительная практика.

Результаты диссертации использовались при подготовке научных публикаций, внедрении соответствующих научных разработок в учебный процесс и правоприменительную деятельность органов внутренних дел. Основные теоретические положения исследования, выводы и предложения диссертанта изложены в 17 научных статьях, 4 из которых опубликованы в журналах, входящих в перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук.

Также результаты диссертационного исследования докладывались диссертантом и обсуждались на 14 всероссийских научных конференциях: Всероссийская научно-практическая конференция «Актуальные вопросы административного права и процесса» (Белгород, 2024 г., 2025 г.), Всероссийская научно-практическая конференция «Актуальные проблемы административного и административно-процессуального права (Сорокинские чтения)» (Санкт-Петербург, 2023 г., 2024 г., 2025 г.), Всероссийская научно-практическая конференция «Проблемы юриспруденции и педагогики высшей школы в работах молодых ученых» (Белгород, 2022 г., 2023 г., 2024 г.), Всероссийский конгресс «Санкт-Петербургские встречи молодых ученых» (Санкт-Петербург, 2023 г., 2024 г.), Всероссийская научно-практическая конференция, посвященная 30-летию принятия Конституции Российской Федерации «Российский конституционализм: история, теория и практика» (Белгород, 2024 г.), Всероссийская научно-практическая конференция «Актуальные проблемы полицейского права» (Омск, 2023 г.), Всероссийская научно-практическая конференция адъюнктов, аспирантов и соискателей «Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований» (Санкт-Петербург, 2022 г.), XIII Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии» (Калининград, 2024 г.).

Материалы и результаты диссертации применяются в образовательном процессе и научно-исследовательской деятельности Санкт-Петербургского университета МВД России, Омской академии МВД России и Белгородского юридического института МВД России имени И.Д. Путилина.

Диссертация подготовлена, обсуждена и одобрена на заседании кафедры административно-правовых дисциплин Белгородского юридического института МВД России имени И.Д. Путилина и рекомендована к защите.

Ряд выводов и предложений используются в системе профессиональной служебной деятельности Белгородского областного суда, Управления организации деятельности участковых уполномоченных полиции и подразделений по делам несовершеннолетних Управления МВД России по Белгородской области, Яковлевского межрайонного следственного отдела следственного управления Следственного комитета Российской Федерации по Белгородской области.

**Структура диссертации** обусловлена характером исследования и состоит из введения, двух глав, объединяющих шесть параграфов, заключения, списка литературы и приложений.

# ГЛАВА 1. АДМИНИСТРАТИВНО-ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

## § 1. Биометрические персональные данные как объект правовой защиты

История становления биометрических персональных данных представляет собой сложный процесс. Периодизация развития идентификации с использованием биометрических характеристик основывается на хронологических периодах становления ее отдельных видов – изображения человека, дактилоскопической информации, геномной информации и т.д.

Исследования исторического характера в отношении биометрических персональных данных осуществлялись Л.А. Конновой и Г.К. Артамоновой<sup>1</sup>, Е.Г. Барковской<sup>2</sup>, Ю.И. Лебеденко<sup>3</sup>, А.И. Челышевым<sup>4</sup>, И.С. Звягиным и А.Ю. Евреиновой<sup>5</sup>, Ш.Н. Хазиевым<sup>6</sup> и другими учеными.

Особенность развития биометрических персональных данных заключается в том, что выделение отдельных этапов является результатом технологического прогресса и правовых потребностей в области защиты биометрических персональных данных.

Безусловно, история биометрических персональных данных тесно связана со становлением криминалистики. Исторически сложилось, что для идентификации биометрические персональные данные использовались в большей степени в правоохранительной деятельности. При этом наука давала возможность

---

<sup>1</sup> Коннова Л.А., Артамонова Г.К. Идентификации личности – история развития и вклад в безопасность жизнедеятельности // Надзорная деятельность и судебная экспертиза в системе безопасности. 2017. № 1. С. 42–49.

<sup>2</sup> Барковская Е.Г. Исторические предпосылки и практические потребности интеграции биометрического и криминалистического знания // Философия права. 2010. № 6(43). С. 28–31.

<sup>3</sup> Лебеденко Ю.И. Биометрические системы безопасности. Тула: ТулГУ, 2012. 159 с.

<sup>4</sup> Челышев А.И. История становления отечественной криминалистики // Вестник Владимирского юридического института. 2006. № 1(1). С. 152–155.

<sup>5</sup> Звягин И.С., Евреинова А.Ю. Основы криминалистической биометрической идентификации // Вестник Воронежского института МВД России. 2025. № 1. С. 209–214.

<sup>6</sup> Хазиев Ш.Н. Криминалистические и судебно-экспертные основы современных биометрических технологий // Теория и практика судебной экспертизы. 2023. Т. 18, № 1. С. 16–21.

использовать в качестве идентификаторов все больший перечень биологических, физиологических и поведенческих характеристик человека.

Исследовав вопросы исторического развития совокупности отдельных биометрических характеристик, мы выделили следующие этапы становления биометрических персональных данных.

I. Донаучный период (VII–XVI вв.). Одно из первых упоминаний биометрических персональных данных относится к дактилоскопической информации, ставшей известной еще в 650 г. нашей эры. Китайский писатель периода Тангов Киа Кунг-Йен отмечал, что в его время отпечатками пальцев пользовались в Китае для предотвращения подделок документов<sup>1</sup>. Уже в VII веке дактилоскопическая информация гарантировала безопасность при подтверждении личности. Однако, на данном этапе не формировались картотеки, и отпечатки пальцев с целью идентификации использовались только для конкретных гражданско-правовых отношений.

К донаучному периоду также относится нанесение в Средневековье каких-либо обозначений лицам, совершившим преступления (правонарушения), в целях их идентификации. В качестве идентификаторов человека употребляли различные способы создания искусственных особых примет путем нанесения на тело татуировок и рубцов, в том числе и путем калечения и клеймения<sup>2</sup>. В России в 1691 г. Указом Петра I предписывалось ссылать всех, кто освобожден от смертной казни, предварительно «запятнав» буквой «В» («буде впредь, кто из тех воров из ссылки сбежит, а объявится в Москве, был бы познан»)<sup>3</sup>.

Таким образом, донаучный период характеризуется практической значимостью биометрических характеристик в процессе идентификации, которая проводилась путем сопоставления отпечатков пальцев и оставлении на теле

---

<sup>1</sup> Криминалистика: Техника и тактика расследования преступлений / под ред. А.Я. Вышинского. М: Юрид. изд-во, 1938. – 11 с.

<sup>2</sup> Барковская Е.Г. Исторические предпосылки и практические потребности интеграции биометрического и криминалистического знания // Философия права. 2010. № 6(43). С. 28.

<sup>3</sup> Коннова Л.А., Артамонова Г.К. Идентификации личности – история развития и вклад в безопасность жизнедеятельности // Надзорная деятельность и судебная экспертиза в системе безопасности. 2017. № 1. С. 43.

отдельных граждан специальных отметок. При этом в указанный исторический период не предпринималось попыток систематизировать практические знания и не создавались картотеки имеющихся материалов.

II. Зарождение научного знания о биометрических характеристиках человека (XVII в. – середина XX вв.).

Данный период характеризуется тем, что в достаточно короткий промежуток времени появились основные виды учетов – по внешним признакам, дактилоскопия и фотографическая регистрация<sup>1</sup>. Появление этих учетов связано с именами таких ученых, как Э.Ф. Видок, А. Бертильон, У. Гершель, Ф. Гальтон, Г. Фулдс, Э. Генри и многими другими<sup>2</sup>.

Основные исторические открытия произошли в период XIX-XX веков<sup>3</sup>.

Идентификация по внешним признакам стала использоваться в России в XVII веке. В заемных кабалах, жилых записях использовались описания физических особенностей для идентификации беглых работников или должников<sup>4</sup>.

Однако как научное явление данный вид идентификации был сформирован лишь в конце XIX в. Альфонсом Бертильоном. Им был разработан и систематизирован словесный портрет как метод описания внешних признаков человека для целей розыска и отождествления<sup>5</sup>.

Почти одновременно с этим в августе 1877 года служащий британской администрации в Индии Вильям Гершель предложил новый метод дактилоскопической идентификации личности. В 1879-1880 годах шотландский врач Генри Фолдс, работавший тогда в токийской больнице, независимо

---

<sup>1</sup> Койсин А.А. История становления и развития уголовной (криминалистической) регистрации // Сибирский юридический вестник. 2018. № 2(81). С. 104.

<sup>2</sup> Там же.

<sup>3</sup> Тимченков В.А., Нестерова О.В. Исторический опыт и вектор развития дактилоскопической экспертизы в РФ // Наукосфера. 2021. № 5-2. С. 247.

<sup>4</sup> Шейдаева С.Г. Ивашка из XVII века: отражение внешности человека в русской деловой письменности и в системе антропонимов // Вестник Удмуртского университета. Серия История и филология. 2022. Т. 32, № 4. С. 697.

<sup>5</sup> Ищенко Е.П., Топорков А.А. Криминалистика: учебник. – 2-е изд. – М.: Инфра-М, 2006. С. 31.

от Вильяма Гершеля, предложил использовать отпечатки пальцев рук для разоблачения преступников<sup>1</sup>.

В 1892 году англичанин Френсис Гальтон издал книгу «Отпечатки пальцев», в которой рассмотрел вопросы упорядочения отпечатков пальцев и их использования для идентификации личности<sup>2</sup>. А уже в 1895 году в Лондоне впервые была создана упрощенная картотека преступников по методу «бертильонажа» с отпечатками пальцев их рук, а к началу XX века дактилоскопия стала основным методом регистрации преступников<sup>3</sup>. Научное же становление дактилоскопии получило свое развитие в странах Европы и связано с именами итальянца Марчелло Мальпиги и чеха Яна Пуркинье<sup>4</sup>.

В России в 1906 году циркуляром № 1 «О применении антропометрии и фотографии к регистрации преступников» Департамент полиции узаконил сбор отпечатков пальцев как более надежный метод<sup>5</sup>. Дактилоскопические карты использовались для идентификации военнопленных и репрессированных.

Таким образом, данному этапу присущи сбор и накопление определенной криминалистически значимой информации о личности преступника (подозреваемого) и внесение такой информации в специальные карты (журналы). Это стало возможным благодаря формированию научного знания о биометрических характеристиках человека.

III. Период научного становления биометрических характеристик в условиях научно-технического прорыва (середина XX вв. – конец XX вв.).

Данный период стал возможен благодаря достижениям науки, которые позволяют идентифицировать человека по более широкому перечню биологических, физиологических и поведенческих характеристик. В этот период

<sup>1</sup> Тебекин А.В., Глазунова И.В. Влияние технологических укладов на развитие криминалистики в XVIII-XX веках // Вестник Российской таможенной академии. 2016. № 2. С. 82.

<sup>2</sup> Возгрин И.А. История возникновения и развития криминалистики // Вестник Санкт-Петербургского университета МВД России. 2000. № 2(6). С. 90.

<sup>3</sup> Там же.

<sup>4</sup> Соколова О.А., Пономарев В.В. Дактилоскопия и дактилоскопическая экспертиза: учебник для вузов / под общ. ред. О.А. Соколовой. М.: Юрайт, 2025. С. 11.

<sup>5</sup> Сборник циркуляров Министерства внутренних дел по вопросам воинской и военно-конской повинности. 1874-1906. – 3-е изд., доп. и испр. – СПб.: Упр. по делам о воинской повинности М-ва внутренних дел, 1906. 747 с.

были сделаны важные открытия, такие как структура ДНК, которая содержит геномную информацию, а также уникальные особенности радужной оболочки глаза и другие биометрические параметры.

Генетическими исследованиями человечество занимается достаточно давно, вопросы наследственности и способов кодирования признаков и функций организма разрабатывались уже в XIX веке<sup>1</sup>. И уже в XX в. выдающимся достижением науки становится разработка идентификационных методов исследования ДНК человека<sup>2</sup>.

В 1985 г. в журнале «Nature» была опубликована статья английских ученых во главе с профессором Лейстерского университета Алеком Джеффрисом об индивидуальности и неизменяемости строения ДНК человека. Позже изобретение полимеразной цепной реакции (ПЦР) Кэри Муллисом позволило анализировать микроскопические образцы ДНК (слюна на окурке, волос с луковицей, капля крови)<sup>3</sup>.

Благодаря активному развитию технических средств вместо полной расшифровки генома стали анализировать STR-локусы (короткие tandemные повторы)<sup>4</sup>. Их количество в ключевых локусах (например, 16 маркеров) обеспечивало точность идентификации до 99.9%.

Радужная оболочка глаза признается одним из самых точных биометрических параметров благодаря уникальности узора, формирующегося к 8-му месяцу внутриутробного развития и сохраняющегося неизменным в течение всей жизни (за исключением редких травм или заболеваний). В 1936 году американский офтальмолог Фрэнк Бурш впервые предположил, что узор радужки

---

<sup>1</sup> Правовое обеспечение безопасного использования генетической и геномной информации: учебник для вузов / под ред. Л.Н. Берг, А.В. Лисаченко. М.: Юрайт, 2025. С. 19.

<sup>2</sup> Барковская Е.Г. Исторические предпосылки и практические потребности интеграции биометрического и криминалистического знания // Философия права. 2010. № 6(43). С. 30.

<sup>3</sup> Полимеразная цепная реакция в микробиологии / Д.П. Гладин, А.М. Королюк, И.В. Дробот [и др.] // Российские биомедицинские исследования. 2021. Т. 6, № 3. С. 37.

<sup>4</sup> Применение метода коротких tandemных повторов для аутентификации клеточных линий / М.Д. Хорольский, И.С. Семенова, Е.В. Мельникова, Ю.В. Олефир // Биопрепараты. Профилактика, диагностика, лечение. 2019. Т. 19, № 4. С. 253.

можно использовать для идентификации личности<sup>1</sup>. Несмотря на то, технологии того времени не позволяли реализовать эту концепцию в полной мере, она стала основой для будущих разработок, которые получили широкое распространение только в конце XX – начале XXI века<sup>2</sup>. В 1987 году: офтальмологи Леонард Флом и Аран Сафир оформили патент на метод идентификации по радужной оболочке глаз, но не разработали практических алгоритмов. Только в 1993 году Джон Даугман создал первый рабочий алгоритм обработки изображений радужки<sup>3</sup>.

Таким образом, развитие технических возможностей позволило выйти идентификации на новый уровень, обеспечив высокую точность при установлении личности.

#### IV. Период автоматизации идентификации (1990-2015 гг.).

В XX веке началось расширение биометрии, появление автоматизированных дактилоскопических систем, а затем и других методов – распознавания радужки, строения лица, голоса, поведенческих признаков.

С наступлением XXI века биометрия не только стала повсеместной – от смартфонов до пограничного контроля, но и тесно соединилась с аппаратной криптографией, формируя высоконадежные решения<sup>4</sup>.

В 1998 году ФБР запускает биометрическую базу данных CODIS, хранящую информацию обо всех ДНК-отпечатках, найденных в ходе следственных мероприятий. В 2005 году Sarnoff Corp. демонстрирует систему фотографирования радужки глаза, способную работать незаметно для человека. В 2013 году Индия становится обладателем крупнейшей мультимодальной (то есть использующей сразу несколько индикаторов) биометрической базы данных AAdhaar<sup>5</sup>.

---

<sup>1</sup> Барсуков С.С. Криминалистическая идентификация по радужной оболочке и сетчатке глаза: современные возможности и проблемы применения // Юрист-Правовед. 2021. № 1(96). С. 170.

<sup>2</sup> Постников Н.А. Биометрия сквозь века: от первых отпечатков к современным методам идентификации // Поволжский вестник науки. 2025. № 1(35). С. 31.

<sup>3</sup> Дроздов А.В. Криминалистическая идентификация по радужной оболочке глаза // Вестник Сибирского юридического института ФСКН России. 2013. № 1(12). С. 83.

<sup>4</sup> Постников Н.А. Биометрия сквозь века: от первых отпечатков к современным методам идентификации. С. 39.

<sup>5</sup> Долганова О.И. Сотрудничество стран Азии в области цифровой идентификации личности // Азия и Африка сегодня. 2023. № 7. С. 43.

Анализ данного периода указывает на возникшие возможности использования биометрических персональных данных для идентификации в условиях глобализма. Автоматизация процессов повысила точность идентификации, увеличила скорость обработки данных и сделала популярной биометрию во всем мире.

V. Период развития биометрических персональных данных в условиях цифровизации общества (2016 г. – по настоящее время).

При этом для данного периода характерным является три значимых особенности:

- биометрия выходит за рамки идентификации в целях обеспечения функций правоохранительной деятельности, а приобретает повсеместный характер использования, в том числе в гражданских правоотношениях;
- активно формируется область правового регулирования биометрических персональных данных;
- для идентификации, а также быстрого поиска конкретного гражданина, используются биометрические персональные данные с применением систем искусственного интеллекта<sup>1</sup>.

Анализируя этапы исторического развития биометрических персональных данных, можно утверждать, что их уникальность была отмечена еще в древности, однако научный переход от теоретических исследований к практическому применению биометрической идентификации занял сравнительно короткий промежуток времени. Благодаря научно-техническим достижениям биометрическая идентификация упростила многие современные процедуры, обеспечив максимальную степень безопасности. Однако нам еще предстоит совершенствовать данную область как в правовом поле, так и в техническом обеспечении.

---

<sup>1</sup> Ковалева Н.Н., Жирнова Н.А. Проблемы обеспечения конфиденциальности персональных данных при использовании систем искусственного интеллекта // Журнал российского права. 2024. Т. 28, № 7. С. 115.

Сегодня видится очевидным тот факт, что без развития информационных технологий невозможно какое-либо развитие или модернизация<sup>1</sup>. Поскольку технологии биометрической идентификации и аутентификации становятся все более распространенными, крайне важно решать возникающие в связи с этим проблемы как этического, так и правового порядка<sup>2</sup>. Законодательные органы стремятся урегулировать имеющиеся и вновь возникающие вопросы в сфере обработки и защиты биометрических персональных данных<sup>3</sup>.

Так, 30 декабря 2021 года Единая биометрическая система стала государственной информационной системой и частью инфраструктуры, обеспечивающей взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме. 29 декабря 2022 года вступил в силу ФЗ № 572 «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации», определяющий единые правила для государственных и коммерческих систем по применению биометрии для предоставления услуг<sup>4</sup>.

Сфера цифровизации – это область общественных отношений, которая направлена на урегулирование социальных, политических, правовых, экономических, культурных и иных областей общественной жизни при помощи информационных технологий; обусловлена переходом на цифровой способ связи,

---

<sup>1</sup> Дизер О.А. Совершенствование административно-правовой защиты прав граждан в условиях формирования и развития информационного общества / Актуальные проблемы административного и административно-процессуального права (Сорокинские чтения): Международная научно-практическая конференция, Санкт-Петербург, 26 марта 2021 года / под общ. ред. А.И. Каплунова. СПб.: СПбУ МВД России, 2021. С. 64.

<sup>2</sup> Фатхи В.И. К вопросу о правовом регулировании порядка использования биометрических персональных данных: международный опыт // Философия права. 2023. № 4 (107). С. 98.

<sup>3</sup> Степенко В.Е., Богдановская А.Д. Биометрические персональные данные // Евразийский Союз Ученых. 2020. № 4 (73). С. 19.

<sup>4</sup> Единая биометрическая система – один из ключевых проектов цифровой инфраструктуры страны / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://ebs.ru/company/> (дата обращения: 26.12.2023).

записи и передачи данных с помощью цифровых устройств, а также реализации информационных прав и обязанностей<sup>1</sup>.

Цифровизация позволила внедрить биометрические персональные данные во все сферы жизни общества.

В России – это обслуживание в МФЦ без предъявления паспорта<sup>2</sup>, «оплата по биометрии» в платежном терминале или на кассе самообслуживания<sup>3</sup>, заселение в гостиницу<sup>4</sup>, вход на объекты без пропусков и многое другое.

Сегодня технологии биометрической идентификации личности являются неотъемлемой частью мирового рынка информационных технологий и становятся важным инструментом для решения широкого круга задач правоохранительной деятельности, а также гражданско-правовых отношений<sup>5</sup>.

Объем платежей по биометрии составляет всего 7,8 млрд руб. За 9 месяцев 2024 года таким образом было совершено 16,2 млн покупок. Платежи по биометрии также развивают Сбербанк и Национальная система платежных карт (НСПК). Сбербанк установил уже около 1 млн биометрических терминалов по всей стране, через которые покупки могут совершать как клиенты «Сбера», так и клиенты других банков<sup>6</sup>.

Биометрия – явление чрезвычайно многоплановое и может составить объект исследования технических и инженерных, биологических и правовых наук<sup>7</sup>. Сразу вызывает дискуссию употребление термина биометрия.

---

<sup>1</sup> Гусева Т.А. Цифровизация в публично-правовой и частно-правовой сферах. – Орёл: Орловский государственный университет имени И.С. Тургенева, 2024. С. 5.

<sup>2</sup> Обслуживание без паспорта/ Официальный интернет-сайт [Электронный ресурс]. – URL: [https://ebs.ru/services/?ELEMENT\\_ID=4189741](https://ebs.ru/services/?ELEMENT_ID=4189741) (дата обращения: 24.05.2025).

<sup>3</sup> Биоэквайринг – оплачивайте покупки по-новому / Официальный интернет-сайт [Электронный ресурс]. – URL: [https://ebs.ru/bio\\_pay/](https://ebs.ru/bio_pay/) (дата обращения: 10.06.2025).

<sup>4</sup> Заселение в гостиницу / Официальный интернет-сайт [Электронный ресурс]. – URL: [https://ebs.ru/services/?ELEMENT\\_ID=4623307](https://ebs.ru/services/?ELEMENT_ID=4623307) (дата обращения: 06.05.2025).

<sup>5</sup> Дивольд В.Е. Предпосылки создания национальной системы биометрической идентификации личности // Научный вестник Омской академии МВД России. 2021. Т. 27, № 2(81). С. 139.

<sup>6</sup> ЦБ впервые раскрыл объем платежей россиян по лицу и QR-кодам / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://www.rbc.ru/finances/> (дата обращения: 11.05.2025).

<sup>7</sup> Безверхов А.Г., Юдин А.В. Биометрия и право: вопросы теории и права // Юридический вестник Самарского университета. 2021. Т. 7, № 1. С. 7–8.

Не случайно С.А. Старостин отмечал: «точность и качество формулировок есть залог качества законодательства, а, следовательно, и эффективности государственного управления»<sup>1</sup>.

В научном мире понятие биометрии используется в разных значениях в зависимости от научного направления.

В широком смысле биометрия (от лат. *bios* – жизнь и *metron* – мера) – это наука о применении математических методов в биологии<sup>2</sup>. Данное определение используют Ю.А. Брюхомицкий, Г.Ф. Лакин<sup>3</sup>, П.С. Катмаков, В.П. Гавриленко, А.В. Бушов<sup>4</sup> и другие.

Иное определение применяют В.И. Волчихин, А.И. Иванов, И.Г. Назаров и Ю.К. Язова. Под биометрией они понимают науку, использующую измеряемые параметры самого человека и его поведения, называемые биометрическими характеристиками, для количественного описания облика индивидуума<sup>5</sup>.

Однако на сегодняшний день термин «биометрия» условно применяется для обозначения совокупности биометрических характеристик. Так, на официальном интернет-ресурсе для информирования о социально-экономической ситуации в России (ОБЪЯСНЯЕМ.РФ) приводится определение биометрии как информации о физиологических и биологических параметрах человека, позволяющих установить его личность<sup>6</sup>.

Именно в этом контексте данный термин используют Председатель Государственной Думы Федерального Собрания Российской Федерации

<sup>1</sup> Старостин С.А. О подмене понятий в государственном управлении // Вестник Томского государственного университета. 2019. № 32. С. 93.

<sup>2</sup> Брюхомицкий Ю.А. Биометрические технологии идентификации личности: учебное пособие. Ростов-на-Дону; Таганрог: Южный федеральный университет, 2017. С. 288.

<sup>3</sup> Лакин Г.Ф. Биометрия. – 3-е изд. М.: Высшая школа, 1980. С. 291.

<sup>4</sup> Катмаков П.С. Биометрия: учебник для вузов / П.С. Катмаков, В.П. Гавриленко, А.В. Бушов. – 3-е изд., перераб. и доп. – М.: Юрайт, 2025. – 186 с. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: <https://urait.ru/bcode/565172> (дата обращения: 14.07.2025).

<sup>5</sup> Нейросетевая защита персональных биометрических данных: монография / Волчихин В.И., Иванов А.И., Назаров И.Г. [и др.]; под ред. Ю.К. Язова. М.: Радиотехника, 2012. С. 8.

<sup>6</sup> Пароль не нужен: что нужно знать о биометрии / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://объясняем.рф/articles/useful/biometricheskie-dannye-chto-nuzhno-znat/> (дата обращения: 03.09.2024).

В.В. Володин<sup>1</sup>, заместитель Председателя Правительства Российской Федерации – Руководитель Аппарата Правительства Российской Федерации Д.Ю. Григоренко<sup>2</sup>, Заместитель Председателя Государственной Думы Федерального Собрания Российской Федерации И.А. Яровая<sup>3</sup> и другие.

В дальнейшем в нашем исследовании мы будем опираться на последнее приведенное определение биометрии. Так как в современных условиях именно оно объединяет совокупность биометрических характеристик и является популярным в правовой и научных сферах.

При этом научной дискуссии подвергается и само определение понятия биометрических персональных данных.

В российском законодательстве термин «биометрические персональные данные» впервые использован в Федеральном законе от 15 августа 1996 г. № 114-ФЗ «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию». В данном нормативном правовом акте упоминалось о том, что основные документы, удостоверяющие личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию, могут содержать биометрические персональные данные<sup>4</sup>. Однако данный Федеральный закон не раскрывал понятия «биометрические персональные данные» и соответственно не предусматривал перечень таких данных. Это создавало правовую неопределенность и в данном вопросе приходилось опираться на опыт зарубежных стран.

---

<sup>1</sup> Законопроект о единой системе биометрических данных россиян принят во втором чтении / Официальный интернет-сайт [Электронный ресурс]. – URL: <http://duma.gov.ru/news/56071/> (дата обращения: 02.02.2023).

<sup>2</sup> Совещание с членами Правительства / Официальный интернет-сайт [Электронный ресурс]. – URL: <http://www.kremlin.ru/events/president/news/76409> (дата обращения: 27.03.2025).

<sup>3</sup> Ирина Яровая: Государственная Дума качественно и системно отработала вопросы противодействия нелегальной миграции / Официальный интернет-сайт [Электронный ресурс]. – URL: <http://duma.gov.ru/news/60401/> (дата обращения: 30.11.2024).

<sup>4</sup> Федеральный закон от 15 августа 1996 г. № 114-ФЗ «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию» // Собрание законодательства Российской Федерации. 1996. № 34. Ст. 4029.

Определение биометрии в российском законодательстве было закреплено значительно позже – в 2006 году и используется по настоящее время. В Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных» под биометрическими персональными данными понимаются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные), и которые используются оператором для установления личности субъекта персональных данных<sup>1</sup>.

Сегодня учеными активно обсуждается вопрос о необходимости внесения изменений в закрепленное вышеуказанным Федеральным законом определение биометрических персональных данных<sup>2</sup>. Это обусловлено развитием современной системы административно-правовой защиты биометрических персональных данных<sup>3</sup>.

Н.И. Платонова<sup>4</sup>, С.В. Баженов, В.Е. Дивольд, А.А. Морозов<sup>5</sup>, Э.В. Талапина<sup>6</sup> и другие предлагали формирование определения биометрических персональных данных в целях создания действенной системы административно-правовой защиты с учетом современных вызовов.

Н.И. Платонова предлагала следующее понятие биометрических персональных данных: «Сведения, которые характеризуют физиологические, физические и поведенческие особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые

<sup>1</sup> Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 31 (1 ч.). Ст. 3451.

<sup>2</sup> Терещенко И.А. Биометрические персональные данные: проблемы и перспективы определения понятия // Закон и право. 2024. № 2. С. 187.

<sup>3</sup> Данелян Р.Н., Яковлев-Чернышев В.А. Особенности правового регулирования биометрических персональных данных в Российской Федерации // Вестник Казанского юридического института МВД России. 2024. Т. 15, № 3(57). С. 31.

<sup>4</sup> Платонова Н.И. Современные правовые подходы к пониманию биометрических данных // Информационное право. 2018. № 1. С. 25.

<sup>5</sup> Создание Концепции национальной системы биометрической идентификации личности / С.В. Баженов, В.Е. Дивольд, А.А. Морозов [и др.] // Труды Академии управления МВД России. 2020. № 2(54). С. 48.

<sup>6</sup> Талапина Э.В. Защита персональных данных в цифровую эпоху: российское право в Европейском контексте // Труды Института государства и права Российской академии наук. 2018. Т. 13, № 5. С. 133.

используются оператором для установления и подтверждения личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи»<sup>1</sup>.

В отличие от определения, предложенного Н.И. Платоновой, иное понятие приводят С.В. Баженов, В.Е. Дивольд, А.А. Морозов и другие. Авторы определяют биометрические персональные данные как сведения, которые характеризуют физиологические, биологические и поведенческие особенности человека, на основании которых можно установить его личность<sup>2</sup>.

Еще одно определение биометрических персональных данных, закреплено в Регламенте Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR). В указанном Постановлении ЕС под биометрическими понимаются персональные данные, полученные в результате специальной технической обработки, относящиеся к физическим, физиологическим или поведенческим характеристикам физического лица, позволяющим или подтверждающим уникальную идентификацию этого физического лица, например, изображения лица или дактилоскопические данные<sup>3</sup>.

В ходе анализа зарубежного опыта также представляется важным определение биометрических персональных данных, используемое в США. Хочется отметить, что в США нет централизованного федерального нормативного правового акта, регулирующего отношения, связанные с биометрией. При этом в законодательстве штатов принципиально отличаются

<sup>1</sup> Платонова Н.И. Современные правовые подходы к пониманию биометрических данных. С. 25.

<sup>2</sup> Баженов С.В. [и др.] Создание Концепции национальной системы биометрической идентификации личности. С. 48.

<sup>3</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Электронный ресурс]. – URL: <https://ogdpr.eu/en/gdpr-2016>.

подходы к пониманию биометрических данных<sup>1</sup>. В соответствии с разделом 10 Закона штата Иллинойс «О конфиденциальности биометрической информации» биометрической информацией является любая информация, независимо от того, как она собирается, конвертируется, хранится или передается, на основе биометрического идентификатора человека<sup>2</sup>. Биометрическая информация не включает информацию, полученную из предметов или процедур, исключенных из определения биометрических идентификаторов<sup>3</sup>. Данное определение не дает ясности по многим правовым категориям, отличается «мягкой» силой правового регулирования.

Анализируя приведенные определения, отметим, что они отличаются от сегодняшнего законодательно закрепленного понятия биометрических персональных данных<sup>4</sup>. Каждое из них обладает рядом преимуществ, но и не лишено недостатков. Однако их ориентиры в совокупности могут дать основы для формирования современного определения биометрических персональных данных.

В приведенных выше определениях используются поведенческие характеристики, отсутствующие в настоящий момент в российском законодательстве, при этом активно используемые в науке и практической деятельности<sup>5</sup>.

К поведенческой биометрии относят обширный перечень особенностей, по которым можно идентифицировать человека. Одними из самых популярных в мире являются запись голоса, походка, мимика, жесты, управление компьютерной мышкой, работа на клавиатуре<sup>6,7,8</sup>. Каждая перечисленная

<sup>1</sup> Государственное регулирование Интернета и права человека / М.С. Саликов, С.Э. Несмеянова, Н.Е. Колобаева [и др.]. – Екатеринбург: УМЦ УПИ, 2022. С. 101.

<sup>2</sup> Monroy v. Shutterfly, Inc. No. 1:2016cv10984 – Document 39 (N.D. Ill. 2017).

<sup>3</sup> Государственное регулирование Интернета и права человека. С. 101.

<sup>4</sup> Карпушина А.В. К понятию биометрических персональных данных // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2023. № 4. С. 119.

<sup>5</sup> Динамические методы биометрической аутентификации / А.А. Островский, Д.Н. Жариков, В.С. Лукьянов, Д.С. Попов // Известия Волгоградского государственного технического университета. 2010. № 6(66). С. 73.

<sup>6</sup> Хазиев Ш.Н. Криминалистические и судебно-экспертные основы современных биометрических технологий // Теория и практика судебной экспертизы. 2023. Т. 18, № 1. С. 20.

<sup>7</sup> Свидетельство о государственной регистрации программы для ЭВМ № 2025661428 Российская Федерация. Биометрическая аутентификация по клавиатурному почерку: заявление. 17.04.2025: опубл. 06.05.2025 / В.А. Валиуллин.

<sup>8</sup> Хачумов М.В., Нгуен Т.З. Распознавание лиц по фотографиям на основе инвариантных моментов // Современные проблемы науки и образования. 2015. № 2-2. С. 187.

характеристика представляет собой мышечную память при воспроизведении определенного действия, которая является уникальной и неповторимой, что непосредственно удовлетворяет признакам биометрических персональных данных. Развитие современных технических устройств позволяет компьютеризированно обрабатывать огромный массив информации, в том числе и сопоставлять биометрические данные для аутентификации и идентификации, которые ранее не могли быть использованы ввиду сложности самих процессов сопоставления<sup>1</sup>.

Анализ правового регулирования в отношении поведенческих биометрических характеристик показал, что российским законодательством они защищены в наименьшей степени<sup>2</sup>.

Вопросы, связанные с административно-правовой защитой поведенческой биометрии, рассмотрены только в отношении записи голоса. Запись голоса человека регистрируется в единой биометрической системе<sup>3</sup>. Порядок сбора, обработки и хранения записи голоса в данной системе регулируется Федеральным законом от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных».

Подводя итог, необходимо отметить, что в сложившихся условиях требуется в понятии биометрических персональных данных законодательно закрепить поведенческие характеристики, чтобы избежать правового несоответствия нормативных положений и обеспечить административно-правовую защиту всем категориям биометрии, используемым для идентификации.

Н.И. Платонова обращала внимание на еще одну неточность в используемом в Федеральном законе о персональных данных определении

---

<sup>1</sup> Фролова Е.Ю., Кошлыкова Ю.А. Идентификация человека по биометрическим данным: обзор современных технологий // Северо-Кавказский юридический вестник. 2022. № 3. С. 168-173.

<sup>2</sup> Храмов Е.Н., Вершинина О.В. Биометрические технологии как фактор повышения безопасности и конкурентоспособности в финансовой инфраструктуре России // Фундаментальные исследования. 2025. № 4. С. 76.

<sup>3</sup> Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства Российской Федерации. 2023. № 1 (часть I). Ст. 19.

биометрических персональных данных. Она аргументировала, что физиологические характеристики есть часть биологических<sup>1</sup>. И если обратиться к специальной литературе, то, по мнению доктора биологических наук, профессора Д.Л. Теплого, автора учебника «Физиология человека и животных», под «физиологией» принято понимать раздел биологии, изучающий функции живых организмов, их клеток, органов и систем в единстве и взаимосвязи с окружающей средой, а также формирование физиологических функций на разных этапах индивидуального развития<sup>2</sup>. Это определение подтверждает замечание Н.И. Платоновой о неточности в определении. И в предложенном Н.И. Платоновой определении биометрических персональных данных вместо использования «биологические характеристики» употребляются «физические».

Эта позиция соответствует определению, приведенному в Регламенте Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR), где термин «биологические» отсутствует, но используется понятие «физические характеристики».

Исходя из этого, для совершенствования правового регулирования в области защиты биометрических персональных данных важно устранить данную коллизию в определении. Для более точной проработки используемой терминологии в определении целесообразно привлечение экспертов из числа ученых-антропологов.

Приведенные для анализа определения биометрических персональных данных указывают на основные признаки, характеризующие их. Изучение и выделение специальных признаков поможет сформулировать современное, соответствующее тенденциям в области развития биометрии, определение таких данных.

---

<sup>1</sup> Платонова Н.И. Современные правовые подходы к пониманию биометрических данных. С. 24.

<sup>2</sup> Физиология человека и животных: учебник / Д.Л. Теплый, Ю.В. Нестеров, Е.В. Курьянова [и др.]; под общ. ред. проф. Д.Л. Теплого. – Астрахань: Астраханский государственный университет, 2017. С. 24.

Данный вопрос остается мало изученным, в связи с чем, в рамках нашего исследования, на основе уже имеющихся научных положений о признаках биометрических персональных данных были структурированы их и выделены ранее неиспользуемые, но доказывающие свою эффективность на практике.

Н.И. Платонова подразделяла признаки на общие и специальные. Общие признаки определяют биометрию как часть персональных данных, в свою очередь специальные подчеркивают особенности и определяют место биометрических персональных данных в системе информации, подлежащей защите<sup>1</sup>. Данное выделение двух основных групп признаков является весьма обоснованным, однако расширение области применения биометрических персональных данных требует выделения дополнительных признаков.

Основываясь на положениях существующей правовой базы, регулирующей вопросы, связанные с биометрическими персональными данными, исследованиях Н.И. Платоновой, можно выделить следующие общие признаки:

1. Идентификация по биометрическим характеристикам проводится исключительно в отношении физических лиц.

Процесс биометрической идентификации может быть применен ко всем физическим лицам, независимо от их пола, расы, национальности, языковой принадлежности и других обстоятельств<sup>2</sup>. Биометрические данные представляют собой физические и физиологические характеристики, присущие человеку. То есть, биометрия ничто иное как информация о биологии человека (физическом строении с его особенностями), его облике и, в том числе, характерных чертах поведения (жесты, мимика, походка и т.д.).

В настоящее время, в условиях стремительного развития информационных технологий, как справедливо отмечено А.А. Протасевич и Е.И. Фойгель, субъектом восприятия внешнего облика являются не только органы чувств человека, но и технические устройства (веб-камера, камера наружного наблюдения, видеорегистратор, сканер, тачскрин мобильного смартфона), что

---

<sup>1</sup> Платонова Н.И. Современные правовые подходы к пониманию биометрических данных. С. 23.

<sup>2</sup> Трофимов А.А. Биометрическая идентификация субъектов частного права: понятие, признаки, способы // Правовая информатика. 2024. № 4. С. 82.

стирает равенство между рефлекторностью и воспринимаемостью внешнего облика человека. Точность восприятия таких устройств выше, чем у органа зрения человека, и позволяет воспринять не только видимые человеческому глазу признаки внешности, но и отдельные свойства слабовидимого характера<sup>1</sup>.

2. Цель сбора биометрических персональных данных – идентификация и аутентификация.

Понятие идентификации закреплено в Федеральном законе от 29 декабря 2022 г. № 572-ФЗ. Под идентификацией принято понимать совокупность мероприятий по установлению сведений о лице и их проверке, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению данных сведений с идентификатором<sup>2</sup>.

Важно, что наряду с идентификацией применяется и аутентификация, которая заключается в совокупности мероприятий по проверке лица на принадлежность ему идентификатора (идентификаторов)<sup>3</sup>. Идентификация и аутентификация являются взаимосвязанными процессами. При идентификации пользователь определяется путем сравнения его биометрических данных со всеми, имеющимися в системе, до момента нахождения совпадения. При биометрической аутентификации пользователь говорит системе, кто он такой (например, вводит уникальный логин), система по этому логину считывает его эталонные биометрические данные из базы данных и затем производит их сверку с теми, которые предоставляет пользователь<sup>4</sup>.

---

<sup>1</sup> Протасевич А.А., Фойгель Е.И. О возможностях криминалистической габитоскопии при реализации мер противодействия современной киберпреступности // Всероссийский криминологический журнал. 2020. Т. 14, № 3. С. 474.

<sup>2</sup> Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства Российской Федерации. 2023. № 1 (часть I). Ст. 19.

<sup>3</sup> Зайцев О.А., Пастухов П.С. Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений // Вестник Пермского университета. Юридические науки. 2022. № 56. С. 286.

<sup>4</sup> Панфилова О.А., Крюкова Д.Ю. Биометрические методы и системы идентификации личности при обеспечении информационной безопасности в уголовно-исполнительной системе: учебное пособие. Вологда, 2022. С. 23.

Именно цель сбора, обработки и хранения физиологических или поведенческих характеристик определяет относятся ли они к категории биометрических персональных данных. На это указывает судебная практика.

Отметим дело № 77RS0023-01-2019-012149-35, рассмотренное Савеловским районным судом города Москвы. Гражданка П. обратилась в ГУ МВД России с административным иском на Департамент информационных технологий (ДИТ) г. Москвы. По мнению истца, ДИТ с помощью камер видеонаблюдения обрабатывает ее биометрические персональные данные. Судебная коллегия не усмотрела факта идентификации, в связи с чем решила, что само по себе получение изображения истца в период ее нахождения на территории, попадающей под сектор наблюдения конкретной камеры, установленной в целях контроля за окружающей обстановкой, не является способом сбора биометрических персональных данных, поскольку не использовалось непосредственно для определения личности, а при отсутствии процедуры идентификации личности, видеоизображения граждан не могут считаться биометрическими персональными данными. Суд посчитал, что в рассматриваемом случае отсутствует необходимость получать письменное согласие гражданина на обработку биометрических персональных данных<sup>1</sup>.

Таким образом, согласно приведенному судебному решению можно сделать вывод, что биометрические персональные данные являются таковыми только при условии, что данные получены в целях идентификации и аутентификации личности. Технологии идентификации и аутентификации субъекта с применением биометрических данных широко используются при обеспечении национальной безопасности, в том числе являются мерой борьбы с террористической угрозой, массовыми беспорядками<sup>2</sup>.

3. Сбор биометрии предполагает ее фиксацию в специальных систематизированных базах.

---

<sup>1</sup> Информация по делу № 02а-0577/2019 / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://mos-gorsud.ru/rs/savyolovskij/services/cases/kas/details/988f386e-be51-47b0-b48f-e871043ef1fc> (дата обращения: 13.04.2025).

<sup>2</sup> Государственное регулирование Интернета и права человека / М.С. Саликов, С.Э. Несмеянова, Н.Е. Колобаева [и др.]. Екатеринбург: УМЦ УПИ, 2022. С. 95.

Технологический прогресс на современном этапе привел к созданию систем идентификации и аутентификации личности на основе биометрических персональных данных<sup>1</sup>. Для фиксации, хранения и обработки биометрии создаются базы данных как в правоохранительных органах, так и в органах публичной власти. Учитывая специфику биометрических персональных данных, часто эти базы выделяются в отдельные, в зависимости от их вида.

Сегодня существуют Федеральная база данных геномной информации<sup>2,3</sup>, Централизованная интегрированная автоматизированная дактилоскопическая информационная система МВД России<sup>4,5</sup>, единая биометрическая система<sup>6,7</sup>.

Зафиксированные с соблюдением законодательных норм биометрические персональные данные подлежат хранению в указанных базах и в установленных законом сроках.

Для приведенных баз характерным является идентификация по отдельным биометрическим характеристикам, однако единая биометрическая система обобщает сразу две характеристики – запись голоса человека, полученную с

---

<sup>1</sup> Создание Концепции национальной системы биометрической идентификации личности / С.В. Баженов, В.Е. Дивольд, А.А. Морозов [и др.] // Труды Академии управления МВД России. 2020. № 2(54). С. 43.

<sup>2</sup> Федеральный закон от 3 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации // Собрание законодательства РФ. 2008. № 49. Ст. 5740.

<sup>3</sup> Попова Т.В., Сергеев А.Б. Федеральная база данных геномной информации в системе обеспечения баланса частных и публичных интересов в уголовном судопроизводстве // Юридическая наука и правоохранительная практика. 2017. № 1(39). С. 134.

<sup>4</sup> Приказ МВД России от 19.06.2018 № 384 (ред. от 20.05.2024) «Об утверждении Порядка проведения идентификации личности человека по отпечаткам пальцев (ладоней) рук в режиме реального времени и Перечня категорий лиц, в отношении которых обязательная государственная дактилоскопическая регистрация не проводится в случае идентификации их личности в результате проверки по отпечаткам пальцев (ладоней) рук в режиме реального времени» // СПС «КонсультантПлюс».

<sup>5</sup> Серго С.В., Снежкова Ж.Ю. К вопросу о реорганизации баз данных дактилоскопических учетов // Юристъ-Правоведъ. 2022. № 1(100). С. 124.

<sup>6</sup> Постановление Правительства РФ от 31 мая 2023 г. № 883 «Об утверждении Положения о единой биометрической системе, в том числе о ее региональных сегментах, и о признании утратившим силу постановления Правительства Российской Федерации от 16 июня 2022 г. № 1089» [Электронный ресурс]. – URL: <http://publication.pravo.gov.ru/document/00012023060100>.

<sup>7</sup> Полякова Т.А., Бойченко И.С. Особенности взаимодействия и правового обеспечения информационной безопасности в единой биометрической системе в Российской Федерации // Правовая политика и правовая жизнь. 2023. № 3. С. 28.

помощью звукозаписывающих устройств, и изображение лица человека, полученное с помощью фотовидеоустройств.

Использование нескольких невзаимосвязанных систем фиксации биометрических персональных данных вызывает дискуссию, особенно на фоне разработок по созданию цифрового профиля гражданина, который предполагает объединение всей совокупности персональных данных, в том числе биометрических<sup>1</sup>.

Делая вывод по данному признаку, отметим, что фиксация биометрических персональных данных производится в отдельных базах в зависимости от целей сбора. При этом в современных условиях данный подход может быть совершенствован в пользу создания единой системы биометрических персональных данных, которая сможет обобщить всю их совокупность, однако, в интересах соблюдения конфиденциальности, необходимо будет предусмотреть ограничение доступа к определенной категории информации.

Приведенные в рамках исследования признаки вытекают из действующего законодательства в области биометрических персональных данных и представляют собой группу общих признаков. Однако биометрические персональные данные обладают рядом специальных признаков, к которым можно отнести следующие:

1. Уникальность. Когда вопрос встает о биометрии, мы сразу понимаем, что каждая биометрическая характеристика отдельного человека уникальна<sup>2</sup>. Именно это делает возможным проведение идентификации. Существует много уникальных параметров человека, которые можно использовать в качестве основы для идентификации<sup>3</sup>. Даже у близких родственников не бывает идентичных дактилоскопических данных, как не бывает и одинакового голоса.

---

<sup>1</sup> Минбалеев А.В. Проблемы цифрового права. Саратов: Амирит, 2022. С. 143.

<sup>2</sup> Дивольд В.Е. Предпосылки создания национальной системы биометрической идентификации личности. С. 140.

<sup>3</sup> Панфилова О.А., Крюкова Д.Ю. Биометрические методы и системы идентификации личности при обеспечении информационной безопасности в уголовно-исполнительной системе. С. 5.

Даже если голоса кажутся похожими, каждый из них обладает какой-то определенной характеристикой, отличающей его от других.

2. Универсальность. Биометрия непосредственно связана с отдельной личностью, подтверждает ее идентичность и уникальность, и поэтому она выступает по-своему универсальным идентификатором<sup>1</sup>. Этот признак заключается в том, что идентификация проводится строго по определенным показателям, свойственным каждому человеку. Простым примером может служить геномная информация. Каждый человек обладает геном, но при этом у каждого человека он уникален, что позволяет его идентифицировать с высокой долей вероятности.

3. Следующий признак включает в себе два показателя, одновременно противоположных друг другу – невозможность к изменениям и изменчивость. Этот признак характеризует качественную сторону используемой для идентификации биометрии. Научно доказано, что ДНК и отпечатки пальцев не изменяются в течение жизни человека. Однако, если рассматривать внешность человека (форма скул, носа, подбородка, губ, разрез глаз и т.д.), то утверждать, что черты лица остаются неизменными в настоящее время будет не совсем правильным. Это утверждение обусловлено развитием современной пластической хирургии и косметологии, когда благодаря им стали возможны радикальные изменения в том числе и маркеров, по которым проводится идентификация личности. В связи с этим биометрия, которую невозможно изменить в течение жизни, наиболее достоверно позволит определить необходимое соответствие. При этом считаем целесообразным требовать уведомления от лица, скорректировавшее свою внешность, оператора биометрических персональных данных для актуализации идентификаторов.

4. Невозможность восстановления утраченных данных. Актуальность создания эффективной системы административно-правовой защиты биометрии обусловлена в главной степени этим специфическим признаком. Если произошла

---

<sup>1</sup> Рассолов И.М., Чубукова С.Г. Защита генетических данных при генетическом тестировании и генотерапевтическом лечении: информационно-правовые аспекты // Актуальные проблемы российского права. 2020. Т. 15, № 5(114). С. 69.

утечка ДНК, то процесс восстановления этого уникального физиологического кода невозможен, например, как процесс обновления взломанного пароля от какой-либо социальной сети. При этом геном может представлять особый интерес для «черного» рынка информации, так как в нем заключается не только информация о человеке, но и косвенная информация о состоянии его здоровья, о его близких родственниках. И конечно, способов изменения ДНК человека не существует, что делает невозможным восстановления его уникальности.

Таким образом, специальные признаки являются важным вектором при определении, относится та или иная физиологическая или поведенческая характеристика к биометрическим персональным данным человека.

Общая совокупность признаков биометрических персональных данных предназначена для формирования современного определения биометрии. Однако, в рамках нашего исследования установлено, что понятие «биометрические персональные данные», закрепленное в статье 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», не предполагает установление рамочного характера, и позволяет отнести к биометрии значительный перечень биологических и физиологических характеристик человека. На эту проблему указывали многие современные авторы: Н.И. Платонова<sup>1</sup>, А.В. Минбалеев<sup>2</sup>, С.В. Баженов, В.Е. Дивольд, А.А. Морозов<sup>3</sup> и др. К сожалению, в настоящее время этот вопрос остается открыт, и на законодательном уровне не принято решение о внесении изменений в определение биометрических персональных данных и установления их конкретного перечня.

С другой стороны, учитывая темпы развития отрасли правового регулирования биометрических персональных данных, данный перечень не может быть закрытым. Было бы допустимым законодательно зафиксировать установленные сегодня биометрические персональные данные, используемые для

---

<sup>1</sup> Платонова Н.И. Современные правовые подходы к пониманию биометрических данных. С. 22–26.

<sup>2</sup> Минбалеев А.В. Проблемы цифрового права: учебное пособие. Саратов, 2022. 233 с.

<sup>3</sup> Создание Концепции национальной системы биометрической идентификации личности / С.В. Баженов, В.Е. Дивольд, А.А. Морозов [и др.] // Труды Академии управления МВД России. 2020. № 2(54). С. 41–53.

аутентификации или идентификации. При этом необходимо данный перечень обновлять на постоянной основе с учетом возникновения новых способов обработки иных биометрических персональных данных.

Изучая правовые аспекты использования биометрии, можно отметить, что к законодательно защищенным данным рассматриваемой категории можно отнести геномную информацию, дактилоскопию, запись голоса человека, полученную с помощью звукозаписывающих устройств, и изображение лица человека, полученное с помощью фотовидеоустройств.

Рассмотрев понятия биометрических персональных данных, и их признаки, по нашему мнению, далее необходимо выделить виды биометрии и классифицировать их.

Довольно всесторонне к этому вопросу подошли Р.Н. Данелян и В.А. Яковлев-Чернышев<sup>1</sup>. Авторы выделили в отдельные группы биометрические персональные данные по 6 квалифицирующим признакам: критерию возобновимости, состоянию, наличию репродуктивной функции, содержанию информации, происхождению, цели использования.

В научной литературе можно встретить классификацию, содержащую три вида биометрических данных: физиологические, поведенческие и промежуточные<sup>2</sup>. Данной классификации придерживались Д.Р. Галиуллина и Н.И. Платонова. По нашему мнению, такой подход обладает универсальностью и с практической точки зрения весьма обоснован.

В Российской Федерации при классификации выделяют два вида систем биометрических данных:

– статические биометрические данные – уникальные признаки, полученные человеком от рождения (ДНК, отпечатки пальцев, геометрия руки, радужная оболочка глаза и иное);

---

<sup>1</sup> Данелян Р.Н., Яковлев-Чернышев В.А. Особенности правового регулирования биометрических персональных данных в Российской Федерации // Вестник Казанского юридического института МВД России. 2024. Т. 15, № 3(57). С. 30-31.

<sup>2</sup> Галиуллина Д.Р. Биометрические персональные данные // Документ. Архив. История. Современность. 2015. Т. 15. С. 265.

– динамические биометрические данные – характеристики, приобретенные со временем или способные меняться с возрастом или под внешним воздействием (динамика воспроизведения подписи, походка, динамика набора текста, голос и иное).

Такой позиции при классификации придерживаются как ученые (С.А. Баженов, В.Е. Дивольд, А.А. Морозов и другие<sup>1</sup>), так и Центральный Банк России<sup>2</sup>. Учеными отмечено, что если ранее наибольшее распространение получили статические биометрические персональные данные, то сегодня эффективность распознавания пользователя на основе динамических методов биометрической аутентификации достигает 92,14 %, что позволяет говорить о высоком потенциале применения данного метода<sup>3</sup>.

Таким образом, классификация биометрических персональных данных весьма многообразна. Однако при проведении исследования установлено, что данную классификацию необходимо дополнить еще одним типом классификации, который ранее не рассматривался, но важен в вопросе административно-правовой защиты биометрических персональных данных.

При утрате уникальности какого-либо из видов биометрии оценивая ущерб, необходимо учитывать возможность восстановления биометрической характеристики. На эту проблему обращал внимание В.Е. Дивольд. Он указывал, что хищение цифровых моделей биометрических профилей может повлечь серьезные последствия, лицо больше не сможет использовать скомпрометированные биометрические признаки<sup>4</sup>.

---

<sup>1</sup> Создание Концепции национальной системы биометрической идентификации личности / С.В. Баженов, В.Е. Дивольд, А.А. Морозов [и др.] // Труды Академии управления МВД России. 2020. № 2(54). С. 43.

<sup>2</sup> Обзор Международного рынка биометрических технологий и их применение в финансовом секторе / Официальный интернет-сайт. – URL: [https://cbr.ru/content/document/file/36012/rev\\_bio.pdf](https://cbr.ru/content/document/file/36012/rev_bio.pdf) (дата обращения: 26.06.2023).

<sup>3</sup> Исследование системы идентификации и подтверждения легитимности доступа на основе динамических методов биометрической аутентификации / М.М. Путято, А.С. Макарян, Ш.М. Чич, В.К. Маркова // Прикаспийский журнал: управление и высокие технологии. 2020. № 3(51). С. 92.

<sup>4</sup> Дивольд В.Е. Предпосылки создания национальной системы биометрической идентификации личности. С. 141.

В целях дальнейшего совершенствования правовой науки представляется целесообразным использовать классификацию биометрических персональных данных на основе принципа восстановления их уникальности. Данная классификация позволит систематизировать подходы к защите и восстановлению персональных данных, обеспечивая их конфиденциальность и целостность. В рамках данной типологии можно выделить следующие категории:

- 1) восполняемые;
- 2) невосполнимые.

К первой категории относятся биометрические персональные данные, которые при возможном посягательстве будут утрачены, но при соблюдении определенных условий могут приобрести вновь уникальность. Предположим, запись голоса. Если голос стал объектом мошеннических действий и не может быть больше использован лицом для идентификации, то вполне возможно с должной подготовкой изменить его главные характеристики, такие как тембр, высота голоса, интонация. В результате чего голос станет вновь уникальной характеристикой человека, по которой впоследствии может осуществляться идентификация или аутентификация. Бесспорно, среди этих данных чаще всего встречаются поведенческие характеристики человека – голос, походка, работа на клавиатуре и т.д. При этом процедура восстановления является трудозатратой, требует значительного количества времени.

Вторая категория характеризуется утратой уникальности биометрических персональных данных при совершении в отношении них мошеннических действий. Самый простой пример – ДНК. Если эти данные будут утрачены, то геномная информация не сможет никоим образом быть изменена в человеке и не будет представлять ценности для идентификации или аутентификации.

Исследуя эту классификацию невозможно не обратить внимание, что при утрате биометрических персональных данных необходимо по-разному квалифицировать действия правонарушителя и соответственно, учитывая к какому виду относятся биометрические персональные данные, применять необходимую санкцию.

Таким образом, следует признать, что вопрос о классификации биометрических данных, подлежащих правовой защите, на сегодняшний день является весьма актуальным. С развитием идентификации и аутентификации с помощью биометрических персональных данных увеличивается перечень таких данных, что существенно расширяет возможность их классификации.

Нами рассмотрены примеры классификации, представляющие интерес с правовой точки зрения, но этот перечень не является исчерпывающим. При более детальном изучении возможна классификация каждого в отдельности вида биометрии. Но для правовой науки и обоснования биометрических персональных данных как объекта правовой защиты приведенные классификации представляются наиболее исчерпывающими.

Следующее положение, требующее детального исследования, заключается в способе предоставления биометрических персональных данных. Таких способов существует два – обязательная и добровольная регистрация биометрических персональных данных.

Государственная политика в данной области направлена на применение «мягкой» силы. Это подтверждает официальная информация, размещенная на сайте Государственной Думы Федерального Собрания Российской Федерации, согласно которой «сдача биометрических персональных данных – абсолютно добровольный процесс <...> Принуждение к сдаче и дискриминация при оказании услуг будут наказываться»<sup>1</sup>.

Важно отметить, что данное утверждение не относится ко всем видам биометрии, а только к отдельным категориям биометрических персональных данных – образец голоса и изображение лица.

Данное положение закреплено частью 11 статьи 3 Федерального закона от 29 декабря 2022 г. № 572-ФЗ. Добровольность предоставления биометрических персональных данных выражается в предоставлении согласия физического лица на сбор, обработку и хранение его биометрии. При этом в вышеупомянутом

---

<sup>1</sup> Как государство защитит биометрические данные россиян / Официальный интернет-сайт [Электронный ресурс]. – URL: <http://duma.gov.ru/news/56087/> (дата обращения: 09.01.2024).

законе указывается перечень отношений, на которые он не распространяет свое действие, и в таких случаях регистрация становится обязательной.

Эти отношения возможно разделить на две группы. Особенность их заключается в цели, определяющей деятельность, в рамках которой будут получены биометрические персональные данные.

Первая группа предусматривает отношения, возникающие при осуществлении идентификации с использованием биометрических персональных данных физических лиц в определенных законодательно закрепленных целях. Указанные цели реализуются в ходе:

- оперативно-разыскной, контрразведывательной или разведывательной деятельности;
- обороны страны, обеспечения безопасности государства и охраны правопорядка, реализации внешней политики;
- функционирования государственной системы миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность;
- обеспечения санитарно-эпидемиологического благополучия.

Вторая группа отношений носит иной характер. Здесь государственная регистрация биометрических персональных данных не регламентируется Федеральным законом от 29 декабря 2022 г. № 572-ФЗ. В случае, если при проведении процедуры идентификации не используется автоматизированный метод верификации соответствия предоставленных биометрических данных физического лица данным, хранящимся в информационной системе государственного органа, органа местного самоуправления, Центрального банка Российской Федерации, организации, индивидуального предпринимателя или нотариуса, идентификация осуществляется с привлечением уполномоченного должностного лица<sup>1</sup>.

---

<sup>1</sup> Карпушина А.В. Вопросы правового регулирования при обязательной государственной регистрации биометрических персональных данных / XIII Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: материалы международной научно-практической конференции, Калининград, 20 декабря 2024 года. – Калининград, 2025. С. 31.

Такое разделение на группы применительно и к другим биометрическим характеристикам. Так, согласно ч. 2 ст. 11 Закона «О персональных данных» предусматривается ряд случаев, когда согласия субъекта не требуется, в частности в связи с осуществлением правосудия, проведением обязательной государственной дактилоскопической и геномной регистрации в Российской Федерации<sup>1</sup>.

Вопросы правового регулирования таких данных отражаются в отдельных нормативных правовых актах: Федеральные законы от 3 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» и от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации». Оба федеральных закона устанавливают одновременно добровольную и обязательную государственную регистрацию. И если добровольная регистрация – результат волеизъявления гражданина, то обязательная – это реализация целей, изложенных в первой группе отношений, а именно осуществление оперативно-разыскной деятельности и обеспечения безопасности государства и охраны правопорядка.

В вопросе добровольной и обязательной регистрации существует так называемая «серая зона». Указанные нормативные правовые акты устанавливают порядок получения только четырех категорий данных – образца голоса, изображения лица, дактилоскопических данных и геномной информации. Помимо приведенных биометрических характеристик, для идентификации используются и иные биометрические данные, не имеющие правовой защиты.

Возможным решением этой проблемы могло бы стать создание единого нормативного правового акта, в котором законодательно был бы закреплён перечень подлежащих защите биометрических персональных данных, порядок сбора, хранения и использования их, а также регламентирован порядок взаимодействия структур по получению доступа к сведениям.

---

<sup>1</sup> Каримов В.Х., Яценко С.В. Актуальные вопросы правового регулирования биометрической регистрации в России // Правда и закон. 2023. № 4(26). С. 29.

Рассмотрев признаки биометрических персональных данных, изучив порядок сбора, обработки и хранения данных, определив возможные классификации, считаем необходимым определить перечень биометрических персональных данных, подлежащих правовой защите.

Хочется подчеркнуть, что этот перечень носит открытый характер. Это обусловлено тем фактом, что в условиях активно развивающейся цифровизации растет список физиологических и поведенческих характеристик, с помощью которых могут быть проведены идентификация и аутентификация, и, соответственно, каждой характеристике биометрии будет требоваться правовая защита.

Сегодня на законодательном уровне обеспечена правовая защита четырех типов данных, относимых к биометрии:

- 1) изображение лица человека, полученное с помощью фотовидеоустройств<sup>1</sup>;
- 2) запись голоса человека, полученная с помощью звукозаписывающих устройств<sup>2</sup>;
- 3) геномная информация<sup>3</sup>;
- 4) дактилоскопическая информация<sup>4</sup>.

В мире для идентификации и аутентификации помимо приведенных характеристик широко используются иные биометрические данные, которые в России не имеют конкретного законодательного регулирования. Сюда можно отнести:

- 1) радужную оболочку глаз;

---

<sup>1</sup> Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства Российской Федерации. 2023. № 1 (часть I). Ст. 19.

<sup>2</sup> Там же.

<sup>3</sup> Федеральный закон от 03.12.2008 № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» // Собрание законодательства Российской Федерации. 2008. № 49. Ст. 5740.

<sup>4</sup> Федеральный закон от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации» // Собрание законодательства Российской Федерации. 1998. № 31. Ст. 3806.

- 2) индивидуальные особенности геометрии лица (геометрия черепа, костномышечный скелет и т.п.);
- 3) геометрию руки;
- 4) форму ушей (конфигурации и особенности ушных раковин);
- 5) рисунок вен;
- 6) распознавание эмоций;
- 7) термограмму лица (схему кровеносных сосудов кожи лица);
- 8) походку;
- 9) динамику набора текста и др.<sup>1</sup>

Возвращаясь к особенностям административно-правового регулирования защиты биометрических персональных данных, хочется отметить результаты анализа, проведенного в 2018 году Центробанком России, по использованию биометрических персональных данных. Так, в отчете указывалось, что в России для биометрической идентификации используются:

- 1) отпечатки пальцев (составляют более 50% всего объема рынка);
- 2) изображение лица (21,6%);
- 3) изображение радужной оболочки глаза (10,2%);
- 4) голос (4%);
- 5) рисунок вен (3%);
- 6) геометрия ладони, ДНК и иное (около 7%)<sup>2</sup>.

Приведенный перечень показывает, что биометрическая идентификация в России не ограничивается 4 биометрическими маркерами, имеющими индивидуальные нормы правового регулирования, а представляет собой «открытый список» возможных физиологических и поведенческих характеристик, используемых для установления личности.

---

<sup>1</sup> Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки: Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30 августа 2013 г. / Официальный интернет-сайт. – URL: <https://www.pd.rkn.gov.ru/press-service/subject1/news2729/> (дата обращения: 20.01.2023).

<sup>2</sup> Обзор Международного рынка биометрических технологий и их применение в финансовом секторе / Официальный интернет-сайт. – URL: <https://cbr.ru/> (дата обращения: 26.06.2023).

При этом статистические данные указывают на то, что особой популярностью пользуется дактилоскопическая информация, используемая в ряде стран для идентификации. Данный способ распознавания личности используется при пересечении границы, разблокировки технических устройств, позволяющих использовать в качестве ключа-доступа отпечаток папиллярных узоров. При этом дактилоскопическая информация обеспечивает высокую достоверность при сопоставлении маркеров.

Согласно приведенным данным использования биометрии, доля на запись голоса и изображение лица составила 25,6%, т.е. процент использования этих биометрических характеристик значителен, однако недостаточен. Принятый Федеральный закон от 29 декабря 2022 г. № 572-ФЗ популяризирует идентификацию и аутентификацию посредством изображения лица и записи голоса. Новые модели телефонов только вводят функцию фейс-ID, позволяющую разблокировать телефон с помощью изображения лица. Управление счетом в банке может осуществляться посредством управления голосом. Новшеством сегодня является оплата по изображению лица в супермаркетах. А совершенно недавно запущена тестовая программа – обслуживание клиентов в МФЦ без паспорта гражданина Российской Федерации, а по идентификации его изображения.

Биометрические персональные данные, приведенные выше, подлежат административно-правовой защите в Российской Федерации. Однако анализ статистических данных свидетельствует, что в практике также используются иные биометрические характеристики, не регулирующиеся действующим законодательством и, следовательно, не обеспеченные должной правовой защитой. Этот пробел необходимо устранить, чтобы исключить случаи нарушения прав граждан путем совершения правонарушений, связанных с этой категорией биометрических персональных данных.

Дополнительно хотелось бы обратить внимание на цели получения биометрических персональных данных. О.В. Белая и Ю.А. Кицай пришли к выводу, что «европейский законодатель делает акцент не на целях использования оператором соответствующих сведений о человеке, а на возможности применения такой

информации для установления личности субъекта при их специальной обработке»<sup>1</sup>. В российском же законодательстве в самом определении заложена цель получения, обработки и хранения биометрических персональных данных – идентификация, при этом отсутствует понятие аутентификации как цели. Хотя мы считаем, что целесообразным является учитывать и ее, так как несовершенство цифровых технологий может допускать искажение хранимых данных вследствие хакерских атак. Данная ситуация характерна для Федерального закона от 27 июля 2006 г. № 152-ФЗ, но урегулирована в Федеральном законе от 29 декабря 2022 г. № 572-ФЗ, где в качестве целей использования единой биометрической системы указаны обе категории.

Значимым аспектом является тот факт, что сведения хранятся не в натуральной форме, а как данные, полученные с использованием информационных технологий путем цифрового преобразования биометрических персональных данных. Такие данные принято называть идентификатор.

Полученные данные передаются в единую биометрическую систему. Однако же в единой биометрической системе хранится только две категории биометрических персональных данных:

- 1) изображение лица человека, полученное с помощью фотовидеоустройств;
- 2) запись голоса человека, полученная с помощью звукозаписывающих устройств<sup>2</sup>.

То есть разработанная система не аккумулирует в себе все виды биометрических характеристик, допустимых для идентификации физического лица. При этом существует еще несколько отдельных баз, обобщающих биометрию по отдельному признаку, например, Федеральная база данных геномной информации (ФБДГИ), в которой размещена геномная информация, полученная от лиц, осужденных и отбывающих наказание в виде лишения свободы за совершение

---

<sup>1</sup> Белая О.В., Кицай Ю.А. Биометрические данные как средство идентификации и аутентификации человека: российский и международный опыт // Право и практика. 2020. № 1. С. 86.

<sup>2</sup> Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства Российской Федерации. 2023. № 1 (часть I). Ст. 19.

преступлений; неустановленных лиц, биологический материал которых изъят в ходе производства следственных действий; лиц, подозреваемых в совершении преступлений, обвиняемых в совершении преступлений; близких родственников лиц, пропавших без вести, а также неопознанных трупов<sup>1</sup>. Из перечисленных типов геномной информации вся относится к обязательной геномной регистрации. А геномная информация, сданная добровольно, например, при проведении исследования на отцовство, учитывается в разных системах сбора и хранения ДНК.

Таким образом, на сегодняшний день в России нет единой национальной базы генетических данных. Рассматривая перспективы, представляется уместным создание единой базы. На эту проблему обращали внимание многие авторы. Например, Н.И. Долженко и Е.А. Купряшина отмечали, что помещение такой информации в соответствующие базы данных и формирование на их основе ДНК-профилей позволяет раскрывать преступления качественнее и быстрее<sup>2</sup>.

Информация, полученная при идентификации физического лица по отпечаткам пальцев (ладоней) рук, хранится в централизованной интегрированной автоматизированной дактилоскопической информационной системе Министерства внутренних дел Российской Федерации<sup>3</sup>.

Для иных биометрических характеристик базы данных носят локальный характер и создаются в большей части для реализации одной определенной цели. При этом Э.И. Лескина обращала внимание на тот факт, что защита персональных данных должна учитывать случаи, когда лицо может быть идентифицировано

---

<sup>1</sup> Федеральный закон от 03.12.2008 № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» // Собрание законодательства РФ. 2008. № 49. Ст. 5740.

<sup>2</sup> Долженко Н.И., Купряшина Е.А., Подмоков Н.С. Криминалистические генетические базы данных: отечественный и зарубежный опыт использования // Современный ученый. 2023. № 1. С. 261.

<sup>3</sup> Приказ МВД России от 19 июня 2018 г. № 384 «Об утверждении Порядка проведения идентификации личности человека по отпечаткам пальцев (ладоней) рук в режиме реального времени и Перечня категорий лиц, в отношении которых обязательная государственная дактилоскопическая регистрация не проводится в случае идентификации их личности в результате проверки по отпечаткам пальцев (ладоней) рук в режиме реального времени» [Электронный ресурс]. – URL: <https://mvd.consultant.ru/documents/1056542> (дата обращения: 09.01.2024).

вследствие объединения различных наборов данных, даже если сами по себе данные ни прямо, ни косвенно не идентифицируют физическое лицо<sup>1</sup>.

По нашему мнению, необходимо создание современной единой базы, объединяющей как биометрические характеристики, полученные как в результате обязательной государственной регистрации, так и добровольной. Это бесспорно приведет к совершенствованию современной системы сбора, обработки и хранения биометрических персональных данных, обеспечит высокий уровень безопасности полученных данных, приведет к обобщению маркеров, по которым производится идентификация, что позволит повысить раскрываемость преступлений и правонарушений посредством идентификации.

Предпосылки к созданию национальной системы биометрической идентификации личности ранее предпринимались. Так, в 2020 году авторским коллективом Омской академии МВД России был разработан проект Концепции национальной системы биометрической идентификации личности (далее – Концепция). С.А. Баженовым, В.Е. Дивольдом, А.А. Морозовым, Д.В. Поповым, Д.М. Сафроновым, А.В. Серовым. В проекте Концепции определяются сферы действия, цели, условия, принципы создания и функционирования, основные требования, структура, участники, этапы создания, требования к обеспечению информационной безопасности, механизмы и источники финансирования системы биометрической идентификации, а также оценка ожидаемого социально-экономического эффекта, возникающего в процессе создания<sup>2</sup>.

В настоящий момент реализация данного проекта не нашла своего отражения. Хотя безусловно, создание такой базы имело бы положительный эффект для общества, о чем в полном объеме изложено в части ожидаемого социально-экономического эффекта в проекте Концепции.

---

<sup>1</sup> Лескина Э.И. Доктринальные аспекты правовых режимов данных в условиях развития технологий больших данных // Журнал российского права. 2024. Т. 28, № 7. С. 133.

<sup>2</sup> Создание Концепции национальной системы биометрической идентификации личности / Баженов С.А. [и др.]. С. 48–52.

Таким образом, рассмотрение вопросов понимания биометрических персональных данных как объекта правовой защиты позволяет сделать следующие выводы:

1. Биометрические персональные данные прошли несколько ключевых этапов исторического развития: донаучный период, зарождение научного знания о биометрических характеристиках человека, период автоматизации идентификации, период развития биометрических персональных данных в условиях цифровизации общества. Выделение отдельных этапов основывается на оценке становления совокупности биометрических идентификаторов, а не отдельных ее видов, систематизации полученных данных и биометрической идентификации в условиях научно-технического прогресса. Современный этап характеризуется активным использованием при идентификации широкого перечня биометрических характеристик с использованием автоматизированных систем распознавания личности, в том числе и с помощью искусственного интеллекта.

2. В настоящее время перечень биометрических персональных данных, используемых для идентификации, постоянно увеличивается. Сегодня к биометрии относятся: ДНК, отпечатки пальцев, голос, изображение лица человека, полученное с помощью фотовидеоустройств, геометрия руки, радужная оболочка глаза, динамика воспроизведения подписи, походка, динамика набора текста и иное. Физиологические и поведенческие особенности человека признаются биометрическими персональными данными при их соответствии следующим признакам: идентификация проводится исключительно в отношении физических лиц; цель сбора – идентификация и аутентификация; фиксация данных осуществляется в специальных систематизированных базах. Именно эти признаки характеризуют биометрические персональные данные как юридическую категорию, которая отличает данные от технических, биологических и социологических областей знаний.

3. К числу особенностей (специальных признаков), обуславливающих необходимость защиты биометрических персональных данных, относятся уникальность, невозможность восстановления утраченных данных, высокий риск

необратимых последствий при утечке, этический аспект (соблюдение принципа неприкосновенности частной жизни). В связи с этим, правовое регулирование в области биометрических персональных данных требует установления для них специального правового режима с усиленными мерами защиты.

4. В настоящее время в Российской Федерации правовой защите подлежат лишь четыре вида биометрических персональных данных (изображение лица человека, полученное с помощью фотовидеоустройств; запись голоса человека, полученная с помощью звукозаписывающих устройств; геномная информация; дактилоскопическая информация), при этом в мировой практике для идентификации уже сегодня используется более 15 физиологических и поведенческих характеристик. Развитие автоматизированных систем создает предпосылки того, что в России также возможна идентификация личности по большому количеству биометрических персональных данных. В связи с чем необходимо принятие централизованного правового акта для того, чтобы исключить эпизодический фрагментированный характер правового регулирования биометрических персональных данных.

## **§ 2. Административно-правовое регулирование защиты биометрических персональных данных**

С.В. Запольский и В.Б. Исаков отмечали, что в настоящее время человечество находится в активной фазе очередной научно-технической революции, движущими факторами которой являются биотехнологии, информационные технологии и искусственный интеллект, и соответствующие процессы не обходят и сферу права<sup>1</sup>. Повсеместная информатизация и цифровизация являются закономерным процессом развития российского государства<sup>2</sup>.

---

<sup>1</sup> Запольский С.В., Исаков В.Б. Новые актуальные основания модернизации в сфере информационного права // Правовая информатика. 2023. № 1. С. 4.

<sup>2</sup> Дугенец А.С. Актуальные проблемы противодействия административным правонарушениям, совершаемым с использованием информационных технологий // Пробелы в российском законодательстве. 2024. Т. 17, № 4. С. 23.

Сегодня во всем мире обостряется проблема недостаточности нормативного правового регулирования и нормативного технического регулирования функционирования различных технологий, включая цифровые<sup>1</sup>.

Учитывая рост интереса к биометрической идентификации человека в условиях нарастающей цифровизации, необходимо перевести эту проблему с уровня нормативно-технической документации в правовую плоскость, законодательно закрепить повышенные требования к защите биометрических персональных данных<sup>2</sup>. Т.А. Полякова и И.С. Бойченко отмечали, что этот вопрос является социально значимым и волнующим общество<sup>3</sup>.

Особая роль в формировании данного института возлагается на административное право. Так, О.А. Дизер отмечал, что административное право располагает наиболее развитой и гибкой системой мер реагирования предупредительного, ограничительного, пресекающего, обеспечительного и наказательного характера, дифференцированной по силе, характеру и масштабам воздействия<sup>4</sup>.

Именно в рамках административного права исследуется правовой режим биометрических персональных данных, однако данная область находится «на стыке» двух отраслей права. Биометрия является также областью изучения учеными информационного права.

Э.И. Лескина определяет правовой режим персональных данных как порядок правового регулирования общественных отношений, складывающихся в процессе сбора, обработки, хранения, анализа и иных действий, совершаемых с персональными данными, выраженный в определенном сочетании юридических

---

<sup>1</sup> Правовое обеспечение суверенитета и кодификация информационного законодательства / Ю.М. Батулин, Т.А. Полякова, А.В. Минбалева [и др.]. М.: Институт государства и права РАН, 2024. С. 12.

<sup>2</sup> Гаврилова Ю.А. Конституционализация информационной безопасности в российском праве: проблема совершенствования теоретической модели // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2023. Т. 27, № 1. С. 112.

<sup>3</sup> Полякова Т.А., Бойченко И.С. Особенности взаимодействия и правового обеспечения информационной безопасности в единой биометрической системе в Российской Федерации. С. 28.

<sup>4</sup> Дизер О.А. Административно-правовая защита общественной нравственности: автореф. ... д-ра юрид. наук: 12.00.14. Омск, 2019. С. 5.

средств и направленный на создание модели желаемого общественного поведения в сфере оборота персональных данных<sup>1</sup>.

Важную роль в построении системы правового регулирования биометрических персональных данных играет опыт зарубежных стран. Данный вопрос весьма глубоко исследован С.С. Кузнецовым, А.Н. Мочаловым, М.С. Саликовым<sup>2</sup>. Авторы отмечали, что первая модель правового регулирования биометрической идентификации и обработки биометрических данных представлена Соединенными Штатами Америки (США). Специальных законов, регулирующих оборот биометрической информации, на федеральном уровне не существует. В региональной практике правового регулирования порядка обработки и защиты биометрических данных сформировалось два подхода: первый предполагает принятие отдельного нормативного правового акта, предметом которого являются исключительно биометрические данные (Иллинойс, Вашингтон, Техас), второй – разработку механизма защиты биометрической информации в рамках общего законодательства о защите персональных данных граждан штата (Калифорния, Нью-Йорк, Аризона, Луизиана, Орегон, Арканзас)<sup>3</sup>. В отличие от США, в Китае регулирование рассматриваемой сферы осуществляется централизованно, так же, как и в странах – членах Европейского союза, где хранение и использование биометрических данных регулируется Общим регламентом по защите персональных данных (General Data Protection Regulation, GDPR) и национальным законодательством, которое не должно противоречить Регламенту<sup>4</sup>.

---

<sup>1</sup> Лескина Э.И. Реформирование правового режима обезличенных данных с целью развития инноваций / Актуальные проблемы науки и практики: Гатчинские чтения – 2023: сборник научных трудов по материалам X Международной научно-практической конференции, Гатчина, 26 мая 2023 года. Гатчина, 2023. С. 40-43.

<sup>2</sup> Кузнецова С.С., Мочалов А.Н., Саликов М.С. Биометрическая идентификация в Интернете: тенденции правового регулирования в России и за рубежом // Вестник Томского государственного университета. 2022. № 476. С. 259.

<sup>3</sup> Государственное регулирование Интернета и права человека / Саликов М.С. [и др.]. Екатеринбург, 2022. С. 98.

<sup>4</sup> Фатхи В.И. К вопросу о правовом регулировании порядка использования биометрических персональных данных: международный опыт // Философия права. 2023. № 4(107). С. 97.

Опираясь на зарубежный опыт, Е.А. Свиридова выделила модели правового регулирования биометрических персональных данных. Она отмечает, что первая модель построена на принципе установления общего правового режима для персональных и биометрических данных (биологические особенности гражданина включаются в общее понятие персональных данных) (Япония, Китай); вторая модель распространяет правила об обработке персональных данных на обработку биометрических данных лишь при условии наличия цели идентификации их субъекта (страны ЕС); третья модель предполагает обособление биометрических данных в особую категорию персональных данных с особым правовым режимом независимо от цели обработки данных<sup>1</sup>.

Е.А. Свиридова придерживается мнения, что Россия принадлежит к первой модели правового регулирования биометрических персональных данных. Данной позиции придерживается Е.А. Мальгинов, который отмечал, что в России биометрические данные не имеют отдельной системы правового регулирования и входят в правовой институт «персональные данные», который является в целом межотраслевым<sup>2</sup>.

М.С. Саликов, С.Э. Несмеянова, Н.Е. Колобаева, С.С. Кузнецова и А.Н. Мочалов придерживаются мнения, что законодательное регулирование оборота биометрической информации в России в большей степени развивается в рамках модели, характерной для азиатских стран.

«Азиатская» модель правового регулирования, вероятно, в большей степени (в сравнении с двумя другими моделями) способствует максимально широкому внедрению технологий биометрической идентификации в онлайн-среду. За счет применения «сквозных» технологий, допускающих биометрическую

---

<sup>1</sup> Свиридова Е.А. Защита персональных данных в условиях цифровой трансформации общественных отношений // Проблемы экономики и юридической практики. 2022. Т. 18. № 6. С. 57.

<sup>2</sup> Мальгинов Е.А. Сбор и обработка биометрических данных топ-менеджеров и предпринимателей: возможно ли защитить корпоративный интерес? // Право и экономика. 2023. № 5(423). С. 13.

идентификацию личности как в Интернете, так и в физической реальности, стирается граница между виртуальным и физическим мирами<sup>1</sup>.

В настоящее время система административно-правового регулирования защиты биометрических персональных данных в России находится на стадии своего активного формирования. Не случайно, О.А. Дизер отмечал, что цифровое пространство нуждается в правовом регулировании, поскольку им охватываются все сферы общественной жизни<sup>2</sup>.

В начале нашего исследования защита биометрических персональных данных в правовом поле обуславливалась общими нормами всей совокупности персональных данных, однако за три года ситуация изменилась. Как справедливо отмечали В.В. Архипов и В.Б. Наумов, права человека, с одной стороны, сами эволюционируют под воздействием всеобщей цифровой трансформации, с другой стороны, права и свободы человека образуют содержание пределов вмешательства цифровых технологий в частную жизнь лица<sup>3</sup>.

Результаты анализа в рамках нашего исследования системы административно-правового регулирования защиты биометрических персональных данных показывают, что государство при разработке государственной политики в данной области идет по пути создания баланса между соблюдением положений, приведенных В.В. Архиповым и В.Б. Наумовым.

Система административно-правового регулирования защиты биометрических персональных данных в Российской Федерации представляет собой комплекс (иерархическую систему) нормативных правовых актов, регулирующих обеспечение технической, социальной и правовой безопасности при осуществлении сбора, обработки и хранения физиологических и поведенческих характеристик человека в целях идентификации и/или аутентификации.

---

<sup>1</sup> Государственное регулирование Интернета и права человека / Саликов М.С. [и др.]. Екатеринбург, 2022. С. 119.

<sup>2</sup> Дизер О.А. Административно-правовая охрана общественного порядка и общественной безопасности в условиях формирования цифрового пространства // Вестник Уфимского юридического института МВД России. 2020. № 3(89). С. 70.

<sup>3</sup> Архипов В.В., Наумов В.Б. Теоретико-правовые вопросы охраны прав человека при использовании биометрических данных системами искусственного интеллекта: европейский опыт // Вестник Удмуртского университета. Серия Экономика и право. 2022. Т. 32, № 1. С. 109.

Глобальное развитие систем распознавания личности, основанных на получении и анализе биометрических персональных данных, имеет широкие перспективы<sup>1</sup>. По нашему мнению, при исследовании системы административно-правового регулирования защиты биометрических персональных данных важно выделить цели регулирования. Среди них обозначим следующие:

- 1) обеспечение конституционного права на неприкосновенность частной жизни (ст. 23 Конституции РФ)<sup>2</sup>;
- 2) гарантия защиты биометрических персональных данных от неправомерного доступа, использования, распространения и уничтожения<sup>3</sup>;
- 3) установление правовых оснований и порядка обработки биометрических данных<sup>4</sup>;
- 4) создание условий для безопасного и эффективного использования биометрических технологий (в системах безопасности, идентификации, предоставлении госуслуг и т.д.)<sup>5</sup>;
- 5) предотвращение злоупотреблений и дискриминации на основе биометрических характеристик<sup>6</sup>.

Таким образом, цели административно-правового регулирования защиты биометрических персональных данных представляют собой большой потенциал для законодательных органов в исследуемой области. Принцип верховенства права и приоритета конституции и законов в системе нормативных актов призван

---

<sup>1</sup> Полуянова Е.В., Ковалев С.Д. Нормативное регулирование использования биометрических персональных данных в Российской Федерации // Вестник Томского института повышения квалификации работников ФСИН России. 2020. № 3(5). С. 50.

<sup>2</sup> Кутейников Д.Л., Ижаев О.А., Лебедев В.А., Зенин С.С. Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности // Lex russica. 2022. Т. 75. № 2. С. 123.

<sup>3</sup> Сухостат В.В., Васильева И.Н. Основы информационной безопасности. СПб.: Санкт-Петербургский государственный экономический университет, 2019. С. 51.

<sup>4</sup> Затолокин А.А., В.В. Стрельцов Административно-правовые аспекты государственного регулирования обработки биометрических персональных данных // Общество и право. 2023. № 1(83). С. 79.

<sup>5</sup> Карцан И.Н. Биометрические данные: новые возможности и риски. Современные инновации, системы и технологии // Modern Innovations, Systems and Technologies. 2023. № 3(3). С. 204.

<sup>6</sup> Старанцова Е.В. Современные методы биометрической идентификации // Международный журнал информационных технологий и энергоэффективности. 2024. Т. 9. № 1(39). С. 45.

отражать ценность и высокую социальную роль права в обществе<sup>1</sup>. Главная задача – разработка основ действующего правового регулирования с учетом этических аспектов, чтобы защитить приватность, свободу и равенство всех людей.

В России система правового регулирования биометрических персональных данных сформирована из нормативных правовых актов различных законодательных уровней и представлена следующим образом:

1. Конституция Российской Федерации.
2. Федеральные законы Российской Федерации (6 основных нормативных правовых актов).
3. Постановления Правительства Российской Федерации (17 основных нормативных правовых актов, из них приняты в период 2022-2025 гг. – 12).
4. Приказы Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (более 10 нормативных правовых актов).
5. Указания и Положения, разъяснения Банка России (более 5 основных нормативных правовых актов).
6. Нормативные правовые акты правоохранительных органов.
7. Нормативные правовые акты уполномоченного органа по защите прав субъектов биометрических персональных данных (Роскомнадзор).

Исходя из приведенного перечня, можно сделать вывод, что сегодня принята значительная совокупность нормативных правовых актов, регулирующих вопросы обеспечения защиты биометрических персональных данных. Система основывается на положениях Конституции Российской Федерации.

В тексте Конституции Российской Федерации нет прямого упоминания о биометрии человека. Однако же статья 2 Конституции Российской Федерации гарантирует соблюдение и защиту прав и свобод человека и гражданина, что, в том числе, включает в себя и административно-правовую защиту биометрических персональных данных.

---

<sup>1</sup> Тихомиров Ю.А. Систематика в праве в условиях глобальной нестабильности // Журнал российского права. 2022. Т. 26, № 5. С. 15.

Конституция РФ также устанавливает, что каждый человек имеет право на охрану своей личной жизни, личную и семейную тайну (ст. 23), а сбор сведений о частной жизни лица без его согласия недопустим (п. 1 ст. 24)<sup>1</sup>. Вся система правового регулирования обращения биометрии выстраивается строго в соответствии с этой нормой, соблюдая принцип верховенства Конституции Российской Федерации.

Однако необходимо отметить, что у ученых в условиях развития современных государственных систем безопасности возникают вопросы о соблюдении баланса между интересами государства и соблюдением прав человека.

На данную проблему указывали Д.Л. Кутейников, О.А. Ижаев, Л.В. Алексеевич и С.С. Зенин. Они отмечали, что, несмотря на то, что в ч. 3 ст. 55 Конституции РФ предусмотрена возможность в отдельных случаях ограничения прав и свобод федеральным законом, при формулировании конкретной процедуры необходимо избежать умаления прав человека на основе использования принципа пропорциональности, сам факт введения в эксплуатацию подобных систем для обеспечения безопасности не отменяет необходимости соблюдения прав человека<sup>2</sup>. Данная проблема весьма актуальна с учетом того, что в обществе существуют опасения тотального контроля со стороны государства, и, как следствие, это является одной из самых болезненных и значимых причин неприятия и противодействия использованию биометрии<sup>3</sup>.

При этом отметим, что в России используется такой показатель, как количество пользователей сервисом биометрической идентификации,

---

<sup>1</sup> Васильев Г.С. Человеческий биоматериал как объект права // Правоведение. 2018. № 2(337). С. 347.

<sup>2</sup> Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности / Д.Л. Кутейников, О.А. Ижаев, Л.В. Алексеевич, С.С. Зенин // Lex Russica (Русский закон). 2022. Т. 75, № 2(183). С. 128.

<sup>3</sup> Михайлов М.А., Кокодей Т.А. Организационные, правовые и этические аспекты получения, хранения и использования биометрической информации в целях всеобщей регистрации населения // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2022. Т. 8 (74), № 4. С. 346.

утвержденный приказом Минцифры России от 31 марта 2023 г. № 333<sup>1</sup>. Исходя из приведенных Росстатом данных, указанный показатель отразил не просто прирост, а увеличение количества пользователей сервисом биометрической идентификации в геометрической прогрессии. Так, если в марте 2022 года он составлял 243 296 человек, то в ноябре 2024 года – 75 731 039<sup>2</sup>. Этот показатель динамичный, он может показывать как резкое увеличение, так и значительный спад. На это влияет ряд факторов, например, возможность запретить гражданами использование биометрических персональных данных в случае отсутствия необходимости (если это не противоречит действующему законодательству), истечение срока, на который предоставлялись данные и прочее. При этом, не смотря на опасения общества, указанный показатель отражает, что значительная часть населения нашей страны, а также иностранные граждане используют биометрические персональные данные для идентификации. Это указывает на эффективность современной системы административно-правовой защиты биометрических персональных данных и возрастающее доверие граждан к использованию биометрии в качестве идентификатора.

Таким образом, важным условием конституционного регулирования в области защиты биометрических персональных данных является соблюдение баланса между интересами государства и граждан. Безусловно, биометрия открывает новые возможности для обеспечения безопасности государства и граждан, однако необходимо учитывать, что популяризация использования биометрических характеристик делает их привлекательными для мошенников и увеличивает риски утраты уникальности предоставленных данных.

---

<sup>1</sup> Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 31 марта 2023 г. № 333 «Об утверждении Методики расчета показателя «Доля массовых и государственных сервисов, обеспеченных возможностью их получения с использованием цифрового профиля гражданина» федерального проекта «Цифровое государственное управление» национальной программы «Цифровая экономика Российской Федерации» и внесении изменений в некоторые приказы Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации об утверждении методик расчета показателей федеральных проектов национальной программы «Цифровая экономика Российской Федерации» [Электронный ресурс]. – URL: <https://base.garant.ru/407410608/>.

<sup>2</sup> Количество пользователей сервисом биометрической идентификации [Электронный ресурс]. – URL: <https://www.fedstat.ru/indicator/62445> (дата обращения: 11.10.2024).

Исследуя опыт международного правового регулирования биометрических персональных данных, необходимо отметить нормативный правовой акт – Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR). Ценность этого нормативного акта заключается в определении термина «биометрические данные», отличного в некоторых аспектах от российского законодательства, что может служить ориентиром в формировании современного понятия биометрических персональных данных в отечественном праве. Также регламентом устанавливается специальный режим обработки биометрических данных, который предполагает общий запрет на совершение соответствующих действий с учетом тех исключительных случаев, когда такая обработка становится возможной<sup>1</sup>. В России, как мы уже отмечали ранее, правовое регулирование биометрии остается в рамках действующего законодательства о персональных данных.

Но если раньше для России данный международный акт был частью правовой системы, то в настоящий момент с 16 марта 2022 года нормативные правовые акты ЕС считаются утратившими действие в отношении РФ в связи с прекращением членства РФ в Совете Европы. Данное положение закреплено Федеральным законом от 28 февраля 2023 г. № 43-ФЗ «О прекращении действия в отношении Российской Федерации международных договоров Совета Европы»<sup>2</sup>.

Таким образом, в настоящее время международные акты, в которых регламентируется порядок обращения с биометрическими персональными данными, могут выступать в качестве международного опыта, а не как нормативный правовой акт, подлежащий исполнению.

---

<sup>1</sup> Государственное регулирование Интернета и права человека / Саликов М.С. [и др.]. Екатеринбург: УМЦ УПИ, 2022. С. 113.

<sup>2</sup> Федеральный закон от 28 февраля 2023 г. № 43-ФЗ «О прекращении действия в отношении Российской Федерации международных договоров Совета Европы» // Собрание законодательства Российской Федерации. 2023. № 10. Ст. 1566.

Сегодня в российском законодательстве основу правового регулирования биометрических персональных данных представляет Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». В нем впервые было законодательно закреплено понятие биометрических персональных данных, правила сбора, обработки и хранения биометрии. Также закреплено положение, согласно которому регистрация биометрии является добровольной процедурой, кроме случаев, установленных действующим законодательством.

Важным аспектом является тот факт, что данным законом не устанавливаются характеристики человека, которые относятся к биометрии, в результате чего данный нормативный акт требует дополнений. Эта проблема решалась созданием отдельных законодательных актов, которые регулируют вопросы административно-правовой защиты биометрические характеристики в отдельности в зависимости от целей получения таких данных. В первом параграфе нашего исследования мы приводили аргументы, которые предполагают внесение изменений в действующее определение биометрических персональных данных. Именно данное решение станет своевременным для построения дальнейшей системы административно-правового регулирования биометрических персональных данных.

Таким образом, на основании изученных в рамках исследования определений, предложенных учеными и используемых в зарубежном опыте, под биометрическими персональными данными следует понимать сведения, относящиеся к физиологическим и поведенческим характеристикам физического лица, полученные в целях идентификации и (или) аутентификации в результате специальной технической обработки, в том числе с использованием автоматизированных систем (приложение 1).

Самым ранним, предшествующим Федеральному закону «О персональных данных», стал Федеральный закон от 25 июля 1998 г. № 128-ФЗ

«О государственной дактилоскопической регистрации в Российской Федерации»<sup>1</sup>. Современная редакция Федерального закона при определении понятия дактилоскопической информации законодательно закрепляет то обстоятельство, что дактилоскопия является биометрическими персональными данными<sup>2</sup>.

Отдельно Федеральным законом от 3 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации»<sup>3</sup> регулируются правоотношения, связанные с еще одной категорией биометрических персональных данных – ДНК. Аналогично с Федеральным законом «О государственной дактилоскопической регистрации», признание ДНК биометрическими персональными данными произошло значительно позднее принятия нормативного правового акта<sup>4</sup>. При этом в научном сообществе вопрос, является ли биометрией геномная информация, долгое время оставался дискуссионным. Лишь в 2023 году законодатель внес изменение в действующие правовые нормы и заложил в понятие геномной информации то, что она представляет собой биометрические персональные данные.

При исследовании двух приведенных нормативных правовых актов нельзя не отметить тот факт, что для них свойственна схожесть многих правовых норм. Оба федеральных закона регулируют сбор и обработку биометрических персональных данных в целях обеспечения государственной безопасности и правопорядка. Регистрация ведется в рамках государственных информационных систем, находящихся в подведомственности правоохранительных органов

---

<sup>1</sup> Федеральный закон от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации» // Собрание законодательства Российской Федерации. 1998. № 31. Ст. 3806.

<sup>2</sup> Федеральный закон от 7 мая 2013 г. № 99-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» и Федерального закона «О персональных данных» // Собрание законодательства Российской Федерации. 2013. № 19. Ст. 2326.

<sup>3</sup> Федеральный закон от 03.12.2008 № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» // Собрание законодательства Российской Федерации. 2008. № 49. Ст. 5740.

<sup>4</sup> Федеральный закон от 6 февраля 2023 г. № 8-ФЗ «О внесении изменений в Федеральный закон «О государственной геномной регистрации в Российской Федерации» и отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. 2023. № 6. Ст. 915.

(преимущественно МВД России, ФСБ России и Следственного комитета России). Оба закона устанавливают обязательную регистрацию для строго определенной категорий лиц, однако предусматривают возможность добровольной регистрации для иных граждан.

Однако, несмотря на схожесть целей и общих принципов, законы имеют принципиальные различия, обусловленные спецификой биометрических характеристик. Во-первых, отличаются результатами идентификации: дактилоскопия позволяет установить личность при ЧС, проверках по отпечаткам с места преступления; геномная информация – идентификация по биологическим следам при раскрытии тяжких и особо тяжких преступлений, идентификация останков, установление родства<sup>1</sup>. Во-вторых, дактилоскопия применяется значительно шире – обязательна для многих категорий граждан (сотрудники силовых структур, госслужащие, мигранты и др.), геномная идентификация применяется в основном для лиц, вовлеченных в уголовный процесс по тяжким/особо тяжким преступлениям (подозреваемые, обвиняемые, осужденные), неопознанные трупы, пропавшие без вести. В-третьих, для дактилоскопической регистрации характерна относительно простая и дешевая процедура снятия отпечатков<sup>2</sup>, а для ДНК – это сложный и дорогостоящий лабораторный анализ. В-четвертых, дактилоскопия не дает информации о человеке, кроме факта его идентификации, в свою очередь геномная информация потенциально связана с уникальными биологическими характеристиками<sup>3</sup>.

Таким образом, законы схожи в своих фундаментальных целях (безопасность, идентификация, раскрытие преступлений) и организационно-правовых принципах (государственные системы, обязательность для категорий, защита данных). Однако они принципиально различаются по характеру чувствительности данных, следовательно, и глубине вмешательства в частную

<sup>1</sup> Эволюция подходов к ДНК-идентификации личности / Д.А. Чемерис, А.М. Сагитов, Ф.Г. Аминев [и др.] // Биомика. 2018. Т. 10, № 1. С. 99.

<sup>2</sup> Пинчук П.В. Дактилоскопия: исторические аспекты и роль в решении идентификационных задач на современном этапе ее развития // Проблемы экспертизы в медицине. 2001. Т. 1, № 2. С. 46.

<sup>3</sup> Кириленко В.С., Хомутова Е.А. Проблемы и перспективы применения ДНК в системе уголовного правосудия // Вестник Алтайской академии экономики и права. 2021. № 11-1. С. 127.

жизнь, широте охвата субъектов, сфере преимущественного применения и связанным с этим уровнем требований к защите и потенциальным рискам.

В связи с этим появляются вопросы, возможно ли создание единого правового акта, который будет регулировать сбор, обработку и хранение таких биометрических персональных данных, как геномная и дактилоскопическая информация, и требуется ли вследствие этого создание единой базы биометрических персональных данных.

Эти вопросы исследовали многие ученые. Позицию по созданию единого правового акта по вопросам правового регулирования биометрических персональных данных озвучивали авторы В.Х. Каримов и С.В. Яценко. Они предлагали создать отдельный законодательный акт, который мог бы определить биометрические характеристики, а также их носителей, подлежащих обязательной и добровольной регистрации, процедуру проведения, права и обязанности участников<sup>1</sup>. Безусловно, данная позиция заслуживает внимания. Создание единого нормативного правового акта позволит исключить дублирование положений, свойственных для используемых правовых инструментариев геномной и дактилоскопической информации. Однако создание такого нормативного правового акта не может регламентировать только два вида биометрии – геномной и дактилоскопической информации, оставляя в стороне закрепленных законодательно как биометрию запись голоса и изображение лица. И если два проанализированных выше нормативных правовых акта имеют очень близкую правовую идентичность, то оба они отличны от закона, регламентирующего сбор, обработку и хранение записей голоса и изображений лиц.

Нормативный правовой акт, регулирующий вопросы обеспечения административно-правовой защиты записи голоса и изображения лица, был принят относительно недавно. Федеральным законом от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных» предусмотрена главная

---

<sup>1</sup> Каримов В.Х., Яценко С.В. Актуальные вопросы правового регулирования биометрической регистрации в России // Правда и закон. 2023. № 4(26). С. 26.

гарантия, которая обсуждалась наиболее бурно при разработке проекта данного нормативного правового акта. В рассмотрении законопроекта участвовали экспертное сообщество, представители Русской православной церкви и Совета по правам человека<sup>1</sup>. Указанный законодательный акт был принят уже с внесенными в него поправками и замечаниями общественности. Как отметил Председатель Государственной Думы Федерального Собрания Российской Федерации Вячеслав Володин, такой консенсус позволил избежать создания «цифрового ГУЛАГа».

Принятие Федерального закона от 29 декабря 2022 г. № 572-ФЗ решило ряд проблем правового характера, назревших в обществе. Результатом стало:

- выделение государственных систем по сбору, обработке и хранению биометрии в отдельные биометрические системы (системы биометрических данных для правоохранительных органов) и Единую биометрическую систему (ЕБС) (для удаленной идентификации для гражданских правоотношений);
- получение обязательного письменного согласия (электронное с УКЭП/НЭП) на обработку биометрии в единой биометрической системе;
- обязанность предоставлять оператором понятную информацию о целях, рисках, условиях обработки;
- конкретизация положения, что к биометрическим персональным данным относится изображение лица и голосовой образ;
- требование от операторов единой биометрической системы строгого соблюдения безопасности при работе с данными;
- конкретизация требований к защите биометрических персональных данных при их обработке и передаче в единой биометрической системе;
- формирование более четких полномочий Роскомнадзора по контролю за соблюдением мер безопасности биометрических персональных данных в единой биометрической системе.

Федеральным законом от 29 декабря 2022 г. № 572-ФЗ разработан перечень ограничений. Так, запрещается:

---

<sup>1</sup> Как государство защитит биометрические данные россиян [Электронный ресурс]. – URL: <http://duma.gov.ru/news/56087/> (дата обращения: 09.01.2024).

- обуславливать предоставление услуги/товара/работы обязательным согласием на обработку биометрии в ЕБС. Следует уточнить, что несогласие физического лица на прохождение идентификации и (или) аутентификации с использованием его биометрических персональных данных не может служить основанием для отказа в оказании ему государственных услуг (ч. 13 ст. 3 Закона № 572-ФЗ)<sup>1</sup>.

- применять неправомерное воздействие или обман для получения согласия.

Однако при наличии положительных результатов от принятия рассматриваемого нормативного правового акта он не лишен недостатков. К ним можно отнести:

- формальное отношение операторов, ответственных за сбор, обработку и хранение биометрических персональных данных, к правовой категории «добровольность предоставления биометрических характеристик»;

- недостаточное разъяснение некоторых норм правового регулирования защиты биометрических персональных данных;

- проблемы совместимости с отраслевыми законами (сохраняется риск коллизий и двойного регулирования);

- закон фокусируется в основном на положениях по защите единой биометрической системы;

- не исключаются риски безопасности единой биометрической системы (фундаментальные риски централизованной утечки или взлома огромной базы биометрических данных граждан остаются крайне высокими. В 2023 году Роскомнадзор зафиксировал 168 утечек персональных данных, в результате которых в открытый доступ попало более 300 млн записей. Согласно данным Роскомнадзора, в 2023 году суды рассмотрели 87 составленных ведомством протоколов по факту утечек персональных данных и назначили штрафы на общую сумму более 4,6 млн рублей<sup>2</sup>).

<sup>1</sup> Полуянова Е.В. Отдельные вопросы функционирования и правового регулирования Единой биометрической системы Российской Федерации // Аграрное и земельное право. 2025. № 3. С. 107.

<sup>2</sup> В 2023 году в сеть утекло более 300 млн записей о россиянах [Электронный ресурс]. – URL: <https://tass.ru/obschestvo/19693845> (дата обращения: 21.03.2024).

Таким образом, принятие Федерального закона от 29 декабря 2022 г. № 572-ФЗ – это новый этап в правовом регулировании использования биометрии, прежде всего в рамках единой биометрической системы. Данный нормативный правовой акт существенно повысил защищенность биометрических персональных данных, но не устранил все системные риски и вызовы, связанные с обработкой биометрических данных в Российской Федерации. Его эффективность будет зависеть от правоприменительной практики, дальнейшего развития подзаконных актов и технологий защиты данных.

Дополнительно отметим, что взаимодействие публичных органов власти и иных организаций с единой биометрической системой в целях осуществления идентификации и (или) аутентификации на сегодняшний день строго регламентировано законом, что в некоторой степени решило проблему негативного отношения общества к процессу цифровизации, результатом которой стало расширение области использования биометрических персональных данных. Усиление роли государства бесспорно вызвало одобрение со стороны юристов-позитивистов. Но принятые нормы удовлетворяют и цивилистов, так как законом не запрещается использование биометрических персональных данных в области гражданских прав.

Как отмечала Т.А. Полякова, для России исключительно важно решение научных вопросов по улучшению информационного законодательства в условиях цифровизации информационного общества и цифровой трансформации. Необходимы новые научно-теоретические подходы, которые позволят создать рациональную систему правовых механизмов, рационализировать не только информационные процессы, но и правовые отношения в рамках информационного пространства. Это обеспечит взаимодействие информационного законодательства с различными отраслями права<sup>1</sup>.

В связи с этим необходимо продолжать работу по обеспечению максимальной безопасности биометрических персональных данных, в том числе и

---

<sup>1</sup> Полякова Т.А., Троян Н.А. Актуальные проблемы систематизации законодательства России под влиянием цифровых технологий в период цифровой трансформации // Вестник университета имени О.Е. Кутафина (МГЮА). 2023. № 2(102). С. 30.

по вопросам административно-правового регулирования. Правовое регулирование в области защиты биометрических персональных данных на сегодняшний день является перспективным. В сфере правового регулирования защиты биометрических данных существуют пробелы – это использование так называемой серой зоны биометрии (рисунков вен, размеров рук и т.д.) негосударственными субъектами. Нужна конкретизация их правового статуса, то есть возможность их обработки частными организациями<sup>1</sup>. Принятым законодательным актам предстоит еще внедрение в практическую деятельность, что конечно может показать проблемы, которые возможно еще предстоит законодательно урегулировать, чтобы максимально исключить возможность правонарушений, связанных со сбором, обработкой и хранением биометрии.

В рамках проведенного нами исследования установлен признак, по которому можно классифицировать существующие нормативные правовые акты в области защиты биометрических персональных данных. Имеющиеся нормативные акты можно условно разделить на две группы:

1. Нормативные правовые акты, регулирующие порядок сбора, обработки и хранения биометрических персональных данных для идентификации личности в целях осуществления гражданских общественных действий. К ним можно отнести Федеральный закон «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных»<sup>2</sup>. Данным нормативным правовым актом регулируются отношения, которые предусматривают порядок сбора, обработки и хранения двух видов биометрии – фотоизображения и записи голоса. Чаще всего эти маркеры используются для идентификации в гражданской сфере – оказание услуг посредством удаленного подтверждения личности, использование цифровых возможностей банковских продуктов и другое.

---

<sup>1</sup> Бурлака С.Н., Бельдина О.Г. Защита биометрических персональных данных: проблемы правового регулирования // Право и государство: теория и практика. 2023. № 10(226). С. 279.

<sup>2</sup> Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства Российской Федерации. 2023. № 1 (часть I). Ст. 19.

2. Нормативные правовые акты, регулирующие порядок сбора, обработки и хранения отдельных видов биометрических персональных данных органами публичной власти в целях обеспечения правопорядка и государственной безопасности. Можно выделить сразу два нормативных правовых акта, используемых органами публичной власти – Федеральные законы «О государственной геномной регистрации в Российской Федерации»<sup>1</sup> и «О государственной дактилоскопической регистрации в Российской Федерации»<sup>2</sup>. Целью данных нормативных актов является урегулирование правовых вопросов по идентификации личности с использованием отдельных биометрических персональных данных. В соответствии с действующим законодательством, государственная регистрация геномной и дактилоскопической информации носит обязательный характер, также предусмотрена возможность прохождения добровольной процедуры регистрации данных.

Таким образом, совокупность нормативных правовых актов, регулирующих правоотношения в сфере биометрических персональных данных, объединяет общая цель – идентификация личности. Данные акты различаются по назначению идентификации, которая может быть направлена на реализацию государственных функций в рамках гражданских правоотношений или обеспечение безопасности<sup>3</sup>.

Приведенные в рамках нашего исследования нормативные правовые акты не представляют собой исчерпывающий перечень, в связи с чем их дополняют иные нормотворческие акты. Например, Федеральный закон от 29 декабря 2022 г. № 572-ФЗ предусматривает дополнение Постановлением Правительства РФ

---

<sup>1</sup> Федеральный закон от 3 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» // Собрание законодательства Российской Федерации. 2008. № 49. Ст. 5740.

<sup>2</sup> Федеральный закон от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации» // Собрание законодательства Российской Федерации. 1998. № 31. Ст. 3806.

<sup>3</sup> Карпушина А.В. Правовые аспекты использования биометрических персональных данных в борьбе с терроризмом // Проблемы правоохранительной деятельности. 2025. № 3(61). С. 55.

от 15 июня 2022 г. № 1067<sup>1</sup> случаев и сроков использования биометрических персональных данных, размещенных физическими лицами в единой биометрической системе с использованием мобильного приложения единой биометрической системы, Постановлением Правительства РФ от 22 мая 2023 г. № 810 утверждаются Правила аккредитации организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, оснований ее приостановления и прекращения<sup>2</sup> и т.д.

Важным аспектом нашего исследования является разграничение субъектов правоотношений в области административно-правовой защиты биометрических персональных данных. Процессы идентификации субъектов различных отношений появились и стали актуальными очень давно, с момента возникновения общественных отношений, требующих юридически значимого определения состава их участников<sup>3</sup>. К субъектам правоотношений в области административно-правовой защиты биометрических персональных данных относятся следующие участники:

1. Операторы биометрических систем. Важным субъектом в правовом механизме административно-правовой защиты биометрических персональных данных является участник правоотношений, обладающий специализированными полномочиями и компетенцией в данной области, - оператор биометрических систем. Понятие оператора персональных данных содержится в Федеральном законе от 27 июля 2006 г. № 152-ФЗ, также в Федеральном законе от 29 декабря 2022 г. № 572-ФЗ выделяется оператор регионального сегмента единой

---

<sup>1</sup> Постановление Правительства РФ от 15 июня 2022 г. № 1067 «О случаях и сроках использования биометрических персональных данных, размещенных физическими лицами в единой биометрической системе с использованием мобильного приложения единой биометрической системы» // Собрание законодательства Российской Федерации. 2022. № 25. Ст. 4337.

<sup>2</sup> Постановление Правительства РФ от 22 мая 2023 г. № 810 «Об утверждении Правил аккредитации организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, оснований ее приостановления и прекращения и признании утратившим силу постановления Правительства Российской Федерации от 20 октября 2021 г. № 1799» // Собрание законодательства Российской Федерации. 2023. № 22. Ст. 3945.

<sup>3</sup> Кузнецов П.У. «Цифровая трансформация государственного управления как этап развития информатизации в России» / Четвертые Бачиловские чтения: материалы международной научно-практической конференции. М.: Саратов: Амирит, 2022. С. 20.

биометрической системы. Оператором является государственный орган, муниципальный орган, юридическое или физическое лицо, на которого возложены полномочия по обработке персональных, в том числе биометрических, данных. Кроме того, поправки в законодательстве направлены на повышение защиты персональных данных россиян и усиление требований к операторам обработки таких данных<sup>1</sup>. Операторы несут основную ответственность за соблюдение требований.

2. Субъекты биометрических персональных данных. Особенностью данной категории является тот факт, что субъектом биометрических персональных данных являются только физические лица, к которым относятся обрабатываемые биометрические характеристики.

3. Уполномоченный орган по защите прав субъектов биометрических персональных данных. Ключевым контролирующим органом, осуществляющим надзор и контроль за соблюдением законодательства о персональных данных, включая биометрические, является Роскомнадзор.

4. Правительство РФ и органы публичной власти, которые устанавливают правила, требования, порядки обработки биометрических данных в рамках своих компетенций (Минцифры, ФСБ России, ФСТЭК России и т.д.).

Объектом административно-правового регулирования защиты в данной области являются биометрические персональные данные.

Дополнительно отметим, что в условиях современной правовой регламентации и технологических инноваций вопрос обработки биометрических персональных данных приобретает особую актуальность, где согласие субъекта на обработку данных является ключевым элементом, обеспечивающим соблюдение принципа добровольности.

Необходимо также учитывать ситуации, когда получение согласия не является обязательным. К таким ситуациям относятся процессуальные действия, такие, как допрос или следственный эксперимент. В этих случаях следователь

---

<sup>1</sup> Равоян Р.А. Правовое регулирование защиты персональных и биометрических данных в условиях цифровизации // Юридическая наука. 2023. № 5. С. 84.

имеет право на сбор образцов голоса или отпечатков пальцев при условии предварительного уведомления субъекта о цели и основаниях таких действий. Уведомление должно быть зафиксировано в соответствующем протоколе, подлежащем подписанию субъектом.

Однако в отношении случаев, когда правоохранительные органы осуществляют запрос на доступ к биометрическим данным через Единую биометрическую систему (ЕБС), существует правовая неопределенность. Хотя запрос на предоставление доступа адресуется субъекту, последний не всегда осведомлен о целях и основаниях такого запроса. В связи с этим предлагается рассмотреть возможность внедрения автоматизированной системы уведомлений, интегрированной с кабинетом Госуслуг, которая будет информировать физическое лицо о любых действиях, связанных с его биометрическими данными.

При этом необходимо отметить, что современная система законодательства строится по принципу, отмеченному Ю.А. Тихомировым. Исследуя право в условиях социальных вызовов, Ю.А. Тихомиров указывал, что гибкая эволюция систематики в праве позволяет преодолевать рассогласованность институтов, споры и противоречия между субъектами права и юридические коллизии<sup>1</sup>.

Таким образом, комплексное решение данных вопросов требует дальнейшего совершенствования нормативно-правовой базы и внедрения эффективных механизмов защиты прав и свобод субъектов биометрических данных.

Подводя итог исследования в рамках данного параграфа, отметим следующее.

1. Биометрические персональные данные как юридическая категория – это сведения, относящиеся к физиологическим и поведенческим характеристикам физического лица, полученные в целях идентификации и (или) аутентификации в результате специальной технической обработки.

Система административно-правового регулирования защиты биометрических персональных данных в Российской Федерации представляет

---

<sup>1</sup> Тихомиров Ю.А. Систематика в праве в условиях глобальной нестабильности // Журнал российского права. 2022. Т. 26, № 5. С. 16.

собой комплекс нормативных правовых актов, направленный на обеспечение технической, социальной и правовой безопасности при проведении сбора, обработки и хранения физиологических и поведенческих характеристик человека в целях идентификации и/или аутентификации.

2. К целям административно-правового регулирования защиты биометрических персональных данных относятся: обеспечение права на неприкосновенность частной жизни; гарантия защиты биометрических персональных данных от неправомерного доступа, использования, распространения и уничтожения; установление правовых оснований и порядка обработки биометрических данных; создание условий для безопасного и эффективного использования биометрических технологий; предотвращение злоупотреблений и дискриминации на основе биометрических характеристик.

Важным условием конституционного регулирования в области защиты биометрических персональных данных является соблюдение баланса между правами граждан и интересами государства в рамках реализации функции обеспечения безопасности.

3. Имеющиеся нормативные правовые акты, регулирующие вопросы сбора, обработки и хранения биометрических персональных данных в зависимости от целей идентификации субъекта биометрических характеристик можно условно разделить на две группы:

А. Нормативные правовые акты, регулирующие порядок сбора, обработки и хранения биометрических персональных данных для идентификации личности в целях осуществления гражданских общественных действий.

В. Нормативные правовые акты, регулирующие порядок сбора, обработки и хранения отдельных видов биометрических персональных данных органами публичной власти в целях обеспечения правопорядка и государственной безопасности.

4. Стремительное развитие биометрических персональных данных в сфере общественных отношений делает необходимыми перманентные процессы по совершенствованию законодательства в исследуемой области. Полагаем, что

применительно к биометрическим персональным данным необходимо создание соответствующего правового режима, при котором государство должно выступать гарантом по реализации прав граждан на конфиденциальность биометрических характеристик.

### **§ 3. Особенности административной ответственности за правонарушения, связанные с обработкой биометрических персональных данных**

Быстрое развитие информационных технологий, использование различных электронных устройств, доступ в Интернет сделали уязвимыми не только собственность, но и личные данные<sup>1</sup>.

Не случайно Президент Российской Федерации В.В. Путин отмечал, что один из безусловных приоритетов работы правоохранительных органов – это борьба с преступлениями с использованием информационных технологий<sup>2</sup>.

Как отмечено Роскомнадзором, сравнительный анализ тематик поступивших в 2024 году обращений показывает активность граждан в части реализации ими законодательно закрепленных прав в сфере защиты персональных данных. Всего в 2024 году в Роскомнадзор поступило 76 811 обращений по указанной тематике (на 7,3% больше, чем в 2023 году), из них 68 748 – с жалобами на неправомерное использование их персональных данных (на 7,4% больше, чем в 2023 году). Количество обращений по защите прав субъектов персональных данных неуклонно растет<sup>3</sup>.

Сегодня особое внимание уделяется правилам обработки персональных данных, в том числе биометрических, правовому обеспечению безбарьерного

---

<sup>1</sup> Запорожец С.А., Крайнова Н.А. К вопросу о противодействии киберпреступности в условиях новой геополитической реальности // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2023. Т. 9 (75), № 3. С. 448.

<sup>2</sup> Расширенное заседание коллегии МВД [Электронный ресурс]. – URL: <http://www.kremlin.ru/events/president/transcripts/deliberations/> (дата обращения: 11.04.2023).

<sup>3</sup> Итоги работы с обращениями граждан в Роскомнадзоре в 2024 году [Электронный ресурс]. – URL: <https://rkn.gov.ru/treatments/p436/> (дата обращения: 25.05.2025).

использования новых цифровых технологий с учетом специфики технологического взаимодействия в цифровых отношениях, конечно, при условии защиты прав и законных интересов субъектов и владельцев данных<sup>1</sup>.

По мнению И.Е. Михеевой, в целях совершенствования правового обеспечения сохранности биометрических данных граждан необходимо усилить ответственность лиц, которые занимаются их сбором, обработкой и хранением<sup>2</sup>.

При проведении опроса в рамках исследования анкетированные придерживались мнения, что наиболее правильно лиц, виновных в утрате биометрических персональных данных, привлекать к административной ответственности (57% опрошенных). Другие виды ответственности как оптимальные указывались реже – дисциплинарная (12%), гражданская (11%), уголовная (20%).

Понятие административного правонарушения закреплено в статье 2.1 КоАП РФ. Так, административным правонарушением признается противоправное, виновное действие (бездействие) физического или юридического лица, за которое КоАП РФ или законами субъектов Российской Федерации об административных правонарушениях установлена административная ответственность<sup>3</sup>.

В свою очередь, административная ответственность – это вид юридической ответственности, которая выражается в назначении органом или должностным лицом либо судьей, наделенным соответствующими полномочиями, административного наказания лицу, совершившему правонарушение<sup>4</sup>. Данное определение представляет собой классический вариант исследуемого определения в административном праве.

О.А. Кожевников вводил понятие административной ответственности как вида юридической ответственности, предусмотренного нормами

---

<sup>1</sup> Вайпан В.А. Источники цифрового права // Вестник арбитражной практики. 2024. № 1(110). С. 14.

<sup>2</sup> Михеева И.Е. Отдельные правовые аспекты биометрической идентификации в банковской сфере // Lex Genetica. 2025. Т. 4, № 1. С. 34.

<sup>3</sup> Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства Российской Федерации. 2002. № 1 (часть I). Ст. 1.

<sup>4</sup> Административное право: учебник / под ред. Л.Л. Попова, М.С. Студеникиной. – 3-е изд., перераб. и доп. М.: Норма: Инфра-М, 2025. С. 39.

административного права, наступающего за совершение виновным лицом административного правонарушения, применяемого уполномоченными органами и должностными лицами в виде административных наказаний с обязательным соблюдением нормативно установленных процедур<sup>1</sup>. Данное определение обращает наше внимание на соблюдение прав субъекта при проведении процедуры привлечения его к административной ответственности.

И.В. Тимошенко дает иное определение административной ответственности. Он указывает, что административная ответственность – это вид государственного принуждения, реализуемого в предусмотренной законом процессуальной форме и отражающего специфическое правовое состояние лица, при котором оно претерпевает неблагоприятные последствия морального, личного, имущественного или организационного характера в результате государственного осуждения совершенного им административного правонарушения<sup>2</sup>. Такая позиция имеет смещение правового акцента на субъект административного правонарушения полностью и указывает на последствия совершения им противоправного действия.

С объективной стороны административная ответственность воспринимается как специфический вид правоохранительной деятельности, включающий совокупность действий компетентных органов (должностных лиц), отражающих реакцию государства на административное правонарушение; действий, имеющих негативные последствия для правонарушителя в виде административного наказания<sup>3</sup>.

Исследовав понятия административной ответственности, отметим, что для данной дефиниции является характерным государственное принуждение, с помощью которого наказывается неправомерное поведение правонарушителя,

---

<sup>1</sup> Кожевников О.А. К вопросу о понятии и признаках административной ответственности // Вестник Уральского юридического института МВД России. 2018. № 1. С. 18.

<sup>2</sup> Тимошенко И.В. Понятие административной ответственности // Северо-Кавказский юридический вестник. 2009. № 2. С. 79.

<sup>3</sup> Волков П.А. Современный подход к определению понятия административной ответственности // Известия Российского государственного педагогического университета имени А.И. Герцена. 2008. № 82-1. С. 94.

влекущего для него неблагоприятные моральные и материальные последствия в виде применяемого к нему наказания.

Административно-правовое регулирование защиты биометрических персональных данных – динамично развивающаяся область. Председатель Государственной Думы Федерального Собрания Российской Федерации В.В. Володин отмечал, что следующим шагом после принятия Федерального закона от 29 декабря 2022 г. № 572-ФЗ станет введение уголовной и административной ответственности за принудительный сбор и утечку биометрических данных<sup>1</sup>.

И действительно, в мае 2023 года с инициативой о введении административной ответственности в части за незаконное размещение биометрических персональных данных выступили Вячеслав Володин и руководители всех фракций Государственной Думы Российской Федерации. В результате в 2023 году были внесены поправки в Кодекс Российской Федерации об административных правонарушениях Российской Федерации, которые законодательно урегулировали вопросы привлечения к административной ответственности за нарушение требований в области размещения биометрических персональных данных.

Особенность административно-правовой защиты биометрических персональных данных заключается в необходимости реализации одновременно правовых, технических, организационных и информационных мер. В связи с чем административная ответственность в области защиты биометрических персональных данных устанавливается за правонарушения, совершаемые за противоправное, виновное действие (бездействие) при реализации указанных мер.

В соответствии с действующим законодательством в Российской Федерации административная ответственность установлена за:

- 1) невыполнение требований по защите персональных данных;
- 2) неисполнение обязанностей при взаимодействии с гражданином – субъектом персональных данных;

---

<sup>1</sup> Принят законопроект об ответственности за нарушения при использовании биометрических данных [Электронный ресурс]. – URL: <http://duma.gov.ru/news/> (дата обращения: 29.02.2024).

- 3) нарушение правил обработки персональных данных;
- 4) нарушение требований к размещению и обработке биометрических персональных данных в ЕБС (других информсистемах, обеспечивающих аутентификацию на основе таких данных);
- 5) неисполнение обязанностей при взаимодействии с Роскомнадзором.

Исходя из приведенного перечня, можно сделать вывод, что особенность административной ответственности в области защиты биометрических персональных данных заключается в выделении составов административных правонарушений по четырем категориям:

правонарушения, выделенные в общей совокупности персональных данных (статья 13.11 КоАП РФ);

правонарушения в сфере обработки биометрии в единой биометрической системе (статья 13.11.3 КоАП РФ);

правонарушения, связанные с неисполнением требований органа публичной власти, уполномоченного в области обеспечения безопасности биометрических персональных данных (статья 13.46 КоАП РФ);

иные правонарушения, связанные со сбором, обработкой и хранением биометрических персональных данных (часть 2.1 статьи 5.63 КоАП РФ).

Важно отметить, что в зависимости от источника, устанавливающего состав административного правонарушения в области защиты биометрических персональных данных, выделяют две группы:

- административные правонарушения, предусмотренные в КоАП РФ;
- административные правонарушения, предусмотренные законами субъектов РФ.

Каждое правонарушение предполагает наличие закрепленного состава административного правонарушения в КоАП РФ. Б.В. Россинский и Ю.Н. Стариков указывали, что наличие состава административного правонарушения в том или ином деянии служит единственным основанием наступления административной ответственности за его совершение. Под составом административного правонарушения следует понимать установленную правом

совокупность признаков, при наличии которых конкретное деяние становится административным правонарушением<sup>1</sup>.

К элементам состава административного правонарушения относятся: объект, объективная сторона, субъект, субъективная сторона<sup>2</sup>.

Объектом административного правонарушения являются общественные отношения, за посягательство на которые установлена административная ответственность<sup>3</sup>.

В теории административного права объекты посягательств административных правонарушений традиционно подразделяются на четыре группы: общий, родовой, видовой и непосредственный<sup>4</sup>. Как отмечено П.И. Кононовым и В.Я. Кикотем, такое деление имеет не только теоретическое, но и практическое значение, так как оно позволяет правоприменителю осуществлять процесс квалификации административных правонарушений, то есть отнесение противоправного деяния к конкретной статье Особенной части КоАП РФ либо статье закона субъекта Российской Федерации, устанавливающего административную ответственность.

Общий объект – это все общественные отношения, за посягательство на которые установлена административная ответственность<sup>5</sup>. Общим объектом административных правонарушений в сфере защиты биометрических персональных данных является установленный государством порядок управления в области обеспечения информационной безопасности, защиты конфиденциальной информации и конституционных прав граждан на

---

<sup>1</sup> Россинский Б.В., Старилов Ю.Н. Административное право: учебник. - 6-е изд., пересмотр. М.: Норма: Инфра-М, 2020. С. 429.

<sup>2</sup> Россинский Б.В. Административное право и административная ответственность: курс лекций. – 2-е изд., перераб. М.: Норма: Инфра-М, 2025. С. 258.

<sup>3</sup> Керимова С.Н., Раджабова М.М. Понятие и основные черты административного правонарушения как основания административной ответственности // Вестник Дагестанского государственного университета. Серия 3: Общественные науки. 2016. Т. 31, № 4. С. 80.

<sup>4</sup> Административное право России: учебник для студентов вузов, обучающихся по специальности 030501 «Юриспруденция» / под ред. П.И. Кононова, В.Я. Кикотя, И.Ш. Киясханова. – 3-е изд., перераб. и доп. М.: ЮНИТИ-ДАНА: Закон и право, 2015. С. 293.

<sup>5</sup> Фиалковская И.Д. Состав административного правонарушения: первичные и вторичные признаки // Законность и правопорядок. 2018. № 3(19). С. 30.

неприкосновенность частной жизни. В условиях цифровизации идентификация человека по биометрическим характеристикам становится настолько популярной, что проникает в значительную часть сфер общественных отношений. Накопленный массив данных уже сегодня позволяет говорить о создании цифрового двойника. Цифровой двойник – это специально спроектированная виртуальная модель человека, созданная на основе его реальных (объективно существующих) физиологических и биологических данных, включающих комплекс характеристик, моделирующих физические параметры, поведенческие аспекты и биометрические данные<sup>1</sup>. При этом, несмотря на развитие общественных отношений, связанных с использованием биометрии, основной ее правовой ценностью является конфиденциальность. Биометрия – это особо чувствительные персональные данные, утечка и расшифровка которых могут привести к значительным негативным последствиям<sup>2</sup>.

В качестве родового объекта выступают общественные отношения, объединенные КоАП РФ в главы (например, административные правонарушения, посягающие на права граждан)<sup>3</sup>. Родовой объект административных правонарушений в области защиты биометрических персональных данных в российском законодательстве – это общественные отношения в сфере охраны и защиты информации (информационной безопасности) и персональных данных, а также установленного порядка управления. Этот родовой объект конкретизируется в главе 13 КоАП РФ – «Административные правонарушения в области связи и информации». Однако, учитывая особенности популяризации биометрических персональных данных, можно утверждать, что данной главой невозможно предусмотреть весь перечень правонарушений. Уже сегодня введены отдельные составы в главе 14 «Административные правонарушения в области

---

<sup>1</sup> Тархов С.В., Тархова Л.М., Назарова Ю.Р. Цифровые двойники человека и личности в организационных системах // Современные наукоемкие технологии. 2025. № 3. С. 48.

<sup>2</sup> Гуртовая К.А., Окунева А.Г. Актуальные проблемы безопасности хранения персональных данных клиентов // Вестник Самарского государственного экономического университета. 2025. № 1(243). С. 107.

<sup>3</sup> Административное право Российской Федерации: учебник для вузов / Ю.И. Мигачев, Л.Л. Попов, С.В. Тихомиров. – 7-е изд., перераб. и доп. М.: Юрайт, 2025. – 474 с. – URL: <https://urait.ru/bcode/580351/p.176> (дата обращения: 31.03.2025).

предпринимательской деятельности и деятельности саморегулируемых организаций» (статья 14.8 КоАП РФ) и в главе «Административные правонарушения, посягающие на права граждан» (часть 2.1 статьи 5.63 КоАП РФ).

Непосредственный объект – конкретное общественное отношение в административно-правовой сфере, на которое посягает определенное административное правонарушение<sup>1</sup>. Непосредственный объект административного правонарушения в области защиты биометрических персональных данных – это те конкретные общественные отношения и охраняемые законом ценности, которым причиняется вред или создается угроза причинения вреда именно данным правонарушением, связанным с обработкой биометрических данных.

Таким образом, объектом административного правонарушения в области защиты биометрических персональных данных является установленный государством порядок в сфере информации и связи, обеспечивающий реализацию конституционных прав граждан на неприкосновенность частной жизни и защиту персональных данных, а также конкретные общественные отношения, гарантирующие соблюдение специального правового режима обработки, конфиденциальности и безопасности уникальных биометрических характеристик человека. Нарушение именно этого порядка и этих отношений образует состав административного правонарушения.

Объективная сторона административного правонарушения – внешнее проявление административного правонарушения, выражающееся в действии или бездействии, нарушающем установленные правовыми нормами правила<sup>2</sup>.

Объективная сторона административного правонарушения обладает рядом признаков. Они подразделяются на общие и факультативные. Б.В. Россинский и Ю.Н. Стариков отмечали, что время, место, способ, характер совершения деяния, его повторность, неоднократность, злостность, систематичность являются

<sup>1</sup> См.: Административное право в схемах: учебник и практикум для вузов / под ред. А.И. Стахова, П.И. Кононова. – 4-е изд., перераб. и доп. М.: Юрайт, 2025. 501 с. – URL: <https://urait.ru/bcode/560835/p.292> (дата обращения: 31.03.2025).

<sup>2</sup> См.: Административное право в схемах: учебник и практикум для вузов. – URL: <https://urait.ru/bcode/560835/p.292> (дата обращения: 31.03.2025).

факультативными признаками состава административного правонарушения, т.е. необязательными. В отличие от них противоправное действие (бездействие), наступившие вредные последствия и причинно-следственная связь между деянием и наступившими в результате него вредными последствиями являются обязательными признаками объективной стороны состава административного правонарушения<sup>1</sup>.

Таким образом, административные правонарушения в области биометрических персональных данных в КоАП РФ выражаются как в действии, так и в бездействии. Перечень действий, направленных на утрату биометрическими персональными данными своей уникальности, с ростом возможностей технологий, развития искусственного интеллекта значительно увеличивается. Однако, на современном этапе административно-правового регулирования ответственности за правонарушения, связанные с биометрией, приняты поправки только в статьи 13.11 и 13.11.3 КоАП РФ в отношении:

- нарушения порядка обработки биометрических данных;
- непринятия мер по обеспечению их безопасности;
- обработки данных без аккредитации.

В статье 13.11.3 КоАП РФ предусматривается самостоятельная административная ответственность за нарушение требований в области размещения биометрических персональных данных граждан в единой биометрической системе<sup>2</sup>.

При этом в отношении биометрических персональных данных совершаются специфические неправомерные действия, характерные только для данной категории данных:

- создание дипфейков с использованием биометрических персональных данных;
- спуфинг в области биометрических персональных данных.

---

<sup>1</sup> См.: Россинский Б.В., Старилов Ю.Н. Административное право: учебник. - 6-е изд., пересмотр. М.: Норма: ИНФРА-М, 2020. 640 с. – URL: <https://znanium.com/catalog/product/> (дата обращения: 07.02.2025).

<sup>2</sup> Усиливается защита персональных биометрических данных граждан [Электронный ресурс]. – URL: <http://duma.gov.ru/news/58432/> (дата обращения: 27.12.2023).

В последние годы широкое распространение получили технологии изготовления поддельных фото и видео, которые, используя методику компьютерного синтеза изображения, основанную на искусственном интеллекте, переносят черты лица с изображения человека на целевое фото (видеозапись) с высокой степенью правдоподобия<sup>1</sup>. В.Б. Наумов, рассматривая институт идентификации, отмечал, что новым вызовом станет возможность подделки видеоизображений в реальном режиме времени, когда ни системы, ни люди не смогут без специального аппаратно-программного обеспечения различать, что является подлинным, что – «сгенерированным» и, чаще всего, с незаконными или недобросовестными целями<sup>2</sup>.

Одним из наиболее обсуждаемых видов биометрических персональных данных, который все чаще подвергается неправомерным действиям посредством использования искусственного интеллекта, является запись голоса. Не случайно директор по информационным технологиям New York Life Билл Кэссиди отмечал: «Людям всегда поступали мошеннические звонки. Но способность ИИ имитировать реальный голос человека, дающего указания что-то сделать, – это совершенно новые риски»<sup>3</sup>.

Правонарушения, связанные с утечкой записей голоса, стали настолько распространены, что в современном мире появился новый термин, обозначающий ложную биометрическую характеристику, полученную посредством использования нейросети, – «дипфейк».

Директор центра противодействия мошенничеству компании «Информзащита» П. Коваленко отмечал, что злоумышленники стали чаще покупать записи голосов и готовы платить за них от 300 до 5 тыс. рублей<sup>4</sup>.

---

<sup>1</sup> Добробаба М.Б. Дипфейки как угроза правам человека // Lex Russica (Русский закон). 2022. Т. 75, № 11(192). С. 113.

<sup>2</sup> Наумов В.Б. Институт идентификации в информационном праве: дис. ... д-ра юрид. наук: 12.00.13 / Наумов Виктор Борисович. Москва, 2020. С. 81.

<sup>3</sup> Мошенники стали в семь раз чаще использовать дипфейки в секторе финансовых технологий [Электронный ресурс]. – URL: <https://ai.gov.ru/mediacenter/> (дата обращения: 23.05.2025).

<sup>4</sup> Одинаковы с лица: в России выросло число атак с применением дипфейков [Электронный ресурс]. – URL: <https://iz.ru/1773345/oksana-belkina/odinakovy-s-lica-v-rossii-vyroslo-cislo-atak-s-primeneniem-dipfeikov> (дата обращения: 22.10.2024).

За три месяца 2025 года в России был выявлен 61 уникальный дипфейк и 2,3 тыс. копий, что в 2,6 раза превышает весь объем дипфейков, зафиксированный в 2023 году<sup>1</sup>.

К сожалению, не смотря на статистику, демонстрирующую рост правонарушений, совершенных указанным способом (в 2024 году число атак выросло на 13% – до 5,7 тыс. случаев<sup>2</sup>), данный термин не является юридическим и не закреплен законодательно.

Правовая оценка создания и распространения deerfake-технологий в рамках российского законодательства весьма затруднительна<sup>3</sup>. Прецеденты с утратой конфиденциальности биометрической характеристики и использования ее в целях совершения неправомерных действий уже имеют свою судебную практику.

В частности, как один из ярких примеров можно привести рассмотрение в открытом судебном заседании Савеловского районного суда административного дела № 2а-975/2024<sup>4</sup>.

В рамках заседания рассматривалось административное исковое заявление прокурора в интересах неопределенного круга лиц (заинтересованные лица – Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Центральному федеральному округу, Департамента информационных технологий) о признании информации, размещенной в сети Интернет, запрещенной к распространению в Российской Федерации.

В обоснование заявленных требований истец указал, что по обращению Департамента информационных технологий адрес по факту незаконной продажи

---

<sup>1</sup> Дипфейк шагает по планете. С чем связан рост числа сообщений, сгенерированных ИИ [Электронный ресурс]. – URL: <https://rg.ru/2025/04/08/dipfejk-shagaet-po-planete.html> (дата обращения: 03.05.2025).

<sup>2</sup> Одинаковы с лица: в России выросло число атак с применением дипфейков [Электронный ресурс]. – URL: <https://iz.ru/1773345/oksana-belkina/odinakovy-s-lica-v-rossii-vyroslo-cislo-atak-s-primeneniem-dipfeikov> (дата обращения: 22.10.2024).

<sup>3</sup> См.: Искусственный интеллект в юридической деятельности: учебник для вузов / под ред. С.Е. Чаннова. М.: Юрайт, 2025. 131 с. – URL: <https://urait.ru/bcode/581673> (дата обращения: 30.06.2025).

<sup>4</sup> Информация по делу № 02а-0975/2024 [Электронный ресурс]. – URL: <https://mosgorsud.ru/rs/savyolovskij/services/cases/kas/details/ad530ee1-f10b-11ee-b51f-5fe397bc9869> (дата обращения: 05.03.2025).

информации, хранящейся в ГИС «ЕЦХД», проведена проверка, в ходе которой выявлен сайт, на котором неопределенному кругу лиц предлагаются услуги о продаже информации из ЕЦХД, а также услуги по пробитию информации по всем службам (МВД, ФМС, ФНС, ГИБДД, ПФР, Росреестра, ЗАГС). На указанном сайте за плату предоставляется информация о персональных данных граждан, об их банковских счетах, движении денежных средств юридических лиц, выписки из Росреестра, сведения о пассажирах поездов и самолетов, сведения об имуществе граждан, информация, хранящаяся в ГИС «ЕЦХД», биометрия, а также иные сведения, которыми располагают банковские организации и органы государственной власти. Доступ к информации, размещенной на указанном сайте, является свободным, ознакомиться с содержанием и копировать ее может любой пользователь сети Интернет. Достоверные сведения о владельцах сайтов или доменных именах получить не представляется возможным, поскольку в российском сегменте сети Интернет сведения о лицах, указанных в качестве владельцев доменных имен, отсутствуют. Нахождение в открытом доступе в сети Интернет подобной информации нарушает права неопределенного круга лиц, противоречит целям и задачам действующего законодательства.

Пунктом 4 статьи 29 и пунктом 3 статьи 55 Конституции Российской Федерации предусмотрено, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Данное право может быть ограничено федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Размещаемая в ЕЦХД информация является информацией для специального использования и не подлежит распространению третьим лицам, в том числе продаже. При этом отсутствует подтверждение достоверности предлагаемой к продаже на указанном ресурсе информации.

Согласно пункту 1 статьи 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», персональные данные – любая информация,

относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных запрещено (ст. 7 Федерального закона «О персональных данных»).

Полномочия по созданию, формированию и ведению Единого реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов отнесены к компетенции Роскомнадзора в соответствии с п.5.1.7 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 16.03.2009 № 228.

Сайт по указанному адресу находится в открытом доступе неограниченному кругу лиц. Нахождение указанных информационных материалов в сети Интернет в свободном доступе может способствовать совершению противоправных действий.

Поскольку размещенная информация противоречит целям и задачам действующего законодательства, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено, суд находит требования прокурора в интересах неопределенного круга лиц о признании указанной информации запрещенной к распространению в Российской Федерации, обоснованными и подлежащими удовлетворению.

Так как указанная информация запрещена к распространению в Российской Федерации, то сведения об этом сайте подлежат включению Управлением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по ЦФО в Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено.

В силу части 4 статьи 265.5 КАС РФ решение суда об удовлетворении административного искового заявления о признании информации запрещенной подлежало немедленному исполнению.

На основании изложенного и руководствуясь ст. 175-180 КАС РФ, суд решил: административный иск прокурора в интересах неопределенного круга лиц о признании информации, размещенной в сети Интернет, запрещенной к распространению в Российской Федерации, удовлетворить.

Таким образом, государством принимаются меры правового регулирования по пресечению неправомерных действия и восстановлению прав граждан в области информационной безопасности. В рамках правового регулирования проводится мониторинг и анализ угроз информационной безопасности, а также осуществляется правоприменительная практика, направленная на обеспечение соблюдения законодательства в данной сфере.

Однако необходимо отметить, что кроме правовых мер, применяются и технические меры. Наиболее ярким является пример, связанный применением специальных мер технического характера по противодействию мошенническим целям, осуществляемым с помощью записи голоса. Так, в 2022 году Главным радиочастотным центром (ГРЧЦ), курируемым Роскомнадзором, введена в эксплуатацию единая платформа верификации телефонных вызовов (ЕПВВ) «Антифрод»<sup>1</sup>. Принцип работы «Антифрода»: информация о всех голосовых вызовах поступает в единую систему, а оператор связи в автоматическом режиме запрашивает и получает данные об активности номера. Если система подтверждает, что вызов реальный и номер не подменный, то устанавливается безопасное соединение. Если такого подтверждения нет, решение о его отклонении принимает оператор связи<sup>2</sup>.

Создание таких систем – один из способов защитить данные от утечки. Однако, есть не менее важный фактор, который влияет на данную область

---

<sup>1</sup> Роскомнадзор запустил платформу для борьбы с телефонным мошенничеством [Электронный ресурс]. – URL: <https://digital.gov.ru/ru/events/> (дата обращения: 13.02.2024).

<sup>2</sup> Официальное сообщение Роскомнадзора (О функционировании системы «Антифрод») [Электронный ресурс]. – URL: <https://cmu.gov.ru/ru/news/2023/11/27/> (дата обращения: 13.12.2023).

правонарушений – коммерциализация персональных данных, в том числе и биометрии.

Таким образом, дипфейк становится весьма распространенной проблемой при обеспечении защиты биометрических персональных данных. Поскольку данный термин не закреплен в законодательстве, он соответственно не был включен в составы административных правонарушений. Хотя, как указывала Л.К. Терещенко, повышенная степень общественной опасности фейковой информации показала необходимость введения не только административной ответственности, но и уголовной<sup>1</sup>.

Учитывая уникальность биометрических характеристик, создание дипфейка является достаточно серьезным правонарушением, которое находится на грани уголовного и административного законодательства. Дипфейк приводит к утрате возможности идентификации по биометрии, подвергшейся дублированию с помощью ИИ. Следовательно, необходимо законодательно закрепить состав административного правонарушения, предусматривающего меры ответственности за неправомерные действия в отношении конфиденциальности биометрических характеристик.

На сегодняшний день в законодательстве создание дипфейков относят к мошенническим действиям. Однако необходимо сформулировать понимание, что дипфейки создаются в двух случаях. Первый – это создание развлекательного контента, второй – использование дипфейка для совершения мошеннических действий. На основании этого можно считать, что дипфейк это отдельное правонарушение, отличное от мошеннических действий, так как само создание дипфейка является инструментом для совершения мошеннического действия.

В связи с этим считаем необходимым внести изменения в КоАП РФ и предусмотреть меры ответственности за административное правонарушение, связанное с созданием дипфейка для совершения мошеннических действий (приложение 4).

---

<sup>1</sup> Терещенко Л.К. Фейки и треш-стримы как угроза информационной безопасности // Журнал российского права. 2023. Т. 27, № 11. С. 107.

Следующим неурегулированным специфическим противоправным в отношении биометрических персональных данных деянием является спуфинг.

Системы биометрической аутентификации подвержены атакам спуфинга, когда неавторизованные клиенты (злоумышленники) могут попытаться обмануть систему путем подмены «живого» изображения лица/записи голоса авторизованного клиента его фотографией или видео-, аудиофайлом<sup>1</sup>.

Спуфинг – это обман биометрических систем путем предоставления биометрическому сенсору копий, муляжей, фотографий, отрезанных пальцев, заранее записанных звуков и т.п.<sup>2</sup> Статические биометрические образы (отпечаток пальца, радужка и другие) являются достаточно уникальными для высокоточной идентификации человека. Однако они уязвимы перед атаками представления (спуфинг), так как их невозможно держать в секрете<sup>3</sup>.

Идентификация по нескольким характеристикам предотвращает проблему спуфинга, так как она связана с несколькими модальностями, поэтому злоумышленнику будет трудно подделать сразу несколько идентификаторов авторизованного пользователя<sup>4</sup>.

В Российской Федерации ответственность за спуфинг рассматривается в рамках уголовного и административного законодательства. Статья 13.11 КоАП РФ «Нарушение законодательства Российской Федерации в области персональных данных» может применяться в случае нарушения правил использования средств связи, включая методы спуфинга<sup>5</sup>, однако прямого употребления этого термина в статье не используется. Данная статья характерна для классических персональных данных.

---

<sup>1</sup> Волкова С.С. Метод обнаружения технологии манипуляции с идентичностью лиц с применением сверточных нейронных сетей // Искусственный интеллект и принятие решений. 2022. № 2. С. 62.

<sup>2</sup> Алгулиев Р.М., Имамвердиев Я.Н., Мусаев В.Я. Методы обнаружения живучести в биометрических системах // Вопросы защиты информации. 2009. № 3(86). С. 16.

<sup>3</sup> Сулавко А.Е. Высоконадёжная двухфакторная биометрическая аутентификация по рукописным и голосовым паролям на основе гибких нейронных сетей // Компьютерная оптика. 2020. Т. 44, № 1. С. 82.

<sup>4</sup> Частикова В.А., Титова А.А., Войлова Д.О. Аналитический обзор методов идентификации личности на основе биометрических характеристик // Вестник Адыгейского государственного университета. Серия: Естественно-математические и технические науки. 2022. № 1(296). С. 95.

<sup>5</sup> Асянова С.Р., Жигалова Я.И. Спуфинг как угроза кибербезопасности: понятие, виды, меры противодействия // Журнал монетарной экономики и менеджмента. 2024. № 11. С. 247.

Важным является разграничение понятий дипфейк и спуфинг. Дипфейк – это инструмент, а спуфинг – процесс (несанкционированный доступ). Например, дипфейк-видео в реальном времени применяется для обхода систем распознавания лица – это биометрический спуфинг с помощью дипфейка.

Таким образом, целесообразно внести изменения в Федеральный закон от 29 декабря 2022 г. № 572-ФЗ и закрепить понятия дипфейка и спуфинга (приложение 3).

Дипфейк биометрических персональных данных – это воссоздание биометрических характеристик человека посредством использования искусственного интеллекта в целях совершения несанкционированного доступа при идентификации личности.

Спуфинг с использованием биометрических персональных данных – это использование дипфейка на основе биометрических характеристик в целях совершения неправомерной идентификации личности, ведущее к не санкционируемому доступу.

При совершении подобных действий необходимо предусмотреть нормы административной ответственности. Для этого необходимо внести соответствующие составы административного правонарушения в действующую редакцию КоАП РФ (приложение 4). Санкции при совершении данных правонарушений должны носить более жестокое наказание в отличие от классических персональных данных. Важно сформировать упредительный характер в области защиты биометрических персональных граждан в обществе.

При проведении исследования 73% респондентов указали, что считают сумму административного штрафа за совершение правонарушений, посягающих на конфиденциальность биометрических персональных данных, достаточной в размере от 500 тыс. руб. до 1 млн руб. При выборе санкции считаем необходимым учесть мнение общества (приложение 1).

Объективная сторона административного правонарушения, выражающаяся в бездействии в отношении защиты биометрических персональных данных, заключается в неисполнении оператором возложенной на него законом прямой

обязанности совершить определенные действия с биометрией или обеспечить их надлежащую обработку.

Бездействие заключается в несоблюдении конкретных обязанностей, установленных Федеральным законом от 27 июля 2006 г. № 152-ФЗ, Федеральным законом от 29 декабря 2022 г. № 572-ФЗ и подзаконными актами, в части обработки биометрических персональных данных.

Наиболее распространенными правонарушениями, выражающимися в бездействии, являются:

- неполучение письменного согласия субъекта на обработку биометрических персональных данных;
- невыполнение требований по обеспечению хранения биометрических персональных данных, в частности, неудаление идентификатора по истечению срока хранения;
- непринятие необходимых мер защиты биометрических персональных данных (отсутствие шифрования, СКЗИ, разграничение доступа и т.д.);
- непредставление уведомления в Роскомнадзор об обработке биометрических персональных данных;
- невыполнение предписаний Роскомнадзора, обязывающих оператора прекратить обработку биометрических персональных данных из-за нарушений.

Само по себе бездействие создает угрозу нарушения прав субъектов биометрических персональных данных (неприкосновенности частной жизни, недопустимости обработки без согласия). При этом должна быть установлена связь между бездействием оператора (невыполнением обязанности) и фактом нарушения установленного порядка обработки биометрических персональных данных. То есть, если бы оператор действовал надлежащим образом (исполнил обязанность), нарушение не возникло бы.

Практически все случаи бездействия в отношении биометрических персональных данных подпадают под различные части статей 13.11 и 13.11.3 КоАП РФ.

Совершение противоправных действий или бездействий в области защиты всегда несет посягательство на право граждан на личную информацию. Такое нарушение влечет за собой ряд негативных последствий, среди которых выделяется утрата приватности и потенциальная компрометация биометрических персональных данных.

Таким образом, объективная сторона правонарушения в виде бездействия в отношении биометрических персональных данных – это общественно опасное, противоправное, осознанное и волевое неисполнение оператором конкретной юридической обязанности, возложенной на него законом для обеспечения правовой защиты биометрических данных.

Субъект административного правонарушения – физическое или юридическое лицо, совершившее административное правонарушение и привлекаемое к административной ответственности<sup>1</sup>.

Субъектами административных правонарушений в области защиты биометрических персональных данных в Российской Федерации (в соответствии с КоАП РФ) являются:

1) оператор, осуществляющий обработку персональных данных (юридическое лицо или индивидуальный предприниматель (ИП), которые самостоятельно или совместно с другими лицами организуют и (или) осуществляют обработку персональных данных, а также определяют цели и содержание обработки);

2) должностные лица оператора (руководитель организации-оператора, ИТ-специалист, ответственный за обработку данных, или иное лицо, выполняющее организационно-распорядительные или административно-хозяйственные функции в организации-операторе, чьи действия (бездействие) привели к правонарушению);

3) государственные и муниципальные органы как операторы (органы публичной власти, органы субъектов РФ, органы местного самоуправления,

---

<sup>1</sup> Административное право в схемах: учебник и практикум для вузов. – URL: <https://urait.ru/bcode/560835/p.292> (дата обращения: 07.07.2025).

государственные и муниципальные учреждения, обрабатывающие биометрические данные в рамках своих полномочий).

Должностное лицо подлежит административной ответственности в случае совершения им административного правонарушения в связи с неисполнением либо ненадлежащим исполнением своих служебных обязанностей<sup>1</sup>.

Индивидуальные предприниматели привлекаются к административной ответственности по ст. 13.11.3 КоАП РФ как должностные лица (примечание к ст. 2.4 КоАП РФ).

Особенность административных правонарушений в области защиты биометрических персональных данных заключается в том, что субъектами правонарушения являются должностные и юридические лица. Юридическое лицо не может нести административную ответственность за противоправное действие (бездействие), состоящее в неисполнении, ненадлежащем исполнении, несоблюдении его руководителем, иными работниками (сотрудниками) обязанностей, запретов и ограничений, возложенных и установленных непосредственно в отношении них законом, иным нормативным правовым актом, локальным правовым актом, образующее объективную сторону административного правонарушения<sup>2</sup>.

Однако среди всей совокупности административных правонарушений обособленное место при исследовании занимает часть 17 статьи 13.11 КоАП РФ, где в качестве субъекта административного правонарушения указываются граждане.

При применении статей КоАП РФ к физическим и юридическим лицам необходимо иметь в виду, что если в статьях КоАП РФ не указано, что установленные данными статьями нормы применяются только к физическому

---

<sup>1</sup> См.: Административное право Российской Федерации: учебник для вузов / Ю.И. Мигачев, Л.Л. Попов, С.В. Тихомиров; под ред. Л.Л. Попова. – URL: <https://urait.ru/bcode/580351/p.178> (дата обращения: 07.08.2025).

<sup>2</sup> Кононов П.И. Проблемы соотношения административной ответственности юридических лиц и их руководителей, иных работников (по материалам арбитражно-судебной практики) // Законодательство Российской Федерации об административных правонарушениях: после реформы, перед реформой: Материалы Международной научно-практической конференции, посвященной памяти Д.Н. Бахраха, Екатеринбург, 17 ноября 2022 года. – Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный юридический университет». 2023. – С. 12.

лицу или только к юридическому лицу, данные нормы в равной мере действуют в отношении и физического, и юридического лица, за исключением случаев, если по смыслу данные нормы относятся и могут быть применены только к физическому лицу<sup>1</sup>.

Таким образом, субъектами административной ответственности за нарушения в сфере защиты биометрических персональных данных являются как организации и госорганы, непосредственно обрабатывающие такие данные (операторы), так и их должностные лица, виновные в нарушениях, которые привели к компрометации биометрической информации.

Субъективная сторона административного правонарушения – это психическое отношение субъекта (физического лица) к противоправному действию (бездействию) и его последствиям<sup>2</sup>. Субъективная сторона административного правонарушения представляет собой вину и может выражаться как в форме умысла, так и неосторожности<sup>3</sup>.

Субъективная сторона административного правонарушения в области защиты биометрических персональных данных в Российской Федерации характеризуется виной правонарушителя, которая может проявляться в форме умысла или неосторожности. Это ключевой элемент состава правонарушения, без которого привлечение к ответственности невозможно (статья 2.1 КоАП РФ).

Вина как обязательный признак субъективной стороны административного правонарушения демонстрирует психическое отношение лица к действию и его последствиям<sup>4</sup>. Форма вины определяется через формулы различного соотношения интеллектуальных и волевых процессов<sup>5</sup>.

---

<sup>1</sup> См.: Административное право Российской Федерации: учебник для вузов / Ю.И. Мигачев, Л.Л. Попов, С.В. Тихомиров; под ред. Л.Л. Попова. – URL: <https://urait.ru/bcode/580351/p.178> (дата обращения: 07.08.2025).

<sup>2</sup> Россинский Б.В., Старилов Ю.Н. Административное право: учебник. - 6-е изд., пересмотр. М.: Норма: Инфра-М, 2020. С. 433.

<sup>3</sup> Административное право: учебник / под ред. Л.Л. Попова, М.С. Студеникиной. – 3-е изд., перераб. и доп. С. 244.

<sup>4</sup> Ковшевацкий В.И., Стащенко С.П. Проблемы установления отдельных признаков субъективной стороны административного правонарушения // Актуальные проблемы административного права и процесса. 2019. № 1. С. 31.

<sup>5</sup> Амельчакова В.Н., Суслова Г.Н. Соотношение вины и субъективной стороны административного правонарушения // Вестник Московского университета МВД России. 2023. № 3. С. 24.

Формы вины при совершении административных правонарушений в области защиты биометрических персональных данных выражаются в форме умысла или неосторожности (статья 2.2 КоАП РФ).

Учитывая специфику административных правонарушений как противоправных деяний, справедливо будет отметить, что именно умысел, вне зависимости от того, выражен он прямо или косвенно, является преобладающей формой вины при их совершении<sup>1</sup>.

Прямой умысел при совершении административного правонарушения в области биометрических персональных данных характеризуется тем, что лицо (оператор) осознает противоправность своих действий (бездействия) в отношении биометрических характеристик, предвидит последующие вредные последствия (нарушение прав субъектов биометрии, риск утечки) и желает их наступления или сознательно допускает.

Косвенный умысел при совершении административного правонарушения в области биометрических персональных данных усматривается, когда оператор биометрии осознает противоправность, предвидит вредные последствия, но безразлично к ним относится (например, осознанно игнорирует требования о получении согласия, понимает, что это может привести к проверке и штрафу, но ему безразлично).

Административное правонарушение признается совершенным по неосторожности, если лицо, его совершившее, предвидело возможность наступления вредных последствий своего действия (бездействия), но без достаточных к тому оснований самонадеянно рассчитывало на предотвращение таких последствий либо не предвидело возможности наступления таких последствий, хотя должно было и могло их предвидеть. В первом случае неосторожность проявляется в форме легкомыслия (самонадеянности), так как лицо предвидело возможность наступления вредных последствий, но

---

<sup>1</sup> Амельчакова В.Н., Суслова Г.Н. Соотношение вины и субъективной стороны административного правонарушения // Вестник Московского университета МВД России. 2023. № 3. С. 24.

самонадеянно рассчитывало их предотвратить. Во втором случае – в форме небрежности<sup>1</sup>.

Легкомыслие можно усмотреть при совершении административного правонарушения, например, когда оператор знает о рисках хранения биометрических персональных данных в незашифрованном виде, но считает, что его ИТ-специалисты успеют все исправить до наступления инцидента.

Небрежность при совершении административного правонарушения будет проявлена, когда правонарушитель, например, должностное лицо не обеспечило контроль за доступом к биометрической базе данных, что привело к утечке, хотя обязано было это сделать по инструкции.

Классификация вины применительно к административным правонарушениям в области защиты биометрических данных имеет свои особенности:

- высокие требования к строгости соблюдения установленных законодательных норм, вытекающие из невозможности восстановления биометрических персональных данных. Хотя форма вины для квалификации по статьям 13.11 и 13.11.3 КоАП РФ остается умысел или неосторожность, сама природа биометрических персональных данных (уникальность, невозможность восстановления, высокий риск в случае утечки) подчеркивает важность должной осмотрительности оператора;

- нарушение требований к обеспечению безопасности биометрических персональных данных. Чаще возникает по неосторожности (небрежность в организации защиты, легкомыслие в оценке рисков), но может быть и умышленным (сознательное игнорирование требований стандартов);

- наличие формального состава. Многие правонарушения в сфере биометрических персональных данных, включая статьи 13.11 и 13.11.3 КоАП РФ, имеют формальный состав. Это означает, что для привлечения к административной ответственности не требуется наступления реальных вредных последствий (например, самой утечки данных), а достаточно самого факта

---

<sup>1</sup> Россинский Б.В. Административное право и административная ответственность: курс лекций. – 2-е изд., перераб. М.: Норма: Инфра-М, 2025. 352 с. – URL: <https://znanium.ru/catalog/product/2174353> (дата обращения: 08.07.2025).

противоправного действия (бездействия) (обработки без согласия, ненадлежащей защиты), совершенного виновным. При этом вина доказывается в отношении самого факта нарушения установленных правил.

Вместе с тем статья 2.1 «Административное правонарушение» КоАП РФ дает специфическое определение вины юридического лица: «Юридическое лицо признается виновным в совершении административного правонарушения, если будет установлено, что у него имелась возможность для соблюдения правил и норм, за нарушение которых настоящим Кодексом или законами субъекта Российской Федерации предусмотрена административная ответственность, но данным лицом не были приняты все зависящие от него меры по их соблюдению»<sup>1</sup>.

Таким образом, субъективная сторона административного правонарушения в сфере защиты биометрических персональных данных – это психическое отношение правонарушителя к своему противоправному деянию и его возможным последствиям, выражающееся в форме умысла (прямого или косвенного) или неосторожности (легкомыслия или небрежности). Доказывание конкретной формы вины является обязательным условием для законного привлечения к административной ответственности по соответствующим статьям КоАП РФ. Характер биометрических данных как особо защищаемой категории персональных данных подчеркивает необходимость высокой степени осмотрительности и соблюдения установленных правил их обработки.

Административным наказанием при совершении административных правонарушений чаще всего выступает административный штраф. Суммы штрафа варьируются в достаточно большом диапазоне – от 10 тыс. руб. до 2 млн руб.

И если рассматривать административный штраф как санкции к данным правонарушениям, то можно отметить негативную тенденцию, на которую обращал внимание А.В. Минбалеев. Крупные организации, использующие биометрию в своей деятельности, легко могут закладывать штрафы в риски,

---

<sup>1</sup> Административное право: учебник / под ред. Л.Л. Попова, М.С. Студеникиной. – 3-е изд., перераб. и доп. С. 237.

связанные с утечкой персональных данных<sup>1</sup>. Соответственно, для них это не будет составлять существенных убытков.

Санкции за административные правонарушения в области защиты биометрических персональных данных должны быть существенно строже, чем за нарушения, связанные с классическими персональными данными. По нашему мнению, именно этот признак указывает на необходимость выделения в отдельные составы административные правонарушения в области защиты биометрических персональных данных. Биометрия обладает своей спецификой, в связи с чем необходимо продолжить ее обособление от классических персональных данных, в том числе и при классификации противоправных действий.

В ходе исследования было установлено, что основной упор законодательства делается на добровольности предоставления биометрических характеристик человека. Как правовую основу реализации данного условия выделяют наличие согласия на обработку персональных данных. Однако отметим, что целесообразно выделить самостоятельного состава, т.к. сегодня законодательно разработано согласие на обработку биометрических персональных данных, и часто, проявляя халатность, операторы биометрии считают достаточным получение только согласия на обработку персональных данных.

Исследуя вопрос добровольности, отметим, что частью 2.1 статьи 5.63 и статьей 14.8 КоАП РФ в качестве отдельных составов выделен отказ обслуживать гражданина при его нежелании подтверждать свою личность с помощью биометрии. Однако перечень отношений, в которых используется биометрия, не ограничивается только этими условиями. В связи с чем целесообразно выделить составов административных правонарушений, предусматривающих ответственность за принуждение к сдаче биометрии, в том числе и сокрытии информации о ее получении, и отказа от совершения правоотношений без идентификации с помощью биометрических характеристик.

---

<sup>1</sup> Минбалеев А.В. Проблемы цифрового права: учебное пособие. С. 173.

Согласно данным, представленным на официальном сайте Агентства правовой информации, за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11, ст. 13.11.1, ч. 2 ст. 13.12, ч. 4,5 ст. 13.13, ст. 13.14 КоАП РФ) в 2023 году рассмотрено 916 дел об административных правонарушениях, из них 703 – подвергнуто наказанию. Общая сумма назначенных штрафов составила 143 334 тысяч рублей<sup>1</sup>.

Однако, если обратиться к статистике, приведенной Управлением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Белгородской области за 2023 год, то здесь ситуация обратная. За 2023 год судами вынесено всего 2 решения/постановления по протоколам об административных правонарушениях на общую сумму 60 тысяч рублей<sup>2</sup>.

В настоящий момент мы не можем оценить практику правоприменения исследуемых новелл в отношении биометрических персональных данных. Однако можем смело отметить, что создание мер правового воздействия на сегодняшний день призвано максимально обеспечить безопасность по сбору, обработке и хранению биометрических персональных данных. При этом государство продолжает реализовывать политику добровольности при использовании гражданами своей биометрии.

Со стороны государства безусловно требуется создание эффективной системы раскрытия преступлений, связанных с утечкой биометрии, и предусмотрение мер ответственности за правонарушения и преступления в зависимости от тяжести наступивших последствий.

Подводя итог исследованию в рамках данного параграфа, отметим следующее.

---

<sup>1</sup> Судебная статистика РФ / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://stat.api-пресс.рф/stats/adm/t/31/s/1> (дата обращения: 16.04.2025).

<sup>2</sup> Результаты деятельности за период с 01.01.2023 по 29.12.2023 / Официальный интернет-сайт [Электронный ресурс]. – URL: [https://31.rkn.gov.ru/docs/31/Otchjot\\_zh\\_12\\_mes\\_2023\\_god.pdf](https://31.rkn.gov.ru/docs/31/Otchjot_zh_12_mes_2023_god.pdf) (дата обращения: 17.04.2024).

1. Особенности административной ответственности за правонарушения в сфере обработки биометрических персональных данных обусловлены спецификой биометрических характеристик человека, их уникальностью и потенциальными рисками, связанными с утратой конфиденциальности данных. Эти риски могут привести к невозможности достоверной идентификации личности, что, в свою очередь, ставит под угрозу безопасность и права граждан.

2. В настоящее время правовое регулирование административной ответственности за правонарушения в сфере защиты биометрических идентификаторов осуществляется в рамках общих положений об административных правонарушениях в отношении персональных данных, а также специальных норм, регламентирующих функционирование единой биометрической системы. Тем не менее, нормы, касающиеся ответственности за отказ в предоставлении услуг по причине нежелания субъектов персональных данных проходить процедуру биометрической регистрации, остаются недостаточно детализированными.

Учитывая стремительное развитие правового регулирования в области защиты биометрических персональных данных, представляется необходимым выделить данную категорию правонарушений в самостоятельные составы административных правонарушений. Это обеспечит установление более строгих санкций за соответствующие деяния, что, в свою очередь, будет способствовать формированию эффективных превентивных мер.

Введение отдельных составов административных правонарушений в сфере защиты биометрических персональных данных позволит более четко определить границы ответственности субъектов правоотношений, а также обеспечить дифференцированный подход к назначению административных наказаний в зависимости от характера и степени общественной опасности совершенного правонарушения. Кроме того, это будет способствовать повышению эффективности правоприменительной практики и уровня защиты прав и законных интересов субъектов персональных данных.

3. В действующей редакции КоАП РФ нормы, закрепляющие правонарушения в сфере защиты биометрической персональной информации, распределены по нескольким главам. Помимо главы 13 «Административные правонарушения в области связи и информации», они также содержатся в главе 5 «Административные правонарушения, посягающие на права граждан» (часть 2.1 статьи 5.63) и главе 14 «Административные правонарушения в области предпринимательской деятельности и деятельности саморегулируемых организаций» (статья 14.8).

Такой разрозненный подход к правовому регулированию вызывает сомнения в эффективности правоприменительной практики и порождает правовую неопределенность для участников правоотношений. В связи с этим представляется целесообразным систематизировать соответствующие нормы и интегрировать их в отдельную главу, что обеспечит более последовательное и логически обоснованное регулирование данной сферы.

Биометрические персональные данные являются одной из наиболее чувствительных категорий информации, требующей специальной защиты. Объединение норм, регулирующих правонарушения в этой области, в рамках единой главы позволит обеспечить комплексный и целенаправленный подход к защите прав и свобод граждан в контексте использования биометрических технологий.

Кроме того, такой подход позволит устранить дублирование норм и противоречия между различными главами КоАП РФ, что повысит правовую определенность и предсказуемость правоприменительной практики, а также будет способствовать более эффективной защите прав граждан в сфере обработки биометрической персональной информации.

4. В условиях стремительного прогресса в области искусственного интеллекта и совершенствования технических процессов наблюдается экспоненциальный рост новых форм противоправных действий, направленных против биометрических персональных данных. Эти угрозы требуют адекватного

правового регулирования, которое должно учитывать специфику современных технологий и их потенциальные риски.

В связи с этим предлагается внести соответствующие изменения в действующее законодательство Российской Федерации. В частности, необходимо дополнить Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» дефинициями понятий «дипфейк» и «спуфинг».

Кроме того, целесообразно предусмотреть меры административной ответственности за указанные правонарушения. Для этого необходимо внести соответствующие изменения в КоАП РФ, закрепив нормы, регулирующие ответственность за создание, распространение и использование дипфейков, а также за осуществление спуфинга.

Эти меры позволят обеспечить правовую защиту биометрических персональных данных и минимизировать риски, связанные с их несанкционированным использованием.

## ГЛАВА 2. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

### § 1. Система органов публичной власти, осуществляющих защиту биометрических персональных данных

Масштабные динамичные социально-экономические и иные процессы существенным образом влияют на механизм публичного управления в целом и на все его составные части<sup>1</sup>. Как обоснованно отмечено М.Н. Кобзарь-Фроловой, термин «публичная власть», введенный в оборот Конституцией Российской Федерации, новеллой для юридической науки не является<sup>2</sup>. Понятие «публичной власти» прошло долгий путь своего научного формирования. Многими учеными были предложены трактовки данного термина с учетом разных этапов исторического развития государства.

Довольно подробный анализ по становлению понятия «публичной власти» изложен в научных статьях И.В. Упорова<sup>3</sup> и Д.Э. Пилия<sup>4</sup>.

Для исследования авторы использовали понятия, предлагаемые Ю.Е. Аврутиным<sup>5</sup>, Б.В. Россинским<sup>6</sup>, Ю.Ю. Сорокиным<sup>7</sup>, В.В. Рачинским<sup>8</sup>,

---

<sup>1</sup> Эффективность государственных управленческих решений в условиях цифровизации / С.М. Зубарев, А.В. Иванов, С.Г. Кирдина-Чэндлер [и др.]. М.: Проспект, 2023. С. 14.

<sup>2</sup> Кобзарь-Фролова М.Н. Система органов публичной власти Российской Федерации: понятие, характерные признаки, взаимодействие // Сибирское юридическое обозрение. 2021. № 2. С. 192–203.

<sup>3</sup> Упоров И.В. Категория «публичная власть» в толковании ученых-правоведов // Форум. 2024. № 2(32). С. 299–304.

<sup>4</sup> Пилия Д.Э. Основные подходы к определению понятия «публичная власть» в публично-правовых (государственно-правовых) науках // Lex Russica (Русский закон). 2023. Т. 76, № 5(198). С. 9–23.

<sup>5</sup> Аврутин Ю.Е. О парадигме государственного управления в контексте модернизации российского административного права / Актуальные проблемы административного и административно-процессуального права: сборник статей: в 3-х ч., Санкт-Петербург, 24 марта 2017 года. Ч. 1. – СПб.: Санкт-Петербургский университет МВД России, 2017. С. 32–47.

<sup>6</sup> Россинский Б.В. Формирование публичной власти как реализация системного принципа ингрессии // Административное право и процесс. 2022. № 7. С. 4–8.

<sup>7</sup> Сорокин Ю.Ю. Публичная власть и интересы общества: проблемы взаимодействия: дис ... канд. юрид. наук. М., 2011. 213 с.

<sup>8</sup> Рачинский В.В. Публичная власть как общеправовая категория (Теоретико-прикладной аспект): дис ... канд. юрид. наук. Уфа, 2003. 195 с.

Б.З. Кушховой<sup>1</sup>, Н.И. Грачевым<sup>2</sup> и другими.

Законодательно же ни одно из определений публичной власти не закреплено, а используется понятие единой системы публичной власти. Под нею понимаются федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, иные государственные органы, органы местного самоуправления в их совокупности, осуществляющие в конституционно установленных пределах на основе принципов согласованного функционирования и устанавливаемого на основании Конституции Российской Федерации и в соответствии с законодательством организационно-правового, функционального и финансово-бюджетного взаимодействия, в том числе по вопросам передачи полномочий между уровнями публичной власти, свою деятельность в целях соблюдения и защиты прав и свобод человека и гражданина, создания условий для социально-экономического развития государства<sup>3</sup>.

Частью единой системы публичной власти являются органы, осуществляющие защиту биометрических персональных данных. В настоящее время в научной литературе вопросы определения понятия системы органов публичной власти, осуществляющих защиту биометрических персональных данных, структуры данной системы и ее классификации не нашли своего отражения.

Это объясняется новизной исследуемой тематики и сложностью построения системы, так как сегодня биометрические персональные данные охватывают все большее количество общественных отношений с привлечением новых участников.

Понятие «система органов публичной власти, осуществляющих защиту биометрических персональных данных» имеет свои особенности. Различные подходы к определению понятия «система» свидетельствуют о том, что в

---

<sup>1</sup> Кушхова Б.З. Юридическая ответственность публичной власти в современной России: общетеоретический аспект. Краснодар, 2009. 199 с.

<sup>2</sup> Грачев Н.И. Публичная власть как политико-правовая категория: понятие, основные признаки и формы // Вестник Волгоградской академии МВД России. 2020. № 4(55). С. 8-19.

<sup>3</sup> Федеральный закон от 8 декабря 2020 г. № 394-ФЗ «О Государственном Совете Российской Федерации» // Собрание законодательства Российской Федерации. 2020. № 50 (часть III). Ст. 8039.

отечественной науке в целом нет единого определения данного понятия<sup>1</sup>. Одним из исторически принятых можно считать определение системы, приведенное Людвигом фон Берталанфи. Он определял систему как комплекс взаимодействующих элементов, находящихся в отношениях и связях друг с другом<sup>2</sup>.

Понятие «система органов публичной власти, осуществляющих защиту биометрических персональных данных» должно отвечать ряду признаков, которые будут заложены в нем, характеризую цели и особенности исследуемого термина.

В результате исследования понятия биометрических персональных данных, нормативной правовой базы, регулирующей правоотношения в данной области, мы предлагаем выделить следующие признаки, характерные для определения системы органов публичной власти, осуществляющих защиту биометрических персональных данных:

- 1) органы и организации должны иметь общую цель деятельности – защита биометрических персональных данных;
- 2) при реализации цели необходимо обеспечить эффективное взаимодействие органов публичной власти;
- 3) в своей деятельности органы и организации должны руководствоваться верховенством Закона;
- 4) органы и организации должны обеспечивать единство методов по защите биометрических персональных данных.

Таким образом, нами выделены основные признаки, на которые мы можем опираться при формировании понятия системы органов публичной власти, осуществляющих защиту биометрических персональных данных. Данные признаки обладают универсальностью для всех субъектов правоотношений, использующих биометрические персональные данные в своей деятельности.

---

<sup>1</sup> Магомедова Е.А., Курзаков М.В., Зайцева М.А. К вопросу о понятии системы права в отечественной юридической науке // Тенденции развития науки и образования. 2024. № 107-5. С. 140.

<sup>2</sup> Bertalanffy L. von (1968). General System Theory: Foundations, Development, Applications. New York: George Braziller, P. 55.

Также основные признаки сформулированы с учетом проблемных вопросов в области обеспечения безопасности биологических и физиологических характеристик человека.

Во-первых, это строгое соблюдение действующего законодательства. При сборе, обработке и хранении биометрии недопустимо халатное отношение к соблюдению правовых норм. Только строгое соблюдение установленных норм позволит сформировать позитивное отношение граждан к использованию биометрии.

Во-вторых, нами обращалось внимание на единство методов. Сегодняшнее законодательство нацелено на централизацию данных процессов, совершенно недопустим тот факт, что органами или организациями осуществляется сбор, обработка и хранение биометрии в частных базах данных и с использованием отличных и противоречащих друг другу методов. Решение этой проблемы позволит государству создать действенную систему контроля за соблюдением прав граждан в вопросах защиты системы органов публичной власти, осуществляющих защиту биометрических персональных данных.

В-третьих, в процессе исследования выявлена проблема взаимодействия между органами публичной власти по реализации их функций. Необходима разработка системы, обеспечивающей создание унифицированных межведомственных запросов.

Предложения по решению данных вопросов будут изложены нами в следующем параграфе диссертации. Решение данных вопросов станет ключом к созданию действенной системы органов публичной власти, осуществляющих защиту биометрических персональных данных.

Таким образом, исходя из вышеприведенных признаков, опираясь на определение единой системы публичной власти, норм действующего законодательства, мы предлагаем авторскую дефиницию, которая может быть сформулирована следующим образом.

Система органов публичной власти, осуществляющих защиту биометрических персональных данных, – это совокупность всех уровней органов

публичной власти (федеральных, субъектов Российской Федерации, местных) и организаций, осуществляющих взаимодействие по сбору, обработке и хранению биометрических персональных данных в установленных действующим законодательствах целях и реализующих меры по обеспечению правовой и технической безопасности полученных данных с соблюдением этических норм в отношении полученных данных.

Подобный подход к данному определению может быть интегрирован в процесс совершенствования нормативно-правовой базы в сфере биометрических персональных данных, способствуя повышению уровня правовой регламентации и эффективности защиты данных.

Анализ нормативных правовых актов, регулирующих административно-правовые отношения в области защиты биометрических персональных данных, и имеющейся научной литературы, показал, что ранее не было предложено вариантов построения данной системы. В связи с чем нами предложено собственное видение возможного представления данной системы.

Систему органов публичной власти, осуществляющих защиту биометрических персональных данных в Российской Федерации, целесообразно структурировать в виде иерархически организованных групп, каждая из которых классифицируется по ряду специфических критериев. Данный подход позволяет более точно определить функциональные обязанности и компетенции каждого органа в рамках комплексной системы обеспечения информационной безопасности и защиты биометрических персональных данных.

#### I. Территориальность уровней управления:

1) федеральный – высший уровень государственной власти (Правительство Российской Федерации, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, Министерство органов внутренних дел Российской Федерации и другие);

2) региональный – уровень субъектов Российской Федерации (Управление Федеральной службы по надзору в сфере связи, информационных технологий и

массовых коммуникаций по Белгородской области, Министерство цифрового развития Белгородской области, УМВД России по Белгородской области и другие);

3) местный – уровень органов местного самоуправления (администрации муниципальных образований, муниципальные учреждения).

Данное разграничение носит весьма универсальный характер. В соответствии с частью 3 статьи 1 Федерального закона от 21 декабря 2021 г. № 414-ФЗ «Об общих принципах организации публичной власти в субъектах Российской Федерации» деятельность органов публичной власти осуществляется по принципу подведомственности: «Федеральные органы государственной власти и иные федеральные государственные органы осуществляют свои полномочия на территории субъекта Российской Федерации непосредственно или через создаваемые ими территориальные органы во взаимодействии с органами государственной власти субъекта Российской Федерации, иными государственными органами субъекта Российской Федерации, органами местного самоуправления, действующими на территории субъекта Российской Федерации». Построение такой системы обладает рядом положительных особенностей. Иерархия органов публичной власти обеспечивает действенный контроль от федерального к местному, реализуя задачу по обеспечению единства методов по работе с биометрическими персональными данными. Положительным является и тот факт, что совершенствование данной системы может идти не только от федеральных органов публичной власти, но и от местных. Негативным же моментом можно отметить, что при такой классификации остаются в стороне ряд организаций, например, Банк России, осуществляющий контроль за целой сферой банковских организаций, которые по данному признаку часто разделены быть не могут.

II. Цель сбора, обработки и хранения биометрических персональных данных:

1) органы и организации, осуществляющие сбор, обработку и хранение биометрических персональных данных для осуществления гражданских правоотношений (Центральный банк России, многофункциональные центры);

2) органы и организации, осуществляющие сбор, обработку и хранение биометрических персональных данных для обеспечения безопасности государства и общества (ФСБ России, МВД России и другие).

По нашему мнению, данная классификация наиболее актуальна в современных условиях. Если ранее биометрия использовалась в целях идентификации только правоохранительными органами, то сегодня она охватывает все сферы общества. При этом, с каждым годом область использования биометрии все шире, в том числе и в рамках деятельности органов публичной власти. Например, недавно запущен эксперимент, который предполагает предоставление государственных услуг в многофункциональных центрах предоставления государственных услуг (МФЦ) в Липецкой, Челябинской и Ленинградской областях без предъявления паспорта, а с помощью идентификации личности по биометрии<sup>1</sup>. Это подтверждает тот факт, что использование биометрии уже давно выходит за рамки правоохранительной деятельности, обретая популярность в гражданско-правовых отношениях и с каждым годом будет становиться шире, что обуславливает актуальность приведенной нами классификации.

III. Направление деятельности органов публичной власти в обеспечении защиты биометрических персональных данных:

1) законодательные органы – формирование государственной политики в области обеспечения защиты биометрических персональных данных (Государственная Дума Российской Федерации, Совет Федерации Федерального Собрания Российской Федерации);

2) исполнительные и контролирующие органы – проведение мероприятий по обеспечению защиты биометрических персональных данных, контроль за соблюдением действующего законодательства в отношении указанных данных (Правительство Российской Федерации, Минцифры России, Роскомнадзор, ФСБ России, МВД России и другие).

---

<sup>1</sup> Определен перечень госуслуг, которые можно получить по биометрии в трех пилотных регионах [Электронный ресурс]. – URL: <https://объясняем.рф/articles/news/> (дата обращения: 12.06.2025).

Предложенная классификация нацелена на выделение в отдельные группы органов публичной власти по виду осуществляемой деятельности в области защиты биометрических персональных данных. Данная классификация требует более детального рассмотрения в целях определения особенностей деятельности органов публичной власти в вопросах обеспечения безопасности биометрии.

Так, законодательные органы определяют векторы развития государственно-правовой политики в области биометрических персональных данных, формируют правовую основу для деятельности органов публичной власти и определяют полномочия всех участников публично-правовых отношений.

Роль законодательных органов выражается в подготовке нормативного правового поля, которое призвано разработать систему эффективного использования биометрических персональных данных, при этом соблюсти баланс по соблюдению конституционных прав граждан<sup>1</sup>.

В отсутствие единого нормативного правового акта, регулирующего административно-правовую защиту биометрических персональных данных, полномочия, возложенные на органы публичной власти, изложены в различных нормативных правовых актах.

Так, Федеральным законом от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных» определен перечень органов публичной власти, которые формируют политику государства в области обеспечения безопасности биометрических персональных данных. Данный Федеральный закон имеет своей особенностью тот факт, что он регулирует использование биометрии человека для реализации гражданских отношений, кроме случаев, когда по соответствующему запросу (в целях оперативно-разыскной, контрразведывательной или разведывательной деятельности; обороны страны, обеспечения безопасности государства и охраны правопорядка, реализации

---

<sup>1</sup> Карпушина А.В. Приоритетные направления правового регулирования биометрических персональных данных // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2024. № 4. С. 104.

внешней политики; функционирования государственной системы миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность; обеспечения санитарно-эпидемиологического благополучия) сведения могут быть направлены в органы, осуществляющие правоохранительную деятельность.

Федеральным законом от 29.12.2022 № 572-ФЗ определены функции, возложенные на Правительство Российской Федерации. Согласно ч. 3 ст. 3 ФЗ от 29.12.2022 № 572 Правительство Российской Федерации утверждает положение о единой биометрической системе по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и Центральным банком Российской Федерации.

В связи с этим на Правительство Российской Федерации возлагается важная роль по формированию методов обеспечения безопасности в отношении биометрических характеристик как с помощью правовых, так и технических методов.

Для этого Правительством РФ образован координационный совет по развитию цифровых технологий идентификации и аутентификации на основе биометрических данных (далее – Координационный совет) (п. 22 ст. 3 ФЗ от 29.12.2022 № 572)<sup>1</sup>.

Координационный совет является постоянно действующим органом. Положение о Координационном совете и его состав, включающий в том числе представителей общественности, централизованных религиозных организаций и экспертного сообщества, утверждаются Правительством Российской Федерации<sup>2</sup>.

Постановлением Правительства Российской Федерации от 29.12.2022 № 2511 «О Координационном совете по развитию цифровых технологий

---

<sup>1</sup> В России образован координационный совет по развитию биометрических технологий [Электронный ресурс]. – URL: <https://digital.gov.ru/news-media/v-rossii-obrazovan-koordinacionnyj-sovet-po-razvitiyu-biometricheskih-tehnologij> (дата обращения: 25.03.2025).

<sup>2</sup> Там же.

идентификации и аутентификации на основе биометрических персональных данных»<sup>1</sup> утверждено Положение о деятельности совета.

К обязанностям, возлагаемым на Координационный совет, относятся:

- определение стратегических направлений развития биометрических технологий в Российской Федерации и развития единой биометрической системы, а также подготовка предложений по их внедрению в различные сферы правоотношений;

- осуществление координации деятельности федеральных органов исполнительной власти, исполнительных органов субъектов Российской Федерации, органов местного самоуправления, правительственных и межведомственных комиссий, советов, общественных объединений, экспертных сообществ, государственных организаций и других организаций по вопросам развития и внедрения биометрических технологий в целях обеспечения недискриминационного доступа к единой биометрической системе;

- рассмотрение вопросов и разработка предложений по совершенствованию биометрических технологий, по унификации требований к инфраструктуре обработки данных с применением биометрических технологий в целях предоставления государственных и муниципальных услуг, а также иных услуг, в том числе в дистанционном формате<sup>2</sup>.

При анализе полномочий Координационного совета нами обращено внимание на тот факт, что вопросы по обеспечению безопасности государства посредством использования биометрических персональных данных не находятся в его подведомственности. Таким образом, Правительство Российской Федерации возлагает данное направление на иные органы публичной власти (МВД России,

---

<sup>1</sup> Постановление Правительства Российской Федерации от 29.12.2022 № 2511 «О Координационном совете по развитию цифровых технологий идентификации и аутентификации на основе биометрических персональных данных» // Собрание законодательства Российской Федерации. 2023. № 1. Ст. 312 (Часть II).

<sup>2</sup> Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства Российской Федерации. 2023. № 1 (часть I). Ст. 19.

ФСБ России). Координационный совет призван обеспечить безопасность самих биометрических данных.

Важно обратить внимание и на состав Координационного совета. Биометрические персональные данные являются и на сегодняшний день темой для дискуссий<sup>1</sup>. Одна часть граждан не видит опасности в использовании биометрии, другая же выступает против идентификации личности по биологическим или физиологическим признакам. В связи с чем при принятии важных решений в отношении использования биометрических персональных данных от государства требуется учитывать мнение общественности, религиозных организаций, экспертного сообщества. На основании этого законодатель включил в состав Координационного совета представителей указанных организаций.

Исходя из этого можно отметить, что государство стремится найти решение по использованию биометрических персональных данных, при котором не будет допущено нарушение конституционных прав граждан<sup>2</sup>.

Одним из направлений в области законодательной власти является разработка национальных проектов, направленных на цифровизацию общества, повышение качества услуг посредством использования удаленной идентификации.

В рамках реализации Указов Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» и от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года», в том числе с целью решения задачи по обеспечению ускоренного внедрения цифровых технологий в экономике и социальной сфере, Правительством РФ сформирована национальная программа «Цифровая экономика Российской Федерации»,

---

<sup>1</sup> Артамонова Я.В., Барсуков С.С., Суханова А.А. Биометрические технологии: отношение населения и преодоление рисков // Государственное и муниципальное управление. Ученые записки. 2024. № 1. С. 232.

<sup>2</sup> Мочалов А.Н. Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности // Lex russica (Русский закон). 2021. Т. 74, № 9. С. 99.

утвержденная протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7<sup>1</sup>.

Национальная программа реализовывалась в рамках государственных программ Российской Федерации «Информационное общество», «Экономическое развитие и инновационная экономика» и других государственных программ Российской Федерации, включая отраслевые государственные программы субъектов Российской Федерации<sup>2</sup>.

Как отмечали М.Б. Добробаба и А.В. Минбалеев, сектор информационных технологий является одним из важнейших секторов российской экономики, который можно рассматривать в качестве ядра цифровой экономики<sup>3</sup>.

Конкретно биометрические персональные данные упомянуты в Федеральном проекте «Информационная безопасность». В качестве основных задач по реализации проекта в области биометрических персональных данных были сформированы следующие направления деятельности:

- создание ресурса для дистанционной регистрации юридических лиц и индивидуальных предпринимателей и открытия им счетов в кредитных организациях с использованием технологии, защищенной с использованием криптографических средств, на основе документов нового образца, содержащих персональные данные гражданина, включая биометрические, а также усиленную квалифицированную электронную подпись указанных данных;
- создание инфраструктуры сбора биометрических данных граждан и выдачи документов нового образца, содержащих усиленную квалифицированную

---

<sup>1</sup> Национальная программа «Цифровая экономика Российской Федерации» [Электронный ресурс]. – URL: <https://digital.gov.ru/target/nacziionalnaya-programma-czifrovaya-ekonomika-rossijskoj-federaczii> (дата обращения: 15.03.2025).

<sup>2</sup> Паспорт национального проекта Национальная программа "Цифровая экономика Российской Федерации" (утв. протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7) [Электронный ресурс]. – URL: <https://base.garant.ru/72296050/> (дата обращения: 15.03.2025).

<sup>3</sup> Добробаба М.Б., Минбалеев А.В. Выработка правовых средств адаптации к санкционным мерам в сфере ИТ-сектора // Журнал Сибирского федерального университета. Серия: Гуманитарные науки. 2024. Т. 17, № 6. С. 1049.

электронную подпись и биометрические данные гражданина на территории всех субъектов Российской Федерации<sup>1</sup>.

На сегодняшний день сложно говорить о результатах подготовки данных пунктов к реализации. Безусловно, Россия идет путем накопления биометрических персональных данных, также внедрена электронная подпись, используются загранпаспорта с биометрией. Однако создание и использование внутреннего паспорта, содержащего биометрическую информацию, требует поддержки общества.

Отношение граждан к использованию биометрических персональных данных информативно изложено в результатах опроса, проведенного ВЦИОМ. Так, согласно приведенным данным, в 2023 году в обществе преобладал нейтрально-негативный настрой в отношении использования биометрических персональных данных, 2024 год характеризуется более позитивным результатом: четверо из десяти россиян относятся к подтверждению личности по биометрии в той или иной степени положительно (41%, 2023 г. – 27%)<sup>2</sup>.

В настоящее время результат опроса говорит о том, что граждане либо недостаточно проинформированы о биометрических персональных данных, либо сказывается этическая сторона использования биометрии (недоверие граждан к степени безопасности предоставляемых данных). Ведь биометрия представляет собой наиболее личную информацию, которая подлежит высокой степени защиты как с правовой стороны, так и с технической. Сегодня о вопросах этики в отношении биометрических персональных данных ведется много дискуссий, однако нет научного консенсуса. Разработка предложений по совершенствованию мер защиты биометрических персональных данных в области этических норм и правил будет предложена в следующем параграфе.

---

<sup>1</sup> Паспорт национального проекта Национальная программа «Цифровая экономика Российской Федерации» (утв. протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7) [Электронный ресурс]. – URL: <https://base.garant.ru/72296050/> (дата обращения: 15.03.2025).

<sup>2</sup> Биометрия на марше: лицом к лицу с будущим / Официальный сайт Акционерного общества «Всероссийский центр изучения общественного мнения» (ВЦИОМ) [Электронный ресурс]. – URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/biometrija-na-marshe-licom-k-licu-s-budushchim> (дата обращения: 12.05.2025).

Одним из направлений стратегических национальных приоритетов, обеспечивающих национальную безопасность государства, является информационная безопасность<sup>1</sup>. Отдельно необходимо рассмотреть один из аспектов государственной стратегии по цифровизации Российской Федерации, которая открывает важное направление государственной политики по использованию биометрических персональных данных. Так, Стратегией развития информационного общества в Российской Федерации на 2017-2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203<sup>2</sup>, в качестве одной из целей выделяют создание цифрового правительства.

Цифровое правительство – новый уровень электронного правительства<sup>3</sup>. Ю.М. Акаткин и Е.Д. Ясиновская считают, что для успешной цифровой трансформации государственного сектора в России необходимо развитие совместного использования информации государственными организациями и построение единого цифрового пространства<sup>4</sup>.

Продолжением работы государства в реализации данного направления стало принятие Распоряжения Правительства Российской Федерации от 16 марта 2024 г. № 637-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления»<sup>5</sup>.

Т.А. Полякова в своей научной статье отмечала, что цифровизация публичного управления формирует новые информационно-правовые механизмы идентификации и аутентификации субъектов – физических лиц, которые, как

---

<sup>1</sup> Дугенец А.С. Государственное регулирование обеспечения информационной безопасности несовершеннолетних как составляющая национальной безопасности России // Административное право и процесс. 2023. № 5. С. 22.

<sup>2</sup> Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

<sup>3</sup> Сморгачева Л.Н. Цифровое правительство как перспектива государственного управления в России: информационно-правовые аспекты // Правовая информатика. 2022. № 2. С. 26.

<sup>4</sup> Акаткин Ю.М., Ясиновская Е.Д. Цифровая трансформация правительства: датацентричность и модели-ориентированность // Информационные ресурсы России. 2019. № 1(167). С. 5.

<sup>5</sup> Распоряжение Правительства Российской Федерации от 16 марта 2024 г. № 637-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления» // Собрание законодательства Российской Федерации. 2024. № 43. Ст. 4169.

показывает существующая практика, идут по пути формирования новых моделей и средств идентификации субъектов информационного обмена<sup>1</sup>.

Одним из таких новшеств стала разработка цифрового профиля гражданина. Вопросы формирования цифрового профиля и ранее рассматривались в научных статьях А.В. Минбалеева<sup>2</sup>, О.И. Долгановой, Е.В. Васильевой, Д.А. Рябова<sup>3</sup>, Б.Б. Славина, О.В. Башкировой<sup>4</sup>, Е. Р. Орловой, Э.В. Голоманчук<sup>5</sup> и других.

Определение понятия «цифровой профиль» в действующем законодательстве отсутствует, а наполняемость охарактеризована количеством возможной информации о гражданине.

Многими учеными предлагались свои трактовки понятия цифрового профиля, однако наиболее удачным, по нашему мнению, является определение, изложенное А.В. Минбалеевым. Он определил, что цифровой профиль – это совокупность актуальных, достоверных данных и иных сведений о гражданах и юридических лицах, формируемых в единой системе идентификации и аутентификации или других информационных систем органов государственной власти и местного самоуправления, а также подведомственных им организаций, взаимодействующих с ней посредством единой системы межведомственного электронного взаимодействия, в целях их предоставления, с согласия соответствующих граждан или юридических лиц субъектам, запросившим доступ к этим сведениям посредством инфраструктуры цифрового профиля<sup>6</sup>.

---

<sup>1</sup> Полякова Т.А., Бойченко И.С. Особенности взаимодействия и правового обеспечения информационной безопасности в единой биометрической системе в Российской Федерации // Правовая политика и правовая жизнь. 2023. № 3. С. 28.

<sup>2</sup> Минбалеев А.В. Проблемы и перспективы обеспечения защиты персональных данных граждан в цифровом профиле // Вестник УрФО. Безопасность в информационной сфере. 2021. № 4(42). С. 59–63.

<sup>3</sup> 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.

<sup>4</sup> Башкирова О.В., Долганова О.И., Славин Б.Б. Цифровой профиль гражданина: мировая практика создания и применения // Информационное общество. 2023. № 2. С. 134–144.

<sup>5</sup> Орлова Е.Р., Голоманчук Э.В. Отдельные вопросы внедрения цифрового профиля гражданина // Труды Института системного анализа Российской академии наук. 2024. Т. 74, № 2. С. 96–105.

<sup>6</sup> Минбалеев А.В. Понятие и правовая природа цифрового профиля человека // Вестник Южно-Уральского государственного университета. Серия: Право. 2022. Т. 22, № 1. С. 113.

Безусловно, темпы развития биометрических персональных данных указывают на перспективу их использования при создании цифрового профиля. Однако следует согласиться с мнением С.С. Кузнецовой и А.Н. Мочалова, которые отмечали, что при всей очевидности преимуществ, появляющихся с введением цифровых профилей, следует обратить внимание и на возникающие в связи с этим конституционно-правовые риски<sup>1</sup>. Разработка нормативных правовых актов должна быть направлена на минимизацию этих рисков.

Е.В. Виноградова, Т.А. Полякова и А.В. Минбалеев обозначили актуальную проблему, которая на сегодняшний день является общей панацеей для всего процесса цифровизации. Они отмечали, что анализ складывающейся практики цифрового профилирования в современном обществе свидетельствует, что правовое регулирование не всегда позволяет успевать за стремительно развивающимися отношениями в данной сфере<sup>2</sup>.

В связи с этим вынуждены согласиться с мнением автора А.В. Остроушко, который отмечал, что на текущий момент реализация концепции цифрового профиля гражданина в Российской Федерации сопровождается большим количеством неразрешенных правовых проблем, связанных с построением архитектуры соответствующего информационно-технологического комплекса, составом и технологиями наполнение профиля данными, обеспечения доступа и безопасности использования и предоставления третьим лицам сведений из него<sup>3</sup>. Однако это не препятствует проведению идентификации граждан с использованием биометрических персональных данных.

Первым государственным органом, использовавшим биометрию для идентификации в целях реализации гражданских прав общества, стал Банк

---

<sup>1</sup> Государственное регулирование Интернета и права человека / М.С. Саликов, С.Э. Несмеянова, Н.Е. Колобаева [и др.]. Екатеринбург: УМЦ УПИ, 2022. С. 77.

<sup>2</sup> Виноградова Е.В. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации / Е.В. Виноградова, Т.А. Полякова, А.В. Минбалеев // Правоприменение. 2021. Т. 5, № 4. С. 11.

<sup>3</sup> Остроушко А.В. Проблемы правового обеспечения процесса внедрения цифрового профиля гражданина // Юридические исследования. 2022. № 5. С. 35.

России. Механизм удаленной идентификации в России позволяет открывать вклады, счета и получать многие другие услуги онлайн<sup>1</sup>.

Изначально любая организация из банковского сектора могла осуществлять сбор и хранение биометрических персональных данных на базе самостоятельно разработанных систем.

Хранение биометрических персональных данных в различных частных системах повышает риски их утечки и несвоевременного установления данного факта, а также создает риски, когда биометрия становится объектом коммерциализации.

Существует негативное отношение к идее создания большой централизованной базы персональных данных<sup>2</sup>. Однако научные дискуссии чаще всего сводились к положениям о пользе централизации сбора, обработки и хранения биометрических персональных данных. Такая позиция отражена в научных работах А.Н. Прокопенко<sup>3</sup>, С.В. Баженова, В.Е. Дивольда, А.А. Морозова<sup>4</sup>, Т.А. Поляковой, И.С. Бойченко<sup>5</sup>. Этой же позиции придерживаются органы публичной власти, что подтверждается информацией, размещенной на сайте Минцифры России, где указано, что централизованное хранение биометрии помогает защитить данные и избежать утечек<sup>6</sup>.

---

<sup>1</sup> Цифровая трансформация экономики и социальной сферы / Г.А. Волкова, О.Н. Суханова, О.В. Ментюкова [и др.] / Актуальные проблемы бухгалтерского учета, аудита и анализа в современных условиях: монография. Пенза: Пензенский государственный аграрный университет, 2023. С. 85.

<sup>2</sup> Денисович В.В., Кудряшов А.В., Перемолотова Л.Ю. Особенности применения современных цифровых технологий в сфере охраны персональных данных // Правопорядок: история, теория, практика. 2024. № 4 (43). С. 102.

<sup>3</sup> Прокопенко А.Н. Борьба с утечками персональных данных – поможет ли ужесточение ответственности? // Вестник Казанского юридического института МВД России. 2024. Т. 15, № 2(56). С. 48–56.

<sup>4</sup> Создание Концепции национальной системы биометрической идентификации личности / С.В. Баженов, В.Е. Дивольд, А.А. Морозов [и др.] // Труды Академии управления МВД России. 2020. № 2(54). С. 41–53.

<sup>5</sup> Полякова Т.А., Бойченко И.С. Особенности взаимодействия и правового обеспечения информационной безопасности в единой биометрической системе в Российской Федерации // Правовая политика и правовая жизнь. 2023. № 3. С. 26–34.

<sup>6</sup> Единая биометрическая система [Электронный ресурс]. – URL: <https://digital.gov.ru/activity/czifrovaya-identifikaciya/edinaya-biometricheskaya-systema> (дата обращения: 21.03.2025).

В целях создания единой безопасной платформы для обращения биометрических персональных данных Центральным банком России совместно с Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации на основании решения правительственной комиссии по информационным технологиям РФ с середины 2016 г. началась активная проработка вопросов, связанных с созданием и эксплуатацией Единой биометрической системы (ЕБС)<sup>1</sup>.

Государственная информационная система Единая биометрическая система (далее – ЕБС) – уникальная система, с помощью которой можно получать услуги с использованием биометрических персональных данных (голоса, лица), в том числе в дистанционном формате<sup>2</sup>.

Оператором системы ЕБС является АО «Центр Биометрических Технологий» (далее – ЦБТ), созданная в соответствии с указом Президента РФ № 693 от 30 сентября 2022 г. и обеспечивающая сбор, хранение, обработку и проверку биометрических персональных данных. Учредителями ЦБТ являются ПАО «Ростелеком», Минцифры и Банк России.

Ключевыми компетенциями компании является разработка, развитие и продвижение цифровых технологий идентификации и аутентификации, а также сервисов подписания и хранения документов, включая создание, развитие и эксплуатацию коммерческих сервисов и типовых решений<sup>3</sup>.

В ЕБС используются две модальности: голос и лицо в их комбинации. На это есть две причины, которые размещены на официальном сайте ЕБС:

- безопасность – по этим модальностям в совокупности можно точно и безопасно идентифицировать человека;

<sup>1</sup> Протасов П.А. Биометрия в банковской системе РФ // Вестник Томского государственного университета. Экономика. 2020. № 49. С. 141.

<sup>2</sup> Единая биометрическая система [Электронный ресурс]. – URL: <https://digital.gov.ru/activity/czifrovaya-identifikacziya/edinaya-biometricheskaya-sistema> (дата обращения: 21.03.2025).

<sup>3</sup> О компании [Электронный ресурс]. – URL: <https://ebs.ru/company/> (дата обращения: 21.03.2025).

- доступность – для снятия биометрии лица и голоса не требуется специальное оборудование, достаточно камеры и микрофона, которыми оснащены большинство ноутбуков и смартфонов<sup>1</sup>.

ЕБС позволила объединить весь массив полученных биометрических персональных данных (фотоизображение и запись голоса) в единую систему. Создание ЕБС стало ключом к разрешению проблемы безопасности предоставляемых данных.

Однако сегодня в банковском секторе, в частности в Сбере, появилась услуга, которая заключается в оплате на кассе посредством улыбки. И как справедливо отмечено О.Б. Сиземовой, сервис «оплата улыбкой» предполагает хранение не только внешности, но и эмоций человека<sup>2</sup>. При этом, если оценить эмоции по выделенным признакам, то их можно отнести к биометрии человека. Законодательно они не признаны биометрией, но используются для идентификации личности.

Таким образом, мы можем говорить, что перечень биологических и физиологических характеристик постоянно пополняется и важно своевременно урегулировать с правовой точки зрения использование новых биометрических характеристик.

Именно в правовом регулировании заключается часть деятельности Центрального банка России как органа публичной власти, обеспечивающего безопасность биометрических персональных данных.

Банком России разработан значительный перечень приказов, указаний, методических рекомендаций по работе с биометрическими персональными данными, в частности и требования к техническим возможностям для аккредитации банковских и кредитных организаций для работы в ЕБС.

---

<sup>1</sup> Какие типы биометрии выбраны для проекта и почему? [Электронный ресурс]. – URL: <https://ebs.ru/faq/project/> (дата обращения: 21.03.2025).

<sup>2</sup> Сиземова О.Б. Правовое регулирование использования технологий искусственного интеллекта в банковской деятельности // Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. № 9(121). С. 137.

Таковыми полномочиями обладает и еще ряд организаций публичной власти – Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Минцифры России) и Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор). При определении функций этих органов публичной власти важно отметить, что Роскомнадзор находится в ведении Минцифры России<sup>1</sup>. Таким образом целесообразно рассмотреть в первую очередь полномочия Минцифры России в области защиты биометрических персональных данных.

Деятельность Минцифры России по обеспечению безопасности биометрических персональных данных осуществляется в рамках действующего законодательства, основу которого составляют Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», постановление Правительства РФ от 30.06.2018 № 772 «Об определении состава сведений, размещаемых в единой биометрической системе, в том числе в ее региональных сегментах»<sup>2</sup>, Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных» и другие, а также в рамках разработанных и утвержденных Министерством нормативных правовых актов (Приказ Минцифры России от 29.11.2023 № 1024, Приказ Минцифры России от 09.10.2023 № 848, Приказ Минцифры России от 27.04.2023 № 43 и другие).

К основным функциям, которые возложены на Минцифры России в рамках методического сопровождения по вопросам реализации мероприятий в целях обеспечения безопасности биометрических персональных данных, относят:

– подготовку и утверждение технических требований, предъявляемых к организациям для прохождения аккредитации с целью получения лицензии на

---

<sup>1</sup> Постановление Правительства РФ от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» // Собрание законодательства Российской Федерации. 2009. № 12. Ст. 1431.

<sup>2</sup> Постановление Правительства РФ от 30 июня 2018 г. № 772 «Об определении состава сведений, размещаемых в единой биометрической системе, в том числе в ее региональных сегментах, а также о внесении изменений в некоторые акты Правительства Российской Федерации» // Собрание законодательства Российской Федерации. 2018. № 28. Ст. 4234.

право использования биометрических персональных данных<sup>1,2</sup>;

– разработку перечня угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации<sup>3</sup>;

– создание методик проверки соответствия предоставленных биометрических персональных данных физического лица соответствующим векторам единой биометрической системы и определении степени взаимного соответствия<sup>4</sup>.

Следующие функции реализуются в рамках контрольно-надзорной деятельности в отношении субъектов, участвующих в сборе, обработке и хранении биометрических персональных данных:

– проведение анализа результатов правоприменительной практики

---

<sup>1</sup> Шипулин А.В., Пархаев А.В. Проблемы нормативного сопровождения цифровой трансформации распознавания и применения биометрических признаков при обеспечении безопасности объектов / Информатизация и техническое обеспечение уголовно-исполнительной системы Российской Федерации: проблемы, решения и перспективы развития: сборник материалов III всероссийской научно-практической конференции, Тверь, 3–4 октября 2024 г. Тверь, 2024. С. 423.

<sup>2</sup> Постановление Правительства РФ от 22 мая 2023 г. № 810 «Об утверждении Правил аккредитации организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, оснований ее приостановления и прекращения и признании утратившим силу постановления Правительства Российской Федерации от 20 октября 2021 г. № 1799» [Электронный ресурс]. – URL: <https://digital.gov.ru/documents/postanovlenie-pravitelstva-rossijskoj-federaczii> (дата обращения 06.04.2025).

<sup>3</sup> Приказ Минцифры России от 5 мая 2023 г. № 446 «Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением организаций финансового рынка, и единой биометрической системы, а также актуальных при взаимодействии информационных систем государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов с указанными информационными системами, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных» [Электронный ресурс]. – URL: <https://digital.gov.ru/documents/prikaz-minczifry-rossii> (дата обращения: 07.04.2025).

<sup>4</sup> Приказ Минцифры России от 17 апреля 2023 г. № 378 «Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица соответствующим векторам единой биометрической системы и определении степени взаимного соответствия биометрических персональных данных и векторов единой биометрической системы, достаточной для проведения идентификации и (или) аутентификации» [Электронный ресурс]. – URL: <https://digital.gov.ru/documents/prikaz-minczifry-rossii-opublikovan-24-05-2023-No-378> (дата обращения: 07.04.2025).

организации и осуществления федерального государственного контроля (надзора) в сфере идентификации и (или) аутентификации (ежегодный доклад)<sup>1</sup>;

- проведение профилактических мероприятий, к которым относятся информирование, обобщение правоприменительной практики, объявление предостережения, консультирование, профилактический визит;

- формирование списка организаций по категориям риска.

Также к функциям Минцифры России относится разработка и координация цифровой структуры:

- утверждение Регламента единой системы идентификации и аутентификации (регламент информационного взаимодействия участников с оператором ЕСИА и оператором эксплуатации инфраструктуры электронного правительства),

- разработка Методических рекомендаций по использованию ЕСИА;

- разработка Методических рекомендаций по интеграции с REST API Цифрового профиля;

- подготовка сценария использования инфраструктуры Цифрового профиля<sup>2</sup>.

Также Минцифрой России проводится работа по технологическому поиску решений вопросов обеспечения защиты биометрических персональных данных, однако исследование данного вопроса не является целью данной диссертации.

При этом отметим, что Минцифры России обладает правом привлекать к ответственности за нарушение установленных правовых норм. Это выражается в блокировке систем, представляющих угрозу обрабатываемым биометрическим персональным данным, лишении лицензии операторов единой биометрической системы, допустивших неправомерные действия, а также в подготовке

---

<sup>1</sup> Приказ Минцифры России от 6 марта 2025 г. № 150 «Об утверждении доклада о правоприменительной практике организации и осуществления федерального государственного контроля (надзора) в сфере идентификации и (или) аутентификации в 2024 году» [Электронный ресурс]. – URL: <https://digital.gov.ru/documents/prikaz-minczifry-rossii-opublikovan-24-05-2023-№-378> (дата обращения: 09.04.2025).

<sup>2</sup> Регламент информационного взаимодействия ЕСИА [Электронный ресурс]. – URL: <https://digital.gov.ru/documents/reglament-informacionnogo-vzaimodejstviya-esia> (дата обращения: 09.04.2025).

необходимых материалов для передачи в правоохранительные органы для привлечения в соответствии с действующим законодательством к необходимому виду ответственности.

В связи с этим отметим, что Минцифры России осуществляет колоссальное взаимодействие с иными органами публичной власти в рамках сбора, обработки и хранения биометрических персональных данных. Взаимодействие охватывает несколько целей одновременно: использование биометрии в качестве объекта для обеспечения безопасности государства; проведение мероприятий по защите самих биологических и физиологических характеристик человека. Этим принципом обусловлена специфика взаимодействия с другими органами. Наиболее частое взаимодействие осуществляется с ФСБ России, МВД России, Центральным банком Российской Федерации, Роскомнадзором России.

Такой перечень органов публичной власти позволяет реализовывать широкий спектр правоотношений, нацеленных на обеспечение безопасности биометрии. Так, Минцифры России совместно с Роскомнадзором России осуществляет взаимодействие по надзору за обработкой биометрических персональных данных, с МВД России проводится работа по противодействию неправомерных действий в отношении биометрии, с Банком России по использованию Единой биометрической системы.

Подводя итог анализу деятельности Минцифры России, можно отметить, что совокупность функций в области защиты биометрических персональных данных является достаточно всеобъемлющей. Перед Минцифры России стоят задачи по совершенствованию правовых норм, технических требований, осуществлению надзора. Одной из перспективных задач для Минцифры России должно стать правовое регулирование понятия «цифровой профиль». На государственном уровне важно стратегически определить, что представляет собой «цифровой профиль», основные направления развития цифрового профилирования, вызовы и риски, а также развитие профилирования в рамках единой системы публичной власти<sup>1</sup>.

---

<sup>1</sup> Виноградова Е.В., Полякова Т.А., Минбалева А.В. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации // Правоприменение. 2021. Т. 5, № 4. С. 14.

Следующим органом публичной власти, чья деятельность направлена на обеспечение безопасности биометрических персональных данных, является Роскомнадзор. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных<sup>1</sup>.

Нормативная правовая база, регулирующая деятельность Роскомнадзора в области биометрии, представлена Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных», Приказом Минцифры России от 12.05.2023 № 453 «О порядке обработки биометрических персональных данных и векторов единой биометрической системы в единой биометрической системе и в информационных системах аккредитованных государственных органов, Центрального банка Российской Федерации в случае прохождения им аккредитации, организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц», Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24 февраля 2021 г. № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения».

Основные направления деятельности Роскомнадзора закреплены постановлением Правительства РФ от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций». Данные направления можно разделить на три группы: методическое руководство, контрольно-надзорная деятельность, регистрация и учет операторов, обрабатывающих биометрические данные.

---

<sup>1</sup> Постановление Правительства РФ от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» // Собрание законодательства Российской Федерации. 2009. № 12. Ст. 1431.

Методическая функция Роскомнадзора выражается в размещении на официальном сайте разъяснений требований законодательства для граждан и операторов ЕБС, разработка рекомендаций по защите биометрических персональных данных. Эта функция объединяет Роскомнадзор с Минцифры России, дублируя зачастую их полномочия, и направлена в большей степени на профилактику правонарушений в исследуемой области. Согласно данным Отчета о выполнении Плана и показателей деятельности Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций за 2023 год<sup>1</sup>, больше всего профилактических мероприятий проведено в области государственного контроля за обработкой персональных данных (61 % от всех профилактических мероприятий).

Степень достаточности принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах оценивается во время проведения государственного контроля и надзора<sup>2</sup>. Контрольно-надзорная функция – основная в деятельности Роскомнадзора<sup>3</sup>. Она подразумевает под собой проведение плановых и внеплановых проверок операторов ЕБС. В рамках проверок осуществляется анализ по соблюдению законодательства в области реализации мер по защите биометрических персональных данных, как правового, так и технического характера.

По итогам деятельности с 1 января по 31 декабря 2023 года территориальными органами Роскомнадзора: проведены 16 425 мероприятий государственного контроля (надзора), из них: 2 плановых мероприятия и 235 внеплановых мероприятий государственного контроля (надзора) во взаимодействии с проверяемыми лицами, 11 849 плановых и 4 339 внеплановых

---

<sup>1</sup> Отчет о выполнении Плана и показателей деятельности Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций за 2023 год [Электронный ресурс]. – URL: <https://digital.gov.ru/documents/reglament-informacionnogo-vzaimodejstviya-esia> (дата обращения: 13.04.2025).

<sup>2</sup> Правовая защита информации: учебное пособие / А.И. Антипов, Д.Е. Дробов, Н.М. Крамаренко [и др.]. СПб.: СПбУ МВД России, 2024. 229 с.

<sup>3</sup> Организационное и правовое обеспечение информационной безопасности: учебник / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов. – 2-е изд., перераб. и доп. М.: Юрайт, 2025. С. 254.

мероприятий государственного контроля (надзора) без взаимодействия с проверяемыми лицами. По результатам мероприятий госконтроля выявлено 17 228 нарушений обязательных требований законодательства Российской Федерации, выдано 560 предписаний об устранении выявленных нарушений, составлено в рамках мероприятий госконтроля 2 073 протокола об административных правонарушениях (всего составлено 41 683 протокола), вынесено 58 предупреждений о приостановлении действия лицензий, вынесено 22 548 постановлений о привлечении к административной ответственности, наложено административных штрафов на сумму более 240 млн рублей<sup>1</sup>.

Отчет Роскомнадзора не выделяет из общего числа персональных данных результаты своей деятельности по обеспечению безопасности биометрических данных. Это негативно сказывается на восприятии гражданами использования таких данных<sup>2</sup>. Отсутствие объективного анализа по использованию биометрии, восстановлению утраченных прав в ее отношении создает информационный вакуум. В связи с чем Роскомнадзору необходимо более детально освещать свою деятельность с биометрическими персональными данными.

Третья функция Роскомнадзора в деятельности с биометрией выражается в регистрации и учете операторов, обрабатывающих биометрические данные. Так, на Роскомнадзор возложены обязанности по ведению реестра операторов, обрабатывающих биометрические данные, регистрации уведомлений об обработке персональных данных и присвоению категорий значимости информационных систем.

Как контрольно-ревизионный орган Роскомнадзор обладает правом привлекать к административной ответственности правонарушителей за совершение неправомерных действий в области обеспечения безопасности биометрических персональных данных. Довольно подробно об этом изложено в

---

<sup>1</sup> Отчет о выполнении Плана и показателей деятельности Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций за 2023 год [Электронный ресурс]. – URL: <https://digital.gov.ru/documents/> (дата обращения: 13.04.2025).

<sup>2</sup> Бурлака С.Н., Бельдина О.Г. Защита биометрических персональных данных: проблемы правового регулирования // Право и государство: теория и практика. 2023. № 10(226). С. 279.

Письме Роскомнадзора от 31.01.2023 № 09-6488 «Об особенностях возбуждения Роскомнадзором дел об административных правонарушениях без проведения КНМ во взаимодействии с контролируемым лицом»<sup>1</sup>.

В соответствии с частью 3.1 статьи 28.1 КоАП РФ дело об административном правонарушении, выражающееся в нарушении обязательных требований, оценка соблюдения которых является объектом государственного контроля (надзора) или муниципального контроля, при наличии одного из оснований, предусмотренных п. 1–3 ч. 1 статьи 28.1 КоАП РФ, может быть возбуждено исключительно после проведения контрольного (надзорного) мероприятия в сотрудничестве с контролируемым лицом проверки или контрольного (надзорного) действия в рамках постоянного государственного контроля (надзора) или постоянного рейда, а также оформления результатов данных мероприятий. Исключения из этого правила предусмотрены ч. 3.2–3.5 статьи 28.1 и статьей 28.6 КоАП РФ.

Частью 3.5 статьи 28.1 КоАП РФ установлен перечень статей КоАП РФ, по которым Роскомнадзор вправе возбуждать дела об административных правонарушениях без проведения контрольных (надзорных) мероприятий во взаимодействии с контролируемым лицом.

Проведение Роскомнадзором контрольных (надзорных) мероприятий в целях возбуждения дел об административных правонарушениях, установленных Перечнем, при наличии одного из предусмотренных пунктами 1–3 части 1 статьи 28.1 КоАП РФ поводов к возбуждению дела об административном правонарушении, не требуется<sup>2</sup>.

Роскомнадзор, публикуя свои отчеты за год, не предусматривает выделения биометрии из общей совокупности персональных данных. Однако с вступлением

---

<sup>1</sup> Письмо Роскомнадзора от 31.01.2023 № 09-6488 «Об особенностях возбуждения Роскомнадзором дел об административных правонарушениях без проведения КНМ во взаимодействии с контролируемым лицом» [Электронный ресурс]. – URL: <https://legalacts.ru/doc/> (дата обращения: 16.04.2025).

<sup>2</sup> Письмо Роскомнадзора от 31.01.2023 № 09-6488 «Об особенностях возбуждения Роскомнадзором дел об административных правонарушениях без проведения КНМ во взаимодействии с контролируемым лицом» [Электронный ресурс]. – URL: <https://legalacts.ru/doc/> (дата обращения: 16.04.2025).

в законную силу, принятых в ноябре 2024 года поправок в КоАП РФ в отношении биометрических персональных данных<sup>1</sup>, в ближайшие несколько лет количество возбужденных дел по новым составам позволит провести анализ эффективности деятельности Роскомнадзора в данной области.

Таким образом, Роскомнадзор продолжает работу Минцифры России в области обеспечения защиты биометрических персональных данных. Если Минцифры России выступает как «законодатель», то Роскомнадзор осуществляет контроль исполнения принятых нормативных правовых актов. Как отмечали А.А. Затолокин и В.В. Стрельцов, в полномочия сотрудников Роскомнадзора входит внушительный перечень мер государственного реагирования, среди которых и проведение проверок (плановых, внеплановых, контрольных), и осуществление иных контрольных (надзорных) мероприятий, и административно-юрисдикционная деятельность<sup>2</sup>.

Рассмотренные органы публичной власти, осуществляющие защиту биометрических персональных данных, являются регуляторами правовых отношений в гражданской области правоприменения. В данном случае идентификация осуществляется в интересах гражданина для упрощения получения государственных услуг. Сдача биометрии является добровольной.

Однако в системе органов власти есть случаи, когда сдача биометрии является обязанностью. Это характерно для деятельности правоохранительных органов<sup>3</sup>. Назначение правоохранительной деятельности – охрана и защита прав и законных интересов граждан, юридических лиц и государства и обеспечение

---

<sup>1</sup> Федеральный закон от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» [Электронный ресурс]. – URL: <http://publication.pravo.gov.ru/document/0001202411300011> (дата обращения: 11.03.2025).

<sup>2</sup> Затолокин А.А., Стрельцов В.В. Административно-правовые аспекты государственного регулирования обработки биометрических персональных данных // Общество и право. 2023. № 1(83). С. 80.

<sup>3</sup> Митянов З.О. Принудительная и добровольная биометрия: содержание и разграничение в российском праве // Теоретическая и прикладная юриспруденция. 2024. № 3 (21). С. 68.

выполнения ими своих обязанностей<sup>1</sup>. К правоохранительным органам относятся МВД России, ФСБ России, Следственный Комитет России и другие<sup>2</sup>.

Данные органы обладают своей спецификой, однако объединены общей целью – обеспечение безопасности. Перечень правоохранительных органов достаточно велик, и их деятельность по обеспечению защиты биометрических персональных данных заслуживает отдельного исследования. Мы же рассмотрим деятельность МВД России в обеспечении защиты биометрических персональных данных, как одного из активных участников по сбору, обработке и хранению биометрической информации.

Правовое регулирование в системе МВД России по защите биометрических персональных данных включает в себя основные нормативные правовые акты, которые были упомянуты ранее. Однако в большей степени они регулируют гражданскую сферу правоотношений и нацелены на сбор двух видов биометрических персональных данных – записи голоса человека и фотоизображения.

Однако в МВД России кроме этого перечня используются базы данных, содержащие геномную информацию и дактилоскопию. Указом Президента РФ от 21 декабря 2016 г. № 699 «Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации»<sup>3</sup> закреплены полномочия территориальных органов по проведению государственной дактилоскопической регистрации и государственной геномной регистрации. Данные виды регулируются индивидуальными правовыми нормами (Федеральный закон от 03.12.2008 № 242-ФЗ

---

<sup>1</sup> Правоохранительные органы России: учебник / Б.Я. Гаврилов, Е.А. Бархатова, А.Ю. Винокуров [и др.]. – 7-е изд., пер. и доп. М.: Юрайт, 2023. С. 12.

<sup>2</sup> Правоохранительные органы: учебник / под общ. ред. М.П. Полякова. – 3-е изд., перераб. и доп. М.: Юрайт, 2025. С. 204.

<sup>3</sup> Указ Президента РФ от 21 декабря 2016 г. № 699 «Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 52 (часть V). Ст. 7614.

«О государственной геномной регистрации в Российской Федерации» и Федеральный закон от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации»).

В отличие от Роскомнадзора МВД России на сегодняшний день уже активно выделяет биометрию в отдельную категорию. На самом высоком государственном уровне обсуждается эффективность ее использования. Так, на расширенном заседании коллегии МВД России 2024 года с участием Президента Российской Федерации В.В. Путина Министр внутренних дел Российской Федерации генерал полиции В.А. Колокольцев доложил, что с помощью биометрических персональных данных раскрыто практически 2,5 тысячи преступлений, которые были совершены гражданами других государств<sup>1</sup>.

Это говорит об открытости данных и построении системы доверительного отношения граждан к использованию биометрических характеристик человека. К.М. Бондарь, В.С. Дунин, А.В. Кантышева утверждают, что цифровые технологии позволяют не только улучшить взаимодействие с населением, но и повысить эффективность работы полиции по профилактике и раскрытию преступлений, предоставить значительные возможности по сбору и фиксации ориентирующей и процессуальной информации<sup>2</sup>.

Однако при исследовании полномочий МВД России в области защиты биометрических персональных данных установлено, что Министерство не обладает правом рассмотрения административных правонарушений, связанных с биометрией, а может только в рамках взаимодействия передать сведения о правонарушении в Роскомнадзор для дальнейшего принятия решения.

С этой позицией нам согласиться трудно, так как, по нашему мнению, МВД России современный орган публичной власти, обладающий правовыми

<sup>1</sup> Письмо Роскомнадзора от 31.01.2023 № 09-6488 «Об особенностях возбуждения Роскомнадзором дел об административных правонарушениях без проведения КНМ во взаимодействии с контролируемым лицом» [Электронный ресурс]. – URL: <https://legalacts.ru/doc/pismo-roskomnadzora-ot-31012023-n-09-6488-ob-osobennostjakh-vozbuzhdenija/> (дата обращения 16.04.2025).

<sup>2</sup> Бондарь К.М., Дунин В.С., Кантышева А.В. Современные цифровые технологии для корректирования социального взаимодействия населения с сотрудниками и обучающимися правоохранительных органов // Мир науки, культуры, образования. 2024. № 6(109). С. 72.

знаниями и техническими возможностями для рассмотрения административных дел, связанных с нарушением прав граждан в области биометрических персональных данных. В связи с этим целесообразно наделение МВД России соответствующими полномочиями.

Рассмотрение позиции защиты биометрических персональных данных с участием органов публичной власти обозначило ряд проблем, требующих своего разрешения. Одна из наиболее важных – правовое регулирование. Многими учеными освещалась актуальность совершенствования законодательства в области биометрии, например, С.Н. Бурлакой, О.Г. Бельдиной<sup>1</sup> Е.В. Виноградовой, Т.А. Поляковой, А.В. Минбалеевым<sup>2</sup> и другими.

При наличии значительного перечня органов публичной власти, осуществляющих защиту биометрических персональных данных, нет полного перечня данных, которые относятся к биометрии. Практически каждый орган формировал свои методические материалы, где указывал свой список биологических и физиологических характеристик<sup>3,4</sup>. При этом в эти перечни часто включали биометрию, которая не нашла своего административно-правового регулирования ни в одном нормативном правовом акте (например, походка, геометрия кисти рук, вес, рост и т.д.).

Также необходимо исключить дублирование полномочий органами публичной власти, регулирующими правоотношения в области биометрических персональных данных. При этом важно обеспечить эффективность работы

---

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> Письмо Министерства цифрового развития, связи и массовых коммуникаций РФ от 28.08.2020 № ЛБ-С-074-24059 «О методических рекомендациях» (вместе с Методическими рекомендациями для общеобразовательных организаций по вопросам обработки персональных данных) [Электронный ресурс]. – URL: <https://www.garant.ru/products/ipo/prime/doc/74485566/>.

<sup>4</sup> Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций разъясняет вопросы отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки [Электронный ресурс]. – URL: <https://25.rkn.gov.ru/news/news54167.htm> (дата обращения 13.05.2025).

системы взаимодействия<sup>1</sup>. Для этого необходимо создание единой системы, в которой хранился весь объем биометрических характеристик, а доступ к ним предоставлялся органам публичной власти в соответствии с их полномочиями.

Вместе с тем подобное увеличение возможных пользователей единой системой биометрических персональных данных требует разработки жестких условий по обеспечению безопасности при работе с данными. Одной из проблем может стать этическая сторона сотрудников органов публичной власти<sup>2</sup>. Важно с их стороны совершенствование своих правовых знаний, соблюдение действующего законодательства, недопустимость утечек биометрии по халатности либо преступному умыслу. В связи с этим необходимо проводить контрольно-надзорную деятельность не только организаций подведомственных, но и собственного коллектива.

В исследовании мы не раз обращали внимание на отсутствие статистики в отношении использования биометрических персональных данных. В современных условиях стоит признать обособленность биометрии в общей совокупности персональных данных, выделить в отдельную категорию, использовать при формировании отчетов о деятельности.

Существующие проблемы межведомственного взаимодействия снижают эффективность защиты биометрических данных и требуют системных мер по совершенствованию координации между органами власти. Ключевое направление – создание единого правового и организационного пространства для работы с биометрией при сохранении специализации ведомств.

Подводя итог исследованию в рамках данного параграфа, можем сделать следующие выводы.

1. Под системой органов публичной власти, осуществляющих защиту биометрических персональных данных, предлагаем закрепить совокупность всех

---

<sup>1</sup> Петрова Д.А., Папкина В.А. Обработка биометрических персональных данных в свете изменения законодательства // Правовая политика и правовая жизнь. 2024. № 3. С. 330.

<sup>2</sup> Михайлов М.А., Кокодей Т.А. Организационные, правовые и этические аспекты получения, хранения и использования биометрической информации в целях всеобщей регистрации населения // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2022. Т. 8 (74), № 4. С. 345.

уровней органов публичной власти (федеральных, субъектов Российской Федерации, местных) и организаций, осуществляющих взаимодействие по сбору, обработке и хранению биометрических персональных данных в установленных действующим законодательствах целях, и реализующих меры по обеспечению правовой и технической безопасности полученных данных с соблюдением этических норм в отношении полученных данных.

Каждый из упомянутых органов выполняет специфические функции, необходимые для обеспечения эффективной работы комплексной системы, направленной на реализацию государственных задач по разработке правовых и технических мер противодействия нарушениям в области защиты биометрических персональных данных. В условиях динамично развивающихся общественных отношений государство сталкивается с необходимостью оперативного реагирования на возникающие вызовы и проблемы.

2. Систему органов публичной власти, ответственных за защиту биометрических персональных данных в Российской Федерации, целесообразно структурировать по характеризующим специфическим критериям:

I. Территориальность уровней управления (федеральный уровень, региональный уровень, местный уровень);

II. Цель сбора, обработки и хранения биометрических персональных данных (органы и организации, осуществляющие сбор, обработку и хранение биометрических персональных данных в рамках гражданских правоотношений; органы и организации, обеспечивающие сбор, обработку и хранение биометрических данных в целях обеспечения национальной безопасности и общественного порядка)

III. Направление деятельности органов публичной власти в сфере защиты биометрических персональных данных (законодательные органы и органы публичной власти).

3. Роскомнадзор представляет собой федеральный орган публичной власти Российской Федерации, наделенный полномочиями по осуществлению государственного контроля и надзора за соблюдением законодательства в области

биометрических персональных данных. Основной задачей данного ведомства является обеспечение соответствия процедур обработки биометрических персональных данных установленным правовым нормам и регламентам, что способствует защите прав и свобод субъектов биометрии, а также поддержанию законности и правопорядка в сфере защиты информации.

4. В результате анализа нормативно-правовой базы, регулирующей деятельность МВД России в сфере защиты биометрических персональных данных, было установлено, что оно не наделено полномочиями по самостоятельному рассмотрению административных правонарушений, связанных с нарушением законодательства в области биометрии. Вместо этого МВД России может лишь в рамках межведомственного взаимодействия передавать информацию о выявленных нарушениях в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) для дальнейшего принятия соответствующих мер.

Данная позиция вызывает определенные сомнения, поскольку представляется, что МВД России, как современный орган государственной власти, обладающий значительным объемом правовых знаний и высоким уровнем технической оснащенности, вполне способен осуществлять функции по рассмотрению административных дел, связанных с нарушением прав граждан на защиту биометрических персональных данных. Учитывая это, представляется целесообразным рассмотреть возможность наделения МВД России соответствующими полномочиями, что позволит более эффективно обеспечивать соблюдение законодательства в данной сфере и оперативно реагировать на правонарушения.

## **§ 2. Меры административно-правовой защиты биометрических персональных данных**

Стремительные процессы цифровой трансформации общественных отношений и сопутствующее развитие дистанционных сервисов и услуг требуют комплекса соответствующих правовых, технологических и методологических

решений по развитию инфраструктуры идентификации<sup>1</sup>. Государство должно предпринять максимально широкий комплекс мер, направленных на создание качественных цифровых условий, способствующих росту доверия населения к государству и понимания своей защищенности<sup>2</sup>.

Анализ научной литературы показал, что исследование мер административно-правовой защиты биометрических персональных данных на сегодняшний день весьма актуально. Данная тематика освещалась в работах А.А. Затолокина, В.В. Стрельцова<sup>3</sup>, М.А. Желудкова, А.Н. Варыгина<sup>4</sup>, М.А. Егоровой<sup>5</sup> и других авторов. Однако, предлагая конкретные меры, авторы не приводили понятия мер административно-правовой защиты биометрических персональных данных.

Отсутствует такое определение и в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных». При этом статья 19 вышеприведенного нормативного правового акта посвящена именно мерам по обеспечению безопасности персональных данных при их обработке. При формировании перечня мер биометрию не выделяют в отдельную категорию, а по умолчанию относят условно ко всей совокупности персональных данных.

Однако в современных условиях важным является формирование методологической основы использования биометрических персональных данных. В связи с чем считаем необходимым разработку понятия «меры административно-

---

<sup>1</sup> Химченко А.И. Формирование цифровой среды доверия: динамика развития инфраструктуры идентификации при реализации цифровых услуг // Вестник Университета имени О.Е. Кутафина (МГЮА). 2023. № 2(102). С. 108.

<sup>2</sup> Казанцева Н.Г. Цифровизация государственного управления и права человека / Мировые научные дискуссии в эпоху цифровизации: от теории к практике: материалы XVI Международной научно-практической конференции, Рязань, 29 декабря 2023 г. Рязань: Концепция, 2023. С. 377.

<sup>3</sup> Затолокин А.А., Стрельцов В.В. Административно-правовые аспекты государственного регулирования обработки биометрических персональных данных // Общество и право. 2023. № 1(83). С. 79–83.

<sup>4</sup> 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.

<sup>5</sup> Егорова М.А. Проблема цифровой идентификации личности в Российской Федерации и Европейском Союзе // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 1(89). С. 17–29.

правовой защиты биометрических персональных данных». Актуальность данного определения обусловлена возможностью его использования в действующем законодательстве в целях совершенствования регулирования правовых отношений в исследуемой области.

При формировании понятия «меры административно-правовой защиты биометрических персональных данных» обратимся к традиционному приему формальной логики. Для это выделим признаки исследуемого явления, расположив их в логической последовательности.

В основу понятия «меры административно-правовой защиты биометрических персональных данных» заложено определение административно-правовой защиты. Данное определение тщательно и всесторонне исследовано в диссертационном исследовании О.А. Дизера<sup>1</sup>. Автор разграничил понятия «защиты» и «охраны». Для нашего определения применимо употребление термина «защита».

Ценным является определение «правовой защиты», предложенное И.А. Минникесом. Под правовой защитой автор определяет основанную на нормах действующего законодательства, осуществляемую с помощью правовых средств деятельность государства, специально уполномоченного органа, должностного лица либо самого человека, направленную на защиту и охрану основных прав и свобод личности<sup>2</sup>. Данная позиция соответствует тому факту, что правовая защита биометрических персональных данных – это уникальное широкое социальное явление, которое зависит не только от государства, но и целого ряда участников, в том числе и от самих граждан.

В продолжение этого утверждения приведем выделенные Ф.М. Рудинским, Ю.В. Гавриловой, А.А. Крикуновой и Т.А. Сошниковой правовые механизмы, использующие свои формы и методы деятельности в правовой защите:

---

<sup>1</sup> См.: Дизер О.А. Административно-правовая защита общественной нравственности: дис ... д-ра юрид. наук. Омск, 2019. 475 с.

<sup>2</sup> Минникес И.А. Правовая защита: понятие и механизм // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). 2013. № 6. С. 15.

- государственный механизм, представленный органами власти Российской Федерации и субъектов;
- механизм публичной власти муниципального образования (органов местного самоуправления);
- механизм защиты со стороны общественных объединений;
- социально-партнерский механизм защиты;
- механизм самозащиты<sup>1</sup>.

Особенность правовой защиты биометрических персональных данных заключается в построении такой системы защиты, где все пять перечисленных механизмов будут представлять собой единую совокупность.

Таким образом, опираясь на приведенные положения, мы можем выделить следующие признаки административно-правовой защиты биометрических персональных данных:

- 1) меры административно-правовой защиты являются инструментом реализации прав граждан на защиту биометрических персональных данных;
- 2) меры административно-правовой защиты регламентированы действующим законодательством и морально-этическими нормами;
- 3) меры по административно-правовой защите биометрии осуществляются широким перечнем участников (органами публичной власти, организациями, осуществляющими сбор, обработку и хранение биометрических характеристик, индивидуальными предпринимателями, а также лично субъектом биометрических персональных данных);
- 4) меры административно-правовой защиты биометрических персональных данных включают в себя меры организационного и принудительного характера.

Исходя из приведенных признаков, предлагаем понимать под мерами административно-правовой защиты биометрических персональных данных совокупность административно-правовых мер, в том числе организационного и принудительного характера, применяемых органами публичной власти и иными

---

<sup>1</sup> См.: Экономические и социальные права человека и гражданина: современные проблемы теории и практики / Ф.М. Рудинский, Ю.В. Гаврилова, А.А. Крикунова, Т.А. Сошникова. М.: Права человека, 2009. 495 с.

участниками правовых отношений в области защиты биометрических персональных данных, направленных на нейтрализацию и устранение угроз в данной области, а также предусматривающие юрисдикционную деятельность в сфере защиты биометрии.

Анализ имеющейся научной литературы показал, что учеными ранее не предпринимались попытки комплексного выделения мер по защите биометрических персональных данных. Данные меры освещались обычно только с одной стороны, либо с правовой (Р.А. Равоян<sup>1</sup>, Н.И. Платонова, А.Ю. Соловьева-Опошнянская<sup>2</sup>, Р.Н. Данелян, В.А. Яковлев-Чернышев<sup>3</sup> и другие), либо с технической (Ю.Н. Семенов, В.И. Кабаров, А.Р.М. Кассу<sup>4</sup>, А.М. Трошков, М.А. Трошков, Д.В. Шлаев<sup>5</sup> и другие).

Однако последние научные труды показывают, что сейчас ученые юридических и технических наук объединяются, что способствует совершенствованию мер защиты биометрических персональных данных. Например, вопросы обеспечения безопасности биометрических персональных данных в информационных системах персональных данных изложены в совместном труде к.ю.н. Е.А. Овчинникова и к.тех.н. Г.В. Попкова<sup>6</sup>.

---

<sup>1</sup> Равоян Р.А. Правовое регулирование защиты персональных и биометрических данных в условиях цифровизации // Юридическая наука. 2023. № 5. С. 83–86.

<sup>2</sup> Платонова Н.И. Соловьева-Опошнянская А.Ю. Биометрические персональные данные: возможности и проблемы // Юрист. 2019. № 6. С. 63–67.

<sup>3</sup> Данелян Р.Н., Яковлев-Чернышев В.А. Особенности правового регулирования биометрических персональных данных в Российской Федерации // Вестник Казанского юридического института МВД России. 2024. Т. 15, № 3(57). С. 26–33.

<sup>4</sup> Семенов Ю.Н., Кабаров В.И., Кассу А.Р.М. Функциональные и технические требования к платформе мультимодальных биометрических решений (регистрация, хранение, идентификация/верификация, обработка и аналитика) / Альманах научных работ молодых ученых университета ИТМО: XLVII научная и учебно-методическая конференция, Санкт-Петербург, 31 января – 3 февраля 2018 г. Т. 2. СПб., 2018. С. 188–191.

<sup>5</sup> Проектирование модели цифровой обработки биометрических характеристик человека / А.М. Трошков, М.А. Трошков, Д.В. Шлаев [и др.] // Вестник АПК Ставрополья. 2017. № 1(25). С. 57–62.

<sup>6</sup> Овчинникова Е.А., Попков Г.В. К вопросу об обеспечении безопасности биометрических персональных данных в информационных системах персональных данных // Телекоммуникации. 2025. № 1. С. 36–40.

Такой консенсус ученых разных областей способен выстроить действенную систему мер защиты биометрических персональных данных. Также эффективность будет зависеть и от признания и разработки иных инновационных мер.

Актуальность исследования мер административно-правовой защиты биометрических персональных данных безусловна. М.А. Желудков и А.Н. Варыгин отмечали, что «правовые, технические, организационные и информационные формы обеспечения реализации биометрических персональных данных имеют существенный момент опоздания в своем развитии, в том числе вследствие недооценки угрозы преступного характера и недостаточного уровня развития системы понятий и приемов решения поставленных задач в исследуемой области общественных отношений»<sup>1</sup>.

Как мы можем отметить, М.А. Желудков и А.Н. Варыгин выделили правовые, технические, организационные и информационные меры.

В статье 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» указаны правовые, организационные и технические меры в рамках административно-правовой защиты.

Однако обе эти позиции не отражают ряда специальных мер, которые уже применяются на практике, но не нашли своего отражения ни в правовой, ни в научной сферах. В связи с чем в рамках нашего исследования мы предлагаем выделить две группы мер административно-правовой защиты биометрических персональных данных: общие и специальные.

Для общих мер административно-правовой защиты характерным является государственно-властный характер. Данные меры регламентируются законодательно и осуществляются в условиях государственной политики по цифровизации общества. К таким мерам, по нашему мнению, целесообразно отнести методологические, правовые, организационные и технические меры.

---

<sup>1</sup> 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. 178.

## I. Методологические меры административно-правовой защиты.

Представляя собой достаточно новое социальное явление, биометрические персональные данные имеют малоизученный понятийный, методологический аппарат. В первом параграфе нами обозначалась проблема несовершенства действующего определения биометрических персональных данных, отсутствия полного перечня таких данных. Соответственно и методы по защите биометрии сформированы в настоящий момент в недостаточном характере. В научном сообществе нет однозначного мнения в вопросе, стоит ли выделять биометрические персональные данные в отдельную категорию, в то время как на законодательном уровне идет процесс, когда меры административной ответственности устанавливаются в отношении биометрии в отдельных статьях.

Таким образом, перед учеными стоит задача сформулировать современный понятийный аппарат в области биометрических персональных данных, выработать методы по обеспечению их защиты. Полученный результат должен стать прочной основой для формирования правового регулирования административно-правовой защиты биометрических персональных данных, обеспечив практическое применение научных изысканий.

## II. Правовые меры административно-правовой защиты биометрических персональных данных.

Безусловно, данная группа мер представляет собой один из наиболее значимых для общества пунктов по защите биометрических персональных данных. Не случайно Э.И. Лескина отмечала, что развитие цифровых технологий зависит в том числе от условий, которые создаются нормативной средой<sup>1</sup>. Основной задачей современного российского государства является создание наиболее благоприятных условий для реализации прав и свобод его граждан<sup>2</sup>.

Активное принятие в последние годы значительного количества нормативных правовых актов в области биометрических персональных данных

---

<sup>1</sup> Лескина Э.И. Характеристика отдельных правовых режимов больших данных (Big Data) // Теоретическая и прикладная юриспруденция. 2025. № 1(23). С. 113.

<sup>2</sup> Мазурин С.Ф., Прокофьев К.Г. Административное право: учебное пособие / под общ. ред. В.П. Сальникова. СПб.: Фонд «Университет», 2019. С. 15.

создает положительную тенденцию в формировании правового поля по защите биометрии.

Однако стоит отметить мнение авторов А.Г. Безверхова и А.В. Юдина, которые небезосновательно отмечали, что «биометрия» и «право» находятся только в начале пути по взаимодействию друг с другом. Пока отсутствует какое-либо комплексное и специальное регулирование складывающихся здесь отношений. Одна из современных задач – сделать так, чтобы отношения, складывающиеся применительно к биометрическим персональным данным, стали правоотношениями с четко определенным кругом взаимных прав и обязанностей их участников<sup>1</sup>.

Данную позицию подтверждает тот факт, что многие авторы при рассмотрении мер административно-правовой защиты биометрических персональных данных ссылаются только на нормы Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных», а также на Кодекс РФ об административных правонарушениях. Это утверждение принадлежит ряду ученых, например, А.А. Затолокину, В.В. Стрельцову<sup>2</sup>, С.Н. Бурлаке, О.Г. Бельдину<sup>3</sup> и другим.

Однако мы считаем эту позицию несовершенной. Возвращаясь к вопросу о системе мер административно-правового регулирования защиты биометрических персональных данных, мы обозначали, что нормативных правовых актов в данной сфере значительно больше, и каждый из них включает в себе регулирование определенной области (технической, организационной, правовой). Также указанные выше акты не являются исчерпывающими по отношению ко всему перечню утвержденных правом биометрических

---

<sup>1</sup> Безверхов А.Г., Юдин А.В. Биометрия и право: вопросы теории и права // Юридический вестник Самарского университета. 2021. Т. 7, № 1. С. 9.

<sup>2</sup> Затолокин А.А., Стрельцов В.В. Административно-правовые аспекты государственного регулирования обработки биометрических персональных данных // Общество и право. 2023. № 1(83). С. 79–83.

<sup>3</sup> 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.

персональных данных. Так, в стороне остаются вопросы по защите таких биометрических характеристик, как дактилоскопия и геномная информация, регулирующиеся отдельными нормативными правовыми актами.

В связи с этим считаем целесообразным при формировании мер административно-правовой защиты биометрических персональных данных опираться на весь имеющийся массив нормативных правовых актов, регулирующих правоотношения в данной области.

Несмотря на развитую нормативную базу, система защиты биометрических данных в России сталкивается с рядом проблем, которые снижают ее эффективность.

Во-первых, недостаточно детализированное управление. Часто законы устанавливают общие требования, в которых отсутствуют четкие предписания. Это негативно сказывается на понимании субъектами правоотношений, связанных с биометрическими персональными данными, устанавливающих норм, что в свою очередь может привести к утрате конфиденциальности полученных данных.

Во-вторых, в настоящее время отсутствует правовое регулирование технологических стандартов для отдельных видов биометрии. В стороне остаются биометрические персональные данные, которые подлежат сбору в мировой практике, однако не используются для идентификации в России.

В-третьих, гражданами отмечается мягкость принимаемых санкций при совершении административных правонарушений в области защиты биометрических персональных данных. По результатам проведенного в рамках диссертационного исследования опроса установлено, что, по мнению 75 % опрошенных, штрафные санкции недостаточны. Такого мнения придерживаются и ученые. Е.А. Свиридова отмечала, что увеличение мер административной ответственности операторов персональных данных будет выступать своего рода превентивной мерой и способствовать предупреждению правонарушений в области сбора и обработки персональных данных<sup>1</sup>.

---

<sup>1</sup> Свиридова Е.А. Защита персональных данных в условиях цифровой трансформации общественных отношений // Проблемы экономики и юридической практики. 2022. Т. 18, № 6. С. 53–58.

В-четвертых, особо остро гражданами ощущается отсутствие правового регулирования в вопросах предоставления им компенсации за моральный вред, связанный с утратой конфиденциальности их биометрических персональных данных. Судебная практика о взыскании компенсации морального вреда за разглашение персональных данных показывает насколько незначительными являются суммы, выплачиваемые истцу. Так, решением Подольского городского суда от 24 ноября 2020 г. по делу № 2-5054/2020 сумма компенсации морального вреда составила 3 000 рублей<sup>1</sup>. Однако, учитывая тот факт, что утрата биометрии невосполнима, такие санкции представляются незначительными. По результатам проведенного нами анкетирования, респонденты указывали как достаточный размер компенсации морального вреда за утрату биометрии сумму от 500 000 до 1 000 000 рублей. Такое мнение выразило 82% опрошенных.

Таким образом, правовые меры административно-правой защиты требуют своего совершенствования. Решение острых правовых вопросов перед государством ставит задачу своевременного реагирования на выявляемые проблемы в сфере защиты биометрических персональных данных.

III. Организационные меры административно-правовой защиты биометрических персональных данных.

Организационные меры заключаются в первую очередь в управленческой функции. Управление следует определять, как главную, регламентированную правовыми нормами, рациональную деятельность специальных, наделенных властными полномочиями субъектов (людей и организаций), оказывающих организационное, регулятивное воздействие на различные общественные процессы, с целью решения стоящих перед государством социально полезных задач в различных сферах общественной жизни государства<sup>2</sup>.

<sup>1</sup> Решение № 2-5054/2020 2-5054/2020~М-4511/2020 М-4511/2020 от 24 ноября 2020 г. по делу № 2-5054/2020 [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/Da9dDaSKUTom/> (дата обращения: 23.05.2023).

<sup>2</sup> См.: Мазурин С.Ф., Прокофьев К.Г. Административное право: учебное пособие / под общ. ред. В.П. Сальникова. СПб.: Фонд «Университет», 2019. 312 с.

Организационные меры административно-правовой защиты биометрических персональных данных направлены на управление процессами сбора, обработки и хранения биометрических персональных данных, а также создание действенной системы контроля в данной области.

Организационные меры закреплены в значительной части в положениях действующего законодательства – в Федеральных законах, постановлениях Правительства Российской Федерации, нормативных правовых актах Роскомнадзора, методических рекомендациях государственных органов.

Безусловно, особое место в вопросах организации сбора, обработки и хранения биометрических персональных данных занимает Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных», им определяются главные направления организационного характера в работе с биометрией. Правительство Российской Федерации определяет федеральный орган исполнительной власти, осуществляющий регулирование в сфере идентификации и аутентификации физических лиц на основе биометрических персональных данных<sup>1</sup>. Эти полномочия в настоящее время возложены на Минцифры России.

На Минцифры России возложена и обязанность по реализации ключевого механизма в организационных мерах по административно-правовой защите биометрических персональных данных, – аккредитация субъектов правоотношений, связанных с биометрией.

Минцифры России проводит аккредитацию:

- организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц;
- государственных органов, Банка России на право владения

---

<sup>1</sup> Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства Российской Федерации. 2023. № 1 (часть I). Ст. 19.

информационными системами, обеспечивающими аутентификацию физических лиц с использованием векторов Единой биометрической системы и (или) осуществления функций их операторов.

Цель аккредитации – формирование безопасного рынка биометрических технологий и развитие сервисов биометрической аутентификации при оказании услуг<sup>1</sup>. Постановлением Правительства Российской Федерации от 22.05.2023 № 810 утверждены Правила аккредитации организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, оснований ее приостановления и прекращения. Правила предусматривают занесение удовлетворяющих требованиям организаций в перечень аккредитованных организаций. Требования изложены в части 2 статьи 17 Федерального закона от 29 декабря 2022 г. № 572-ФЗ.

Наибольший интерес вызывают требования, касающиеся иностранного участия. К аккредитации допускаются только российские организации, а также юридические лица, в уставном (складочном) капитале которого доля участия иностранных юридических лиц не превышает 49 процентов. Отдельно уточняется, что для обработки биометрических персональных данных и создания векторов единой биометрической системы используются исключительно базы данных, расположенные на территории Российской Федерации.

Таким образом, государство нацелено на сохранение суверенитета биометрических персональных данных от иностранных государств. Однако это относится только к биометрии двух типов – запись голоса и изображение человека. В стороне остается еще и другая, не менее важная биологическая характеристика человека – ДНК.

К сожалению, на сегодняшний день не урегулирована деятельность частных клиник, проводящих исследования геномной информации. Безусловно, общее регулирование осуществляется Федеральными законами «О персональных данных» и «Об основах охраны здоровья граждан», однако на практике этого

---

<sup>1</sup> Аккредитация в сфере аутентификации на основе биометрических персональных данных [Электронный ресурс]. – URL: <https://digital.gov.ru/activity/gos-uslugi/akkreditacziya-v-sfere-autentifikaczii-na-osnove-biometricheskih-personalnyh-dannyh> (дата обращения: 04.12.2024).

недостаточно. В нарушение всех требований организациями допускалась передача геномной информации третьим лицам<sup>1</sup>, а иногда и вовсе утекала за рубеж<sup>2</sup>. В связи с чем в данной области необходимо создание действенной системы контроля органами публичной власти, направленной не только на выявление правонарушений, но и на проведение мероприятий упреждающего характера.

Среди требований требованиям для получения аккредитации, заслуживает внимания пункт о наличии финансового обеспечения ответственности за убытки, причиненные третьим лицам вследствие их доверия к результату аутентификации на основе биометрических персональных данных, осуществленной организацией, в сумме не менее чем 100 миллионов рублей. Законодателем обозначена достаточно существенная сумма, хотя на практике суммы возмещения гораздо ниже, однако часто утечка имеет массовый характер, это и обосновывает потребность в таком размере.

С одним из положений Правил аккредитации организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, оснований ее приостановления и прекращения (далее – Правила) мы не можем выразить полного согласия. Согласно пункт 4 указанных Правил аккредитация организаций действует без ограничения срока. Проводя аналогию с лицензионно-разрешительной деятельностью государства, мы можем отметить процедуру по продлению лицензии, т.е. предполагается, что при определенных условиях лицензия может быть не продлена. Бесспорно, Правилами предусмотрено приостановление и прекращение действия аккредитации, но в условиях динамично развивающейся цифровизации, когда меняются технические условия, повышаются риски утечки данных, нам кажется

---

<sup>1</sup> ВС РФ: взятие буккального эпителия для генетических исследований уже само по себе требует наличия медлицензии по генетике [Электронный ресурс]. – URL: <https://www.garant.ru/news/1313455/> (дата обращения: 22.05.2024).

<sup>2</sup> Госдума предложила проверить социальную сеть MyHeritage [Электронный ресурс]. – URL: <https://iz.ru/980229/2020-02-26/gosduma-predlozhila-proverit-sotcialnuiu-set-myheritage> (дата обращения: 08.04.2025).

целесообразным устанавливать период повторной проверки всех сведений, обеспечивающих защиту биометрических персональных данных.

Аккредитация организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, характеризуется строгой регламентацией, что способствует оптимизации структуры участников правоотношений. Однако данный подход приводит к возникновению дискриминационных барьеров для юридических лиц с ограниченным капиталом, не превышающим 500 миллионов рублей, что существенно ограничивает их возможности в конкурентной среде.

В результате проведенного исследования было установлено, что существующий порог капитала может быть адаптирован с целью снижения пороговых значений, что, в свою очередь, повысит доступность биометрических идентификационных систем и уменьшит уровень дискриминации в данной сфере. Данный вывод подкрепляется анализом существующих практик и нормативных актов, регулирующих аккредитацию подобных организаций.

Таким образом, предлагается рассмотреть возможность пересмотра существующих критериев аккредитации с целью оптимизации условий для участия юридических лиц с различным уровнем капитала, что будет способствовать более равномерному развитию рынка биометрических технологий и повышению их эффективности.

Важным участником правоотношений в области организационных мер по административно-правовой защите биометрии является оператор регионального сегмента единой биометрической системы. Он представляет собой орган исполнительной власти субъекта Российской Федерации или подведомственное ему государственное учреждение либо государственное унитарное предприятие, определяемые высшим исполнительным органом субъекта Российской Федерации, осуществляющие создание, развитие, модернизацию и эксплуатацию регионального сегмента единой биометрической системы и являющиеся владельцами технических средств, в том числе программно-технических средств, а также программ для электронных вычислительных машин, предназначенных

для обработки биометрических персональных данных, векторов единой биометрической системы, используемых в региональном сегменте единой биометрической системы<sup>1</sup>.

Отдельно в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных» приводится определение оператора. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Исходя из определения, можем отметить, что перечень обязанностей оператора биометрических персональных данных весьма значителен, а в основе деятельности оператора значится именно организационная составляющая, на основе которой выстраивается вся последующая деятельность.

Также организационные меры включают в себя разработку внутренних регламентов, обучение персонала, контроль доступа и аудит.

Анализируя опыт разработки внутренних регламентов, можем отметить методические рекомендации Банка России №19-МР от 09.10.2024 «Методические рекомендации Банка России по нейтрализации организациями финансового рынка угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением единой биометрической системы, а также актуальных при

---

<sup>1</sup> Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства Российской Федерации. 2023. № 1 (часть I). Ст. 19.

взаимодействии информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей с указанными информационными системами»<sup>1</sup>. Данные Методические рекомендации представляют собой один из наиболее проработанных инструментов для реализации организационных мер защиты. Они охватывают вопросы формирования политики по защите биометрии, назначения ответственных лиц, технического оснащения и правового регулирования. Такой комплекс мер обеспечивает эффективное управление в сфере защиты биометрии.

При этом отметим, что политика обработки биометрических персональных данных должна быть общедоступной (публичной), а сотрудники организаций должны доступно разъяснять гражданам их права и обязанности, связанные с предоставляемой ими биометрией. В связи с чем организациям, осуществляющим сбор биометрических персональных данных важно организовать должное изучение своим персоналом действующего законодательства в области защиты биометрических персональных данных. Для этого нам представляется целесообразным проведение регулярных контрольных срезов на знание персоналом норм права в области биометрии.

Таким образом, организационные меры административно-правовой защиты представляют собой многообразие форм и методов построения системы, в основе которой заложены управленческие решения в целях реализации прав граждан на защиту биометрии. Весь спектр организационных мер представляет эффективную систему, однако требует доработки в отдельных вопросах.

---

<sup>1</sup> Методические рекомендации Банка России № 19-МР от 09.10.2024 «Методические рекомендации Банка России по нейтрализации организациями финансового рынка угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением единой биометрической системы, а также актуальных при взаимодействии информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей с указанными информационными системами» [Электронный ресурс]. – URL: <https://cbr.ru/crosscut/lawacts/file/9881>.

IV. Технические меры административно-правовой защиты биометрических персональных данных.

Технические меры направлены на защиту биометрических данных от несанкционированного доступа, утечек и модификации с использованием специализированных средств и технологий.

Основные требования заключаются в том, что полученные биометрические персональные данные подлежат обязательному шифрованию и криптографической защите. Согласно информации, представленной на официальном сайте Центра Биометрических Технологий, единая биометрическая система защищена в соответствии с самыми строгими требованиями российских регуляторов<sup>1</sup>. В ней используются только отечественные криптографические и программные решения. Биометрические данные хранятся в ЕБС в зашифрованном виде и никогда не покидают периметра системы. За пределами системы могут использоваться только биометрические векторы – обезличенные наборы символов, сгенерированные на основе биометрических образцов, хранящихся в системе.

Особое место в системе правового регулирования биометрических персональных данных от несанкционированного доступа составляют: национальный стандарт Российской Федерации ГОСТ Р 58624.1-2019 (ИСО/МЭК 30107-1:2016) «Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 1. Структура», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 31 октября 2019 года № 850-ст1; национальный стандарт Российской Федерации ГОСТ Р 58624.2-2019 (ИСО/МЭК 30107-2:2017) «Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 2. Форматы данных», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 31 октября 2019 г. № 851-ст2; национальный стандарт Российской Федерации ГОСТ Р 58624.3-2019 (ИСО/МЭК

---

<sup>1</sup> О биометрии и Единой биометрической системе [Электронный ресурс]. – URL: <https://ebs.ru/documents/> (дата обращения: 24.11.2024).

30107-3:2017) «Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 20 ноября 2019 г. № 1197-стЗ.

Указанные ГОСТы содержат:

- принципы и методы оценки эксплуатационных характеристик методов ОАБП;

- протоколы результатов испытаний методов ОАБП;
- классификацию известных типов атак.

Однако стандарты не определяют:

- конкретные методы ОАБП;
- детальную информацию о методах противодействия (то есть о методах защиты от спуфинга), алгоритмах или датчиках;
- общую оценку безопасности или уязвимости биометрической системы.

Атаки, рассмотренные в серии стандартов ГОСТ Р 58624, направлены на биометрический сканер во время биометрического предъявления и сбора биометрических данных<sup>1</sup>.

В свою очередь технические меры защиты биометрии предусматривают систему безопасности от утечек (DLP-системы), мониторинг передачи данных (выявление попыток копирования/отправки биометрии), запрет на запись данных на съемные носители (флешки, внешние HDD).

Сегодня цифровое общество стали заполнять «дипфейки» с записями голосов и видеоизображениями. Дипфейками называют реалистичную замену лиц и голоса посредством использования генеративно-состязательных нейросетей<sup>2</sup>. Опасность дипфейков может заключаться и в том, что посредством «искажения»

<sup>1</sup> ГОСТ Р 58624.3-2019 Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний [Электронный ресурс]. – URL: <https://base.garant.ru/402129295/>.

<sup>2</sup> Киселев А.С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2021. № 3. С. 54–64.

нейросетями полученных биометрических персональных данных в преступных целях биометрия становится инструментом при совершении противоправных действий. Однако в противовес этому явлению во всех биометрических сервисах используется *liveness detection* – технология определения витальности, которая позволяет отличить человека от его имитации.

Таким образом, технические меры включают в себя шифрование и контроль доступа к биометрии, защиту от утечек и атак и иные технические методы по защите биометрических персональных данных с использованием инновационных информационных телекоммуникационных технологий.

Рассмотрев основные меры административно-правовой защиты биометрических персональных данных, можно сделать вывод, что государственная политика использует комплексный подход к обеспечению безопасности данных. Однако уникальность биометрии требует дополнительных мер – специальных. К ним можно отнести – информационные меры, этические меры и судебную защиту.

***Информационные меры*** административно-правовой защиты биометрических персональных данных.

Проблема современного общества в отношении биометрических персональных данных – это отсутствие полноценной информации о биометрии, целях ее обработки и способах защиты.

Согласно опросу, проведенному Всероссийским центром изучения общественного мнения (ВЦИОМ) в 2024 году, самооценка информированности россиян о биометрии продемонстрировала впечатляющие темпы роста – с 55% до 68%. То есть сегодня в той или иной степени знакомы с этим понятием почти семь из десяти наших сограждан. Впервые узнали, что такое биометрия в ходе октябрьского опроса ВЦИОМ около трети опрошенных (32%, 2023 г. – 39%)<sup>1</sup>.

---

<sup>1</sup> Биометрия на марше: лицом к лицу с будущим [Электронный ресурс]. – URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/biometrija-na-marshe-licom-k-licu-s-budushchim> (дата обращения: 12.05.2025).

И как справедливо отмечено А.П. Федосеевой, неинформированные пользователи – это потенциальные нарушители. Информационные материалы, обучение на рабочем месте, тематические заставки, видеоролики, плакаты и телевидение могут помочь информировать население об основных киберугрозах и обеспечить его безопасность. Необходимо внедрять системы повышения осведомленности пользователей, обучения и управления знаниями в области цифровой гигиены<sup>1</sup>.

Таким образом, на данном этапе цифровизации общества важно сформировать систему по информированности граждан. При соблюдении строгой конфиденциальности полученных биометрических характеристик государство должно соблюдать принцип публичности, предоставлять полную информацию о перечне биологических и физиологических характеристик в качестве биометрии, мерах их защиты.

**Этические меры** административно-правовой защиты биометрических персональных данных.

Этические стандарты традиционно являются важнейшей основой и предпосылкой для формирования в будущем саморегулирования в той или иной области<sup>2</sup>. В части, касающейся биометрии, данный вид мер изучен в минимальной степени. Попытки дать анализ по формированию этических мер защиты биометрических персональных данных предпринимал М.А. Михайлов и Т.А. Кокодей<sup>3</sup>. Реализацию мер этического характера авторы видели в соблюдении принципа добровольности предоставления биометрических

---

<sup>1</sup> Федосеева А.П. Цифровая гигиена как средство защиты от цифровых угроз в информационном пространстве / XII Сильвестровские педагогические чтения. Духовность и нравственность в образовательном пространстве: глобальные вызовы современности и духовный выбор человека: материалы Всероссийской научной конференции, Тара, 30 марта 2023 года. Омск: Амфора, 2023. С. 159–162.

<sup>2</sup> 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.

<sup>3</sup> Михайлов М.А., Кокодей Т.А. Организационные, правовые и этические аспекты получения, хранения и использования биометрической информации в целях всеобщей регистрации населения // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2022. Т. 8 (74), № 4. С. 345–353.

персональных данных гражданами. Однако, по нашему мнению, данный вид мер должен быть значительно шире.

Весьма успешный опыт в данном вопросе имеет Белоруссия. Для этого в Белоруссии создано Руководство по конфиденциальности, а также другие руководства по исследованию, выбору, обеспечению, внедрению и тестированию биометрии, а также четкий набор этических принципов<sup>1</sup>.

К принципам этики в отношении биометрии в Белоруссии относят:

1. Этичное поведение. Члены отрасли должны действовать этично, даже если этого не требует закон. Необходимо избегать действий, которые могут нанести вред людям или среде обитания.

2. Право собственности на биометрические данные и уважение к персональным данным отдельных лиц. Физические лица обладают значительным, но не полным владением своими персональными данными (независимо от того, где данные хранятся и обрабатываются). К биометрическим данным необходимо относиться с максимальной осторожностью.

3. Служба человечеству. Технологии должны служить людям и идти на благо общества, обеспечивая безопасность и предоставляя чистые выгоды для людей.

4. Справедливость и ответственность. Биометрический институт принимает принципы открытости, независимого надзора, ответственности и права на апелляцию и соответствующее возмещение.

5. Продвижение технологий, обеспечивающих конфиденциальность. Предъявляются высокие требования к качеству используемых технологий, таких как точность, обнаружение и исправление ошибок, надежность и возможность контроля качества.

6. Признание достоинства отдельных лиц и семей. Авторы принципа признают права и достоинство отдельных лиц и семей при условии, что это не противоречит законным целям системы уголовного правосудия.

---

<sup>1</sup> Семь этических принципов Института биометрии [Электронный ресурс]. – URL: <https://tcn.by/statii/sem-eticheskikh-printsipov-instituta-biometrii> (дата обращения: 16.03.2025).

7. Равенство. Используемые технологии должны предотвращать дискриминацию или системные предубеждения, основанные на религии, возрасте, поле, расе и др.

Данный перечень весьма исчерпывающий и может быть использован в российской науке и при разработке законодательных актов. Не смотря на это хотелось бы дополнить его такими мерами, как конфиденциальность, получение согласия на честной добровольной основе, с пояснением цели сбора, обработки и хранения биометрии, разъяснением сроков хранения и правил исключения полученных данных из баз биометрических персональных данных.

Весь наш перечень сконцентрирован на сотруднике, ответственном непосредственно за личный контакт по сбору биологических и физиологических характеристик человека. В связи с чем нам кажется целесообразным допускать к работе с биометрическими персональными данными, сотрудников, прошедших обучение принципам мер по этической защите биометрии. Данное обучение должно представлять собой централизованную форму, инициироваться центральным органом публичной власти, на которого возложено регулирование в сфере идентификации и аутентификации физических лиц на основе биометрических персональных данных. Для данного обучения будет значимым изучение всех исследуемых нами мер в целях формирования компетентностных характеристик высокого профиля, чтобы при общении сотрудник мог сформировать у гражданина адекватное понимание биометрии, развеять мифы, связанные с биометрическими персональными данными.

Однако этические меры по защите биометрических персональных данных должны соблюдаться не только операторами по сбору, обработке и хранению таких данных, но и самими гражданами. Сегодня все большее внимание уделяется «цифровой гигиене».

В.А. Гусев отмечал, что эффективным способом индивидуальной профилактики киберпреступлений выступает соблюдение цифровой гигиены посредством применения комплекса мер, выработанных практикой обеспечения

кибербезопасности<sup>1</sup>. Безусловно, Роскомнадзором проводятся профилактические мероприятия, однако они затрагивают в большей степени органы и организация, а, как кажется нам, необходимо доносить сведения о противодействии киберпреступлениям в первую очередь до граждан.

Согласно Сведениям о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, опубликованным МВД России, за 2024 год зарегистрировано 765,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 13,1% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 34,8% в январе-декабре 2023 года до 40,0%. Практически все такие преступления (98,7%) выявляются органами внутренних дел. Почти половина таких преступлений (48,2%) относится к категориям тяжких и особо тяжких (369,3 тыс.; +7,8%), четыре преступления из пяти (84,8%) совершаются с использованием сети Интернет (649,1 тыс.; +23,2%), почти половина (45,2%) – средств мобильной связи (346,0 тыс.; +14,3%)<sup>2</sup>.

Довольно часто потерпевшая сторона становится таковой в силу отсутствия необходимых минимальных знаний о кибербезопасности. Решение этой проблемы положительно скажется на количестве зарегистрированных преступлений в данной сфере.

В качестве решения данной проблемы мы предлагаем совершить следующую процедуру.

На портале «Госуслуги» к маю 2025 года зарегистрированы более 112 млн человек<sup>3</sup>. Считаем целесообразным, подготовить Роскомнадзором качественный

---

<sup>1</sup> Гусев В.А. Цифровая гигиена vs. киберпреступность // Психопедагогика в правоохранительных органах. 2022. Т. 27, № 1(88). С. 107.

<sup>2</sup> Состояние преступности в Российской Федерации за январь – декабрь 2024 года [Электронный ресурс]. – URL: <https://мвд.рф/reports/item/> (дата обращения: 09.04.2025).

<sup>3</sup> На портале «Госуслуги» зарегистрировались более 112 млн человек [Электронный ресурс]. – URL: <https://объясняем.рф/articles/news/na-portale-gosuslugi-zaregistrirovalis-bolee-112-mln-chelovek> / (дата обращения: 20.05.2025).

информационный материал для ознакомления пользователей личных кабинетов на портале «Госуслуги» с возможными мерами по противодействию мошенническим действиям, связанным с биометрическими персональными данными. В целях действенного контроля за изучением предложенных материалов предоставить возможность прохождения обязательного тестирования на знание мер. Важно подойти этично к проведению данной работы, сформировать у граждан сознание, что знание материала – это ключ к безопасности именно в их личных интересах. При этом это тестирование не должно быть разовым, а должно проводиться в соответствии с новыми вызовами, возникающими в сфере борьбы с кибермошенничеством.

Таким образом, этические меры на сегодняшний день требуют реальной поддержки от законодательных органов. Только наличие четко организованной системы в данном вопросе позволяет сформировать положительное отношение у населения к использованию биометрических персональных данных.

**Судебная защита** – это особая категория мер, которую невозможно оставить не отмеченной. Восстановление прав граждан при незаконном обращении с биометрическими персональными данными одна из важных мер, играющих ключевую роль в защите биометрических персональных данных и обеспечивающих правовую оценку их обработки, разрешение споров и защиту прав граждан.

В научной литературе на сегодняшний день не выделены функции судебной власти по обеспечению защиты биометрических персональных данных. В связи с этим мы считаем целесообразно определить роль судебных органов в данной области и обозначить их функции.

Анализ судебной деятельности позволяет обозначить следующие функции, характерные для судебной системы в рамках деятельности по обеспечению безопасности биометрии:

1. Толкование законодательства. Данная функция находит свою реализацию в разъяснении норм законов, регулирующих обработку биометрических персональных данных.

Вопрос о защите биометрических данных был особенно спорным в контексте видеонаблюдения в городских системах. Одним из ключевых аспектов

обсуждения стало определение того, следует ли считать видеозаписи с камер системы «Городская система видеонаблюдения» биометрическими данными, и требуется ли получать согласие граждан на их обработку. Законодательное разрешение данного вопроса было получено именно от судебных органов<sup>1</sup>.

Так, в рамках судебного постановления было принято одно из наиболее важных решений в отношении видеозаписи как биометрии человека. Согласно Апелляционному определению по административному делу № 33а-707/2020 (р/с № 2а-577/2019 от 30 января 2020 года), при отсутствии процедуры идентификации личности видеоизображения граждан не могут считаться биометрическими персональными данными. Соответственно, отсутствует необходимость получать письменное согласие гражданина на обработку биометрических персональных данных<sup>2</sup>.

Данный пример отражает роль судебных органов в формировании правоприменительной практики в отношении биометрических персональных данных. Результатом становится отсутствие двойственного трактования нормы и строгое соблюдение прав граждан.

2. Защита прав граждан. Данная функция направлена на восстановление прав граждан при совершении неправомерных действий в отношении биометрических персональных данных. Сюда относятся рассмотрение исков, предусматривающих меры административной, уголовной ответственности, оспаривание решений органов публичной власти (в случаях обязательной государственной регистрации), а также выносятся решения о компенсации морального вреда в случае нарушения прав граждан. На сегодняшний день мы не можем достоверно судить о деятельности судов в данной области, так как выделение биометрических персональных данных в отдельную категорию началось совершенно недавно, последние поправки, которые предусматривают как

---

<sup>1</sup> Суд посчитал, что технологии распознавания лиц не нарушают законодательство о персональных данных [Электронный ресурс]. – URL: <https://www.advgazeta.ru/novosti/sud-poschital-cto-tehnologii-raspoznavaniya-lits-ne-narushayut-zakonodatelstvo-o-personalnykh-dannikh/> (дата обращения: 13.04.2025).

<sup>2</sup> Информация по делу № 02а-0577/2019 [Электронный ресурс]. – URL: <https://mosgorsud.ru/rs/savyolovskij/services/cases/kas/details/988f386e-be51-47b0-b48f-e871043ef1fc> (дата обращения: 13.04.2025).

административную, так и уголовную ответственность за неправомерные действия в отношении биометрии граждан, внесены только в ноябре 2024 года<sup>1</sup>. Поэтому анализ эффективности данной функции возможно будет осуществить в последующих исследованиях.

3. Контроль за деятельностью субъектов, осуществляющих сбор, обработку и хранение биометрических персональных данных. Данная функция реализуется посредством использования таких методов как соблюдение соответствия принимаемых нормативных правовых актов действующей Конституции РФ (юрисдикция Конституционного Суда РФ), рассмотрение исковых заявлений по нарушениям, связанным со сбором, обработкой и хранением биометрии (дела находятся на рассмотрении судов общей юрисдикции), контроль за исполнением судебных решений по удалению исследуемых данных из баз.

Анализ функций судебной системы по обеспечению безопасности биометрических персональных данных позволил выявить следующие проблемы:

1. При вынесении судебного решения часто суд руководствуется приоритетом государственной безопасности над правом граждан на приватность. Эта проблема подрывает доверие граждан к использованию биометрии. Для решения этой проблемы должна быть разработана строгая регламентация действий правоохранительных органов по сбору, обработке и хранению данных. Также необходимо предусмотреть сроки и условия, в соответствии с которыми полученная, в том числе и при обязательной государственной регистрации, биометрия будет удалена из базы.

2. Несовершенство технических знаний судей. Данная проблема весьма актуальна. Судья, в силу своих профессиональных знаний, в редких случаях обладает высокими познаниями в технических сферах. Идентификация с помощью биометрических персональных данных эволюционирует на базе постоянно развивающихся технических инноваций. Правовое регулирование технических требований – это результат уже существующей деятельности,

---

<sup>1</sup> Федеральный закон от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» [Электронный ресурс]. – URL: <http://publication.pravo.gov.ru/document/0001202411300011> (дата обращения: 11.03.2025).

требующей как законодательного регулирования, так и разработки мер ответственности при несоблюдении установленных норм. В связи с этим было бы целесообразно опираться не только на правовые нормы, но и на мнения экспертов в технической сфере. В деятельности судов было бы возможным назначение внештатного эксперта из числа сотрудников Роскомнадзора или иной независимой организации.

3. Отсутствие четкого разграничения в законодательстве по соблюдению баланса безопасности и приватности биометрических персональных данных. Решение этой проблемы скрывается в несовершенстве действующего законодательства. Отсутствие единого нормативного правового акта по регулированию защиты биометрии граждан порождает правовые коллизии. В связи с этим необходимо создание единого правового акта, который будет гарантировать права граждан на приватность, при этом обеспечивать идентификацию без согласия граждан в случаях угрозы обществу.

Дополнительно хотим отметить в деятельности Верховного Суда Российской Федерации подготовку обзоров судебной практики. В настоящий момент вопросам защиты биометрических персональных данных уделяется, по нашему мнению, недостаточное внимание. Проведенный анализ обзоров судебной практики Верховного Суда Российской Федерации за 2020-2025 год показал, что вопросы защиты биометрических персональных данных не освещались.

В связи с несовершенством правовой системы по обеспечению защиты биометрии граждан, весьма актуальным стало бы разъяснение правовой позиции в данной области по результатам полугодия или же года. Введение данной практики способствовало бы исключению двусмысленной трактовки нормативных правовых актов, и повысило качество правоприменительной практики субъектами правоотношений в области защиты биометрических персональных данных.

Таким образом, судебная система обеспечивает баланс между субъектами правоотношений в области сбора, обработки и хранения биометрических

персональных данных. При этом важно отметить, что без действенного судебного контроля правовое регулирование в сфере биометрии не будет настолько эффективным, чтобы сформировать в обществе доверие к государственному регулированию в данной области.

Однако обеспечивая защиту и восстановление прав субъектов правоотношений, связанных с биометрическими персональными данными, суды сами в скором времени станут участниками таких отношений. Сегодня в судебной системе используется практика проведения судебных заседаний с использованием технологии веб-конференции. На официальном сайте Верховного суда Российской Федерации опубликована информация, согласно которой в будущем планируется внедрение в судебную деятельность технологии биометрической аутентификации участника судебного заседания по лицу и голосу. При этом отмечается, что для более масштабного применения технологии необходимо провести интеграционные и коммуникационные мероприятия, согласование всех процессуальных процедур<sup>1</sup>. Таким образом, перед судебными органами будет стоять задача по соблюдению ими требований действующего законодательства в отношении защиты биометрии граждан.

Подводя итог в рамках данного параграфа, отметим следующее.

1. На современном этапе система административно-правовой защиты биометрических персональных данных представлена двумя основными группами мер: общими и специальными.

Общие меры направлены на создание условий, способствующих реализации государственной политики в области цифровизации социума. Органы публичной власти разрабатывают и внедряют соответствующие меры, осуществляя при этом контрольно-надзорную функцию. К общим мерам можно отнести методологические, правовые, организационные и технические аспекты. Эти меры формируют комплексную систему, направленную на обеспечение безопасности биометрических данных на всех этапах их обработки и хранения.

---

<sup>1</sup> Четверть века применения видео-конференц-связи в Верховном Суде Российской Федерации [Электронный ресурс]. – URL: [https://www.vsrfr.ru/press\\_center/news/](https://www.vsrfr.ru/press_center/news/) (дата обращения: 20.05.2025).

Специальные меры акцентируют внимание на субъекте биометрических персональных данных и стимулируют общество к активному участию в решении проблем, связанных с защитой биометрии. В эту группу входят информационные, этические меры и механизмы судебной защиты.

Важно отметить, что каждый из этих аспектов требует постоянного совершенствования в условиях динамично развивающейся цифровой среды и новых вызовов в области кибербезопасности.

2. Судебная система выступает в роли гаранта правовой стабильности и справедливости в условиях стремительного развития биометрических технологий, обеспечивая баланс между интересами государства, общества и отдельных граждан.

В контексте динамично развивающейся цифровой среды и растущего интереса к биометрическим технологиям необходимо подчеркнуть значимость судебного контроля как неотъемлемого элемента правового регулирования в данной области. Без эффективного судебного надзора механизмы правового регулирования биометрии рискуют утратить свою действенность, что, в свою очередь, может подрвать общественное доверие к государственным институтам и их способности обеспечивать соблюдение прав и свобод граждан в условиях цифровой трансформации.

3. Проблема кибербезопасности, особенно в контексте предотвращения мошенничества с биометрическими данными, приобретает все большую актуальность в современном цифровом обществе. Отсутствие базовых знаний в этой области у значительной части пользователей, в частности на платформе «Госуслуги», где зарегистрировано более 112 миллионов человек, создает благоприятные условия для преступных действий. В целях минимизации рисков и повышения уровня цифровой грамотности населения предлагается комплексная инициатива, направленная на интеграцию образовательных программ в существующие информационные системы.

Видится целесообразным Роскомнадзором разработать и внедрить на портале «Госуслуги» специализированные информационные материалы, направленные на ознакомление пользователей с современными методами защиты биометрии и противодействия кибермошенничеству. Данный контент должен быть представлен в структурированной и доступной форме, учитывающей специфику аудитории и современные тенденции в области информационной безопасности. Для обеспечения эффективного усвоения предложенной информации предлагается ввести систему обязательного тестирования, направленного на проверку знаний пользователей в области кибербезопасности. Тестирование должно быть интегрировано в пользовательский интерфейс портала и проводиться на регулярной основе с учетом актуальных угроз и изменений в законодательстве.

4. В целях обеспечения надлежащего уровня защиты биометрических данных предлагается внедрение дополнительных мер, включая обязательное обучение должностных лиц органов публичной власти и операторов систем биометрических персональных данных по вопросам этических норм и принципов работы с субъектами биометрии. Это предполагает необходимость формирования у указанных категорий лиц компетенций, направленных на соблюдение этических стандартов и предотвращение возможных нарушений прав и свобод субъектов биометрии.

### **§ 3. Совершенствование деятельности органов внутренних дел Российской Федерации по административно-правовой защите биометрических персональных данных**

В настоящее время научные технологии способны производить обработку ключевых человеческих идентификаторов – термограммы лица, венозного рисунка кистей, параметров голоса, особенностей глазного дна, узора радужной оболочки глаз, что дает возможность с высокой точностью отличить одного

человека от другого<sup>1</sup>. Такое стремительное развитие естественно стимулирует различные органы, в частности правоохранительные, применять биометрические данные при реализации своей деятельности<sup>2</sup>.

Роль биометрических персональных данных в правоохранительной деятельности весьма значительна. Изначально она выражалась только в криминалистических задачах, но в условиях развивающейся цифровизации получает все большее распространение.

Исторические этапы развития биометрических персональных данных в правоохранительной деятельности изложены в работах А.М. Зинина<sup>3</sup>, Ш.Н. Хазиева<sup>4</sup>, И.С. Звягина и А.Ю. Евреиновой<sup>5</sup>.

Рассматривая исторический контекст, хотелось бы выделить модель исторического становления биометрических персональных данных, приведенную Е.Г. Барковской<sup>6</sup>.

Е.Г. Барковская отмечала, что становление, эволюция и внедрение в правоохранительную деятельность биометрических технологий могут быть дифференцированы на четыре этапа<sup>7</sup>.

Для первого этапа Е.Г. Барковская указывала периодизацию начиная с древности (от истоков формирования эмпирической антропометрии) до 90-х гг. XIX в. Характерным признаком было использование биометрических характеристик до создания официально признанной научной базы.

<sup>1</sup> Шатов Д.В., Барсуков С.С., Шипанов И.Н. Лицевая биометрия и нейронные сети в криминалистике: современные возможности и проблемы применения // Юристъ-Правоведъ. 2023. № 1(104). С. 155–163.

<sup>2</sup> Шумилин В.П. Биометрический метод распознавания лица в правоохранительных органах / Современное состояние и перспективы обеспечения безопасности дорожного движения: теория и практика: сборник материалов Всероссийской научно-практической конференции, Орел, 21 ноября 2019 года. – Орел: Орловский юридический институт МВД России имени В.В. Лукьянова, 2020. С. 166–171.

<sup>3</sup> Зинин А.М. Биометрические системы и идентификация человека // Lex Russica (Русский закон). 2012. Т. 71, № 5. С. 1064–1070.

<sup>4</sup> Хазиев Ш.Н. Криминалистические и судебно-экспертные основы современных биометрических технологий // Теория и практика судебной экспертизы. 2023. Т. 18, № 1. С. 16–21.

<sup>5</sup> Звягин И.С., Евреинова А.Ю. Основы криминалистической биометрической идентификации // Вестник Воронежского института МВД России. 2025. № 1. С. 209–214.

<sup>6</sup> Барковская Е.Г. Исторические предпосылки и практические потребности интеграции биометрического и криминалистического знания // Философия права. 2010. № 6(43). С. 28–31.

<sup>7</sup> Там же.

Второй этап, по мнению Е.Г. Барковской, ознаменован применением систематизированного научного биометрического подхода, разработанного Альфонсом Бертильоном для идентификации арестованных преступников, а также воплощение идей В. Гершеля и Г. Фолдса, которые послужили базой для дальнейшего развития дактилоскопии в трудах Френсиса Гальтона.

Третий этап Е.Г. Барковская связывала с разработкой новейших альтернативных биометрических технологий, основанных на современных достижениях науки и техники (биохимии, компьютерных и информационных технологий и др.).

Четвертый этап, по мнению Е.Г. Барковской, характеризуется как повсеместное внедрение биометрических технологий в повседневную жизнь человека.

Такую точку зрения по периодизации исторического внедрения биометрических данных в правоохранительную деятельность разделяют многие ученые. Данная классификация кажется нам слишком обобщенной, однако, применительно к деятельности органов внутренних дел, в области биометрических персональных данных указаны основные периоды и здесь необходимо разделить позицию автора.

Безусловно, сегодня наше государство находится на четвертом этапе. Биометрические технологии применяются теперь не только в правоохранительной деятельности, но в гражданских правоотношениях. Растет и перечень биометрических персональных данных, если раньше для идентификации использовалось только фото и дактилоскопическая информация, то сегодня этот перечень пополняется новыми характеристиками. Это стало возможным благодаря автоматизации идентификации, что ускорило сам процесс сравнения данных и повысило результативность использования биометрии.

Задача государства теперь заключается в построении системы правового регулирования, чтобы обеспечить баланс между правом граждан на частную жизнь и соблюсти интересы государства при обеспечении безопасности общества, связанные с применением биометрических персональных данных.

О роли органов внутренних дел Российской Федерации в данном вопросе указывал Н.В. Макарейко, ссылаясь на Положение о МВД России, он отмечал, что потенциал органов внутренних дел в большей степени позволяет обеспечить общественную безопасность, информационную безопасность, личную безопасность, безопасность дорожного движения, транспортную безопасность<sup>1</sup>. При этом эффективность реализации полицейских функций напрямую зависит от оснащения адекватными мерами защиты от различных угроз<sup>2</sup>.

Говоря о совершенствовании деятельности органов внутренних дел Российской Федерации по административно-правовой защите биометрических персональных данных, можно отметить, что в Российской Федерации создана правовая основа законодательного регулирования использования в розыскной и идентификационной деятельности достижений современной науки в области дактилоскопии, генетики, биометрии и технических средств<sup>3</sup>. Отличительной чертой является то, что все перечисленные области регулируются отдельными законодательными актами и определяют границы деятельности в области использования и защиты биометрических персональных данных.

А.Л. Гогаева в своей научной статье выделяла следующие сферы практического внедрения биометрических технологий идентификации личности для решения правоохранительных задач органов полиции:

- судебно-экспертная идентификация личности;
- оперативное распознавание (идентификация) при осуществлении оперативно-розыскных мероприятий;
- идентификация при осуществлении контроля физического или логического доступа к объектам;

---

<sup>1</sup> Макарейко Н.В. Органы внутренних дел как субъект обеспечения национальной безопасности // Полиция и общество: проблемы и перспективы взаимодействия. 2024. № 6. С. 87.

<sup>2</sup> Александров А.Н., Дизер О.А. Организационно-правовые аспекты применения полицией специальных технических средств противодействия беспилотным воздушным судам / Актуальные проблемы полицейского права: материалы международной научно-практической конференции, Омск, 1–2 июня 2023 года. Омск: Омская академия МВД России, 2023. С. 3.

<sup>3</sup> Буряков Е.В. Использование достижений науки в розыскной и идентификационной деятельности // Вестник Уфимского юридического института МВД России. 2023. № 3 (101). С. 53–59.

- идентификация при осуществлении рубежного контроля<sup>1</sup>.

Под судебно-экспертной идентификацией понимают вид идентификационных исследований, осуществляемых судебным экспертом в целях установления групповой (родовой) принадлежности или тождества объекта на основе специальных знаний, применяемых в ходе производства экспертизы<sup>2</sup>. Различают идентификацию личности криминалистическую и судебно-медицинскую, включающую медико-криминалистическую идентификацию. Данное направление находится в ведении Экспертно-криминалистического центра МВД России, который аккумулирует деятельность масштабной сети экспертно-криминалистических подразделений на всей территории страны<sup>3</sup>.

Бесспорно, судебная экспертная идентификация личности играет важную роль в правоохранительной деятельности, являясь инструментом установления личности и обеспечения законности.

Криминалистические экспертизы с использованием биометрических персональных данных в целях идентификации проводятся на всех этапах расследования: для установления неизвестного лица либо личности погибшего, исполнителя, круга подозреваемых. В этих случаях кроме ДНК, дактилоскопии, используются фоноскопия (распознавание человека по голосу), почерковедческая экспертиза, идентификация по походке из видео с камер наблюдения.

Немаловажную роль играют биометрические характеристики при установлении связи подозреваемого или обвиняемого с местом преступления. Одним из ярких примеров стало раскрытие дела 32-летней давности. В 2025 году эксперты повторно изучили обнаруженные на месте преступления улики: провели

---

<sup>1</sup> Гогаева А.Л. Сферы практического внедрения биометрических технологий идентификации личности для решения правоохранительных задач органов полиции / Инновационные технологии производства и переработки сельскохозяйственной продукции: материалы всероссийской научно-практической конференции в честь 90-летия кафедр «Кормление, разведение и генетика сельскохозяйственных животных» и «частная зоотехния» факультета технологического менеджмента, Владикавказ, 30–31 марта 2021 года: в 2-х ч. Владикавказ: Горский государственный аграрный университет, 2021. Ч. 2. С. 179–181.

<sup>2</sup> Романько Н.А., Зинин А.М., Хазиев Ш.Н. О судебно-экспертной идентификации личности по признакам внешности и особенностям строения тела // Судебная медицина. 2017. Т. 3, № 1. С. 21–25.

<sup>3</sup> История ЭКЦ [Электронный ресурс] <https://мвд.рф/mvd/structure1/> (дата обращения: 23.05.2025).

молекулярно-генетическую экспертизу ДНК с окурков, бутылки и мебели, а также дактилоскопические исследования системой «ПАПИЛОН», которые подтвердили причастность фигуранта к массовому убийству<sup>1</sup>. Лицо, совершившее преступление, было не только установлено, но и привлечено к уголовной ответственности.

Экспертное заключение об идентификации личности – это доказательство, имеющее высокую доказательственную силу в суде, так как основано на научных методах и выдается независимым экспертом. Оно помогает преодолеть субъективность показаний свидетелей и потерпевших (особенно при опознании).

В пользу использования биометрических персональных данных указывает ряд преимуществ, к которым можно отнести:

- объективность. Экспертиза является результатом использования научных методов, она лишена субъективности;
- достоверность. Идентификация по биометрическим персональным данным показала на практике высокую эффективность. Научный прогресс позволяет раскрывать дела, которые десятилетиями оставались нераскрытыми;
- точность. Современные методы обладают исключительно высокой дифференцирующей способностью;
- независимость. Исследование проводится экспертом, не заинтересованным в исходе дела.

При этом нельзя утверждать, что судебно-экспертная идентификация личности является совершенной. В первую очередь нужно учитывать, что в России нет тотального сбора биометрии, базы данных наполняются только в случаях применения обязательной государственной регистрации (данные случаи строго регламентированы действующим законодательством) или же за счет добровольной регистрации.

Однако этих сведений часто бывает недостаточно, и в базах нет материалов биометрии, которые обнаружены на месте преступления. Также результат зависит

---

<sup>1</sup> На Урале начался суд над убийцей, который 32 года назад забил молотком 7 человек [Электронный ресурс]. – URL: <https://www.papillon.ru/about/blog/na-urale-nachalsja-sud-nad-ubijcej-kotoryj-32-goda-nazad-zabil-molotkom-7-chelovek/> (дата обращения: 23.05.2025).

от качества и количества обнаруженных следов и сравнительных образцов. И стоит признать, что некоторые виды экспертиз являются дорогостоящими и требуют значительных временных трудозатрат.

Таким образом, можно сделать вывод, что судебная экспертная идентификация личности – это незаменимый инструмент современной правоохранительной деятельности. Она обеспечивает научную основу для установления истины по уголовным делам, связывая конкретных людей с конкретными действиями и обстоятельствами. Ее роль в раскрытии, расследовании и предупреждении преступлений, обеспечении неотвратимости наказания и защите прав граждан невозможно переоценить. Постоянное развитие экспертных методик (особенно в области генетики и компьютерного анализа изображений) только усиливает ее значение.

Следующим важным направлением использования биометрических персональных данных в правоохранительной деятельности является оперативно-разыскная деятельность. Совершенствование и использование в деятельности оперативных подразделений технического отождествления личности на основе биометрической идентификации является перспективной и эффективной формой отождествления личности, которая может существенно улучшить работу оперативных подразделений по выявлению, пресечению и раскрытию преступлений, розыску скрывающихся преступников и выполнению других задач оперативно-разыскной деятельности<sup>1</sup>.

Автоматизация и использование современных технологий при идентификации личности по биометрическим персональным данным создают условия для повышения эффективности оперативно-разыскных мероприятий. Полученные данные позволяют распознать личность в короткие сроки посредством сравнения с данными, имеющимися в базах.

---

<sup>1</sup> Ховавко С.М. Теоретико-правовые и организационные основы технического отождествления личности на основе биометрической идентификации в оперативно-розыскной деятельности // Вестник Уральского юридического института МВД России. 2022. № 2. С. 155.

При чем данные могут быть получены оперативными сотрудниками не только из баз, находящихся в введении МВД России. Например, в соответствии с постановлением Правительства РФ от 28.12.2018 № 1703 «О предоставлении оператором единой биометрической системы и оператором регионального сегмента единой биометрической системы в Министерство внутренних дел Российской Федерации и Федеральную службу безопасности Российской Федерации сведений, содержащихся в единой биометрической системе и региональном сегменте единой биометрической системы»<sup>1</sup> данные, хранящиеся в единой биометрической системе, по мотивированному запросу в целях обеспечения обороны страны и безопасности государства, охраны правопорядка, транспортной безопасности и противодействия терроризму могут быть предоставлены в МВД России. Указанные сведения предоставляются оператором единой биометрической системы в течение одного дня со дня получения запроса. Данный факт говорит о важности оперативности идентификации при проведении оперативно-разыскных мероприятий и доступности к биометрическим персональным данным для правоохранительной деятельности.

Рассмотрению общих вопросов автоматизации криминалистической информации (криминалистических учетов и регистрации) посвящены научные труды Р.С. Белкина, Е.Р. Россинской, Л.Г. Эджубова, З.И. Кирсанова, В.Я. Колдина, И.С. Полевого, В.А. Снеткова, А.И. Хвыли-Олинтера и других<sup>2</sup>.

В настоящее время одним из перспективных направлений в решении задач, стоящих перед правоохранительными органами по борьбе с преступностью, является использование достижений науки и техники в сфере информационных

---

<sup>1</sup> Постановление Правительства РФ от 28.12.2018 № 1703 «О предоставлении оператором единой биометрической системы и оператором регионального сегмента единой биометрической системы в Министерство внутренних дел Российской Федерации и Федеральную службу безопасности Российской Федерации сведений, содержащихся в единой биометрической системе и региональном сегменте единой биометрической системы» // Собрание законодательства Российской Федерации. 2018. № 53 (часть II). Ст. 8727.

<sup>2</sup> Эйхвальд Н.Л. Использование дактилоскопических карт, полученных посредством комплекса «Живой сканер» и АДИС «Папилон», при производстве дактилоскопической экспертизы // Юридическая наука и правоохранительная практика. 2020. № 4(54). С. 98–104.

систем видеозаписи и контроля<sup>1</sup>. Основным достоинством видеозаписи является то, что с ее помощью доступна фиксация как звуковой, так и зрительной информации, а также эмоционально-психологического состояния запечатленных субъектов процессуального разбирательства, в том числе, разрабатываемых лиц в ходе проведения оперативно-розыскных мероприятий<sup>2</sup>.

Максимальную эффективность противодействия правонарушениям могут обеспечить лишь интеллектуальные системы видеонаблюдения<sup>3</sup>.

При этом искусственный интеллект – сложная технология, цель которой не только имитация деятельности человеческого мозга, но и совершение наиболее точных действий в целях упрощения и систематизации различных процессов<sup>4</sup>.

Исходя из многочисленных опытов, утомляемость, неспособность к длительной концентрации сказываются на человеке уже через полчаса работы с несколькими камерами, что приводит к резкому падению эффективности наблюдения. В то же время интеллектуальные системы видеонаблюдения дают стабильное и высокое качество, а решение таких задач, как распознавание номеров движущихся автомобилей на дорогах общего пользования в режиме реального времени, практически не представляется возможным для человека<sup>5</sup>.

В связи с этим в число приоритетных направлений использования информационно-коммуникационных технологий в оперативно-аналитической деятельности органов внутренних дел на сегодняшний день предлагается

<sup>1</sup> Машковцев А.А., Моляров Е.А. Электронное наблюдение как современный способ оперативно-розыскного документирования преступлений // Вестник Сибирского юридического института МВД России. 2024. № 4(57). С. 91–99.

<sup>2</sup> Получение визуальной информации с использованием современных технических средств в целях выявления, пресечения и раскрытия преступлений / А.Ю. Молянов, В.Г. Любан, К.А. Сермягин, С.М. Филиппов. М.: МосУ МВД России имени В.Я. Кикотя, 2019. 88 с.

<sup>3</sup> Технические средства визуального контроля, используемые в органах внутренних дел / А.А. Черных, Ф.В. Безгачев, Е.А. Лаппо, А. Лхамсурэн. Красноярск: Сибирский юридический институт МВД России, 2022. 124 с.

<sup>4</sup> Добробаба М.Б. Проблема обеспечения безопасности персональных данных, обрабатываемых с использованием систем искусственного интеллекта / Российская правовая система: в поисках национальной идентичности: сборник докладов XIV Московской юридической недели, Москва, 26–29 ноября 2024 года. В 6-ти ч. М., 2025. С. 119.

<sup>5</sup> Могилин К.А., Селищев В.А. Интеллектуальные системы видеонаблюдения в комплексах безопасности // Известия Тульского государственного университета. Технические науки. 2020. № 3. С. 89–94.

включить разработку и внедрение новейших технологий видеоаналитики, обладающей возможностью удаленного мониторинга психофизиологического состояния людей с целью определения уровня потенциальной опасности в различных ситуациях<sup>1</sup>.

Однако, учитывая чувствительность биометрических персональных данных, нельзя не обратить внимание на настороженность со стороны общества, которая проявляется в отношении использования камер видеонаблюдения для идентификации личности. А.А. Машковцев и Е.А. Моляров исследовали данный дискуссионный вопрос о возможном чрезмерном ограничении конституционного права граждан на тайну личной жизни. Они отмечали, что целью расширения полномочий в рамках оперативной деятельности должно являться прежде всего обеспечение безопасности общества и государства от преступных посягательств, повышение эффективности раскрытия преступлений, розыска скрывшихся опасных преступников и, в конечном итоге, привлечение к ответственности виновных, восстановление справедливости и обеспечение прав пострадавших от преступлений<sup>2</sup>.

В глазах большинства граждан и при большинстве обстоятельств, где требуются повышенные меры для обеспечения правопорядка и защиты граждан, видеонаблюдение рассматривается как полезная неизбежность, но оно не должно превращаться в слежку. Государством разработана правовая система, позволяющая избежать чрезмерного нецелевого использования биометрических характеристик при использовании видеонаблюдения. Оперативно-розыскная деятельность регламентируется законодательными актами, подзаконными актами и ведомственными нормативными актами. К первым следует отнести Конституцию Российской Федерации, в статье 19 которой устанавливаются обязанности государства по обеспечению охраны правопорядка, прав и свобод

---

<sup>1</sup> Саркисян Г.Г. Использование информационно-коммуникационных технологий в оперативно-аналитической деятельности органов внутренних дел Российской Федерации // Труды Академии управления МВД России. 2024. № 4(72). С. 172–181.

<sup>2</sup> Машковцев А.А., Моляров Е.А. Электронное наблюдение как современный способ оперативно-розыскного документирования преступлений // Вестник Сибирского юридического института МВД России. 2024. № 4(57). С. 91–99.

граждан. В статьях 23, 24, 25 устанавливается право граждан на неприкосновенность личности, жилища, тайны частной и личной жизни, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Требования указанных статей Конституции Российской Федерации налагают определенные ограничения на методы сбора и получения соответствующей информации, в том числе с помощью технических средств<sup>1</sup>.

Но при этом встречаются случаи превышения должностных полномочий и нецелевое использование биометрических характеристик. В связи с чем, несомненно, необходимо совершенствовать систему профилактики и расследования должностных преступлений, связанных с неправомерным использованием баз данных, содержащих сведения о гражданах, а также принимать меры, направленные на повышение доверия граждан правоохранительной системе<sup>2</sup>. Поэтому крайне важно, чтобы сотрудники правоохранительных органов обладали достаточными знаниями в части, касающейся требований законодательства, предъявляемых к получению достаточной для разрешения уголовного дела цифровой информации<sup>3</sup>.

В ходе исследования вопросов совершенствования деятельности органов внутренних дел Российской Федерации по административно-правовой защите биометрических персональных данных нами установлены пробелы в правовом регулировании биометрических персональных данных в оперативно-разыскном законодательстве.

В первую очередь, это отсутствие детального регулирования сбора и обработки биометрических персональных данных в оперативно-разыскной деятельности, в том числе отсутствие перечня биометрических характеристик по

---

<sup>1</sup> Получение визуальной информации с использованием современных технических средств в целях выявления, пресечения и раскрытия преступлений / А.Ю. Молянов, В.Г. Любан, К.А. Сермягин, С.М. Филиппов. М.: МосУ МВД России имени В.Я. Кикотя, 2019. 88 с.

<sup>2</sup> Машковцев А.А., Моляров Е.А. Электронное наблюдение как современный способ оперативно-розыскного документирования преступлений // Вестник Сибирского юридического института МВД России. 2024. № 4(57). С. 95.

<sup>3</sup> Жандров В.Ю. Решение задач оперативно-розыскной деятельности посредством получения сведений в информационно-телекоммуникационной среде // Вестник Московского университета МВД России. 2024. № 4. С. 64.

которым возможно проведение идентификации. Безусловно, в целях правоохранительной деятельности не требуется согласие субъекта биометрических персональных данных, как это предусмотрено при добровольной регистрации. По нашему мнению, требуется альтернатива данному согласию, например, письменное уведомление с указанием перечня биометрических персональных данных, которые будут использованы в ходе оперативно-разыскной деятельности с обязательным ознакомлением под подпись. Во-вторых, существует пробел в регулировании вопроса сбора биометрии в отношении подозреваемых, чья вина в правонарушении или преступлении не подтвердилась. Так, данные вносятся в базу и не удаляются после окончания оперативно-разыскных мероприятий. Как нам кажется, данная ситуация неправомерна. Ее решением должно стать согласие либо отказ субъекта биометрических персональных данных от их хранения в базе. И в таком случае недопустима халатность со стороны сотрудников правоохранительной деятельности. В-третьих, необходима система контроля в области использования биометрических персональных данных в оперативно-разыскной деятельности. Отмечается, что действующий судебный и прокурорский контроль за оперативно-разыскными мероприятиями часто формален и не приспособлен для оценки сложных технологических аспектов сбора и использования биометрических персональных данных, их соразмерности и необходимости<sup>1</sup>. Решение этой проблемы, по нашему мнению, заключается в привлечении кадров, обладающих соответствующими данными либо обучение (повышение классификации) действующих сотрудников и судей.

Таким образом, рассматривая роль биометрических персональных данных в оперативно-разыскной деятельности, можем сделать следующий вывод. Биометрические данные кардинально усиливают возможности оперативной идентификации, делая ее более эффективной в борьбе с преступностью. Однако их применение несет серьезные риски для фундаментальных прав на неприкосновенность частной жизни. Нынешнее правовое регулирование в России

---

<sup>1</sup> Семенчук В.В. Судебный контроль за оперативно-розыскной деятельностью – альтернатива прокурорскому надзору // Вестник Нижегородского университета имени Н.И. Лобачевского. 2020. № 4. С. 130.

фрагментарно, и часто не успевает за технологиями. Узловой проблемой является отсутствие пропорциональности и четких правовых рамок для сбора и использования биометрических персональных данных в оперативно-разыскной деятельности, особенно автоматизированного распознавания лиц. Соответственно, перед государством стоит задача по совершенствованию действующего законодательства и подготовки высококвалифицированных кадров.

Следующим направлением использования биометрических персональных данных в правоохранительной деятельности является идентификация при осуществлении контроля физического или логического доступа к объектам.

Понятия физического и логического доступа к объектам изложены в ГОСТе Р 57580.1-2017 «Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

Так, под физическим понимается доступ к объекту доступа, включая доступ в помещение, в котором расположен объект доступа, позволяющий осуществить физическое воздействие на него.

Логический – доступ к ресурсу, в том числе удаленный, реализуемый с использованием вычислительных сетей, позволяющий, в том числе без физического доступа, осуществить доступ к защищаемой информации или выполнить операции по обработке защищаемой информации.

Ограничение физического доступа предполагается в помещениях, требующие дополнительных мер безопасности, в частности, в зданиях правоохранительных органов. Несмотря на тот факт, что биометрические персональные данные вошли в оборот не так давно, они стали активно использоваться и в системах физического доступа сотрудников на территорию полиции по идентификации по фотоизображению. Такие системы все чаще устанавливаются в отделах полиции.

Сегодня передовой компанией, успешно внедряющей результаты своей инновационной деятельности в области биометрических персональных данных, является ООО «ИТ-Папилон». Данная компания создает программные продукты

для мультибиометрической идентификации, баллистической идентификации и комплексной безопасности. Компания Папилон – российская производственная и IT-компания, занимающаяся комплексной разработкой, внедрением и сопровождением биометрических и криминалистических систем национального масштаба для силовых структур, государства и бизнеса<sup>1</sup>. Системы Папилон внедрены и в деятельность органов внутренних дел Российской Федерации. Самая масштабная из них – единая многоуровневая система автоматизированных дактилоскопических учетов МВД России с одним из крупнейших в мире федеральным дактилоскопическим банком данных.

Рассматривая возможности обеспечения физического доступа по биометрической идентификации, необходимо отметить такие продукты, как АДИС (AFIS) Папилон – система мультибиометрической идентификации (АДИС-8.4 и АДИС-9).

Система представляет собой мультибиометрические банки данных неограниченного объема криминалистического и гражданского назначения для регистрации/идентификации личности:

- по всем видам дактилоскопических отпечатков (пальцев и ладоней);
- по изображениям лица;
- по изображениям радужных оболочек глаз.

Созданная автоматическая обработка и отождествление поступающей биометрической информации, а также следов пальцев рук и ладоней с мест преступлений, подходит для экспертов-криминалистов, правоохранительных и надзорных органов, других государственных служб. Биометрическая экспресс-идентификация личности осуществляется в режиме реального времени<sup>2</sup>.

Бесспорно, такие многопрофильные системы необходимы для использования в деятельности органов внутренних дел, и в первую очередь они должны быть использованы именно в целях обеспечения безопасности.

---

<sup>1</sup> Ключевые компании [Электронный ресурс]. – URL: <https://www.papillon.ru> (дата обращения: 07.03.2025).

<sup>2</sup> АДИС (AFIS) Папилон – система мультибиометрической идентификации [Электронный ресурс]. – URL: <https://www.papillon.ru/products/programs/adis/> (дата обращения: 12.05.2025).

Свою эффективность по предоставлению физического доступа по биометрии доказали системы идентификации при проведении массовых мероприятий (спортивные, конференции, концерты и другие). Для обеспечения санкционированного входа на территорию объекта и в зоны ограниченного доступа, выход из них путем идентификации личности осуществляется по комбинации различных признаков: вещественный код (вигандкарточки, ключи touch memory и другие устройства), запоминаемый код (клавиатуры, кодонаборные панели и другие устройства), биометрические признаки (отпечатки пальцев, сетчатка глаз и другие признаки), идентификация лиц<sup>1</sup>.

На законодательном уровне установлен порядок прохождения болельщиками процедуры идентификации с использованием биометрических персональных данных. Определен регламент применения персонифицированных карт для допуска на спортивные мероприятия, а также процедуры идентификации и аутентификации участников официального спортивного соревнования и иных лиц, задействованных в его проведении<sup>2</sup>. Идентификация посетителя спортивного соревнования для целей посещения мест проведения официального спортивного соревнования является обязательной и осуществляется однократно<sup>3</sup>. На спортивных мероприятиях разрешена идентификация, в том числе и с помощью систем видеонаблюдения, лиц, в отношении которых вступило в законную силу постановление суда об административном запрете на посещение мест проведения официальных спортивных соревнований. То есть использование биометрических данных людей, которые когда-либо совершали административные правонарушения, на официальных спортивных мероприятиях законодательством

---

<sup>1</sup> Сердюк А.С., Абросимова Е.М. Обеспечение безопасности на объектах спортивной инфраструктуры / Современные материалы, техника и технология: сборник научных статей 7-й международной научно-практической конференции, Курск, 29–30 декабря 2017 года. Курск: Университетская книга, 2017. С. 346.

<sup>2</sup> Постановление Правительства РФ от 25 июня 2022 г. № 1140 «О порядке применения персонифицированной карты для посещения спортивного соревнования, а также идентификации и аутентификации зрителей, участников официального спортивного соревнования, иных лиц, задействованных в проведении такого соревнования» (с изменениями и дополнениями) // Собрание законодательства Российской Федерации. 2022. № 27. Ст. 4835.

<sup>3</sup> Там же.

Российской Федерации разрешено. Кроме того, регламентирована работа по ведению МВД России базы данных на лиц, имеющих административный запрет на посещение мест проведения официальных спортивных соревнований в дни их проведения на срок от одного года до семи лет.

По мнению авторов В.В. Комарова, С.Н. Поповой, В.А. Ворожейкина и Д.С. Давидова, данные меры административной ответственности представляются полными и сбалансированными<sup>1</sup>. В своем исследовании мы разделяем точку зрения авторов в данном вопросе. Хотелось бы отметить, что опыт идентификации по биометрическим характеристикам может применен и в рамках иных мер по обеспечению физического доступа.

Логический доступ к объекту с помощью биометрической идентификации в деятельности полиции в настоящий момент не получил своего распространения. Это объясняется особым статусом биометрии сотрудников правоохранительных органов. При поступлении на службу в органы внутренних дел Российской Федерации кандидат проходит обязательную дактилоскопическую регистрацию и предоставляет свое фотоизображение. Учитывая статус сотрудника полиции, для многих правонарушителей утечка таких данных – особый успех», поэтому важно сохранить конфиденциальность полученных данных. Однако, переход существенных объемов оперативно значимой информации в киберпространство порождает потребность в использовании в оперативно-служебной деятельности полиции специфических форм и методов доступа к ней<sup>2</sup>. В связи с чем в ближайшем будущем возможным способом удаленной идентификации сотрудника органов внутренних дел станет установление личности при помощи биометрических персональных данных.

---

<sup>1</sup> Комаров В.В., Попова С.Н., Ворожейкин В.А., Давидов Д.С. Исследование технологий распознавания лиц для идентификации участников несанкционированных публичных мероприятий // Вестник экономической безопасности. 2022. № 6. С. 138.

<sup>2</sup> Осипенко А.Л., Луговик В.Ф. Проблемы доступа правоохранительных органов к скрываемой компьютерной информации при раскрытии преступлений // Общество и право. 2021. № 2(76). С. 60.

Хочется отметить эффективность использования биометрических персональных данных для обеспечения физического доступа к объекту. В данной области важно внедрение новых технологий и незамедлительное их правовое регулирование.

Идентификация при осуществлении рубежного контроля занимает особое место в деятельности органов внутренних дел Российской Федерации. Современная миграционная политика в Российской Федерации находится на этапе своего активного совершенствования. Данный процесс носит комплексный характер, в котором участвуют одновременно законодательная и исполнительная власть, перед которыми стоит задача по урегулированию всех возникших вопросов в области сложившейся внутривластной ситуации, связанной с миграцией<sup>1</sup>.

В октябре 2024 года Председатель Государственной Думы Федерального Собрания Российской Федерации В.В. Володин отмечал, что работа по совершенствованию законодательства в сфере миграционной политики продолжается, и с начала года было принято 7 законов, регулирующих данную сферу<sup>2</sup>.

В свою очередь, на расширенном заседании коллегии МВД России 2024 года Президент Российской Федерации В.В. Путин поставил перед Министерством внутренних дел Российской Федерации задачу, согласно которой необходимо «глубоко, кардинально обновить подходы к миграционной политике»<sup>3</sup>.

В рамках исполнения этого поручения Президента Российской Федерации запущен инновационный проект, разработанный Министерством внутренних дел Российской Федерации и Министерством цифрового развития, связи и массовых

---

<sup>1</sup> Карпушина А.В. Вопросы правового регулирования биометрических персональных данных в условиях современной миграционной политики / Проблемы юриспруденции и педагогики высшей школы в работах молодых ученых: сборник материалов Всероссийской научно-практической конференции, Белгород, 28 ноября 2024 года. Белгород: Белгородский юридический институт МВД России, 2025. С. 94.

<sup>2</sup> Депутаты приняли еще три законопроекта, направленных на совершенствование миграционной политики [Электронный ресурс]. – URL: <http://duma.gov.ru/news/> (дата обращения: 10.12.2024).

<sup>3</sup> Расширенное заседание коллегии МВД [Электронный ресурс]. – URL: <http://www.kremlin.ru/events/president/news> (дата обращения: 07.04.2024).

коммуникаций Российской Федерации – разработка цифрового профиля иностранного гражданина.

Создание цифрового профиля иностранного гражданина осуществляется в соответствии с Планом мероприятий по реализации в 2024-2025 гг. Концепции государственной миграционной политики РФ на 2019-2025 гг., утвержденного Распоряжением Правительства РФ от 16 января 2024 г. № 30-р<sup>1</sup> (далее – План).

Авторами Е.В. Евсиковой и С.Б. Буц было отмечено, что формирование цифрового профиля мигранта является одним из приоритетных мероприятий по совершенствованию правовых, организационных и иных механизмов, регулирующих порядок въезда в Российскую Федерацию и пребывания (проживания) на территории Российской Федерации иностранных граждан<sup>2</sup>.

Безусловно, такая авторская позиция отражает современную тенденцию в области совершенствования миграционной политики. Поэтому хочется более детально рассмотреть вопрос использования данного профиля, особенно в отношении особых и чувствительных персональных данных – биометрических.

Однозначно, создание цифрового профиля иностранного гражданина предусматривает сбор не только информации о паспортных данных, но и получение дактилоскопической информации, изображения человека. В связи с этим не случайно в пунктах 8-10 Плана сделан акцент на биометрических персональных данных. Именно их сбор, обработка и хранение требуют обеспечения максимальной безопасности полученных данных.

Планом также предусмотрены:

– апробация сбора биометрических данных иностранных граждан в пунктах пропуска через государственную границу Российской Федерации аэропортов московского транспортного авиаузла;

---

<sup>1</sup> Далее – «План».

<sup>2</sup> Евсикова Е.В., Буц С.Б. Некоторые аспекты совершенствования миграционного контрольно-надзорного производства в аспекте введения «цифрового профиля мигранта» / Вопросы судебной деятельности и правоприменения в современных условиях: сборник статей по результатам II международной научно-практической конференции, Симферополь, 15 марта 2024 года. Симферополь: Ариал, 2024. С. 430.

– апробация процесса аутентификации иностранных граждан в пунктах пропуска через государственную границу Российской Федерации с использованием биометрических персональных данных, размещенных в единой биометрической системе;

– выдача карты иностранного гражданина в государственном бюджетном учреждении города Москвы «Многофункциональный миграционный центр», проведение государственной геномной регистрации и записи голоса иностранных граждан<sup>1</sup>.

Анализируя положения Плана с точки зрения цифрового профиля мигранта, сразу обращает на себя внимание тот факт, что предлагается расширить перечень биометрии, которую обязан предоставить мигрант при въезде в Россию. Кроме дактилоскопии и изображения человека, предлагается получать геномную информацию и запись голоса. Расширение перечня предоставляемых данных одновременно повышает требования к обеспечению безопасности их сбора, обработки и хранения, но при этом, посредством благ цифровизации, может позволить повысить оперативность по борьбе с нелегальной миграцией и раскрытием преступлений, совершенных мигрантами.

Как справедливо в своей статье отмечал А.В. Минбалеев, для обеспечения безопасности граждан и юридических лиц чрезвычайно важно исследовать и тщательно прорабатывать систему цифрового профилирования граждан сквозь призму защиты персональных данных, а также иной личной информации<sup>2</sup>.

Подводя итог проведенному анализу, можно отметить, что, безусловно, биометрические персональные данные представляют собой действенный способ в борьбе с незаконными миграционными процессами. Использование инструментов, полученных в процессе цифровизации общества (в том числе возможность создание цифрового профиля мигранта), способно повысить

<sup>1</sup> Распоряжение Правительства РФ от 16.01.2024 № 30-р «О Плате мероприятий по реализации в 2024-2025 гг. Концепции государственной миграционной политики РФ на 2019-2025 гг.» [Электронный ресурс]. – URL: <https://www.consultant.ru>.

<sup>2</sup> Минбалеев А.В. Понятие и правовая природа цифрового профиля человека // Вестник Южно-Уральского государственного университета. Серия: Право. 2022. Т. 22, № 1. С. 110.

качество миграционного контрольно-надзорного производства. При этом государственная политика нацелена на совершенствование миграционного вопроса и активно организует работу в данном направлении через изменения в действующем законодательстве и формирование исполнительной властью новых методик работы с мигрантами.

При проведении исследования по совершенствованию деятельности органов внутренних дел Российской Федерации по административно-правовой защите биометрических персональных данных установлено, что в перечне обязанностей полиции отсутствуют полномочия по привлечению к административной ответственности за совершение противоправных действий в исследуемой области. На сегодняшний день при обращении физического лица с заявлением о нарушении его прав в отношении его биометрических персональных данных, полномочия полиции ограничиваются необходимостью передачи сведений в подведомственность Роскомнадзора.

При этом при проведении нами анкетирования 78% респондентов на вопрос о том, в какое учреждение они обращались или обратились бы при нарушении их прав в отношении биометрических персональных данных заявили, что этим органом было (бы) МВД России. Общество воспринимает именно полицию гарантом защиты своих нарушенных прав. В связи с этим на законодательном уровне необходимо проработать вопрос о наделении правом на проведение административного расследования сотрудников органов внутренних дел. Это решение обусловлено тем фактом, что процесс цифровизации общественных отношений, вызвавший обострение проблемы защиты прав человека, ставит перед российской полицией новые задачи<sup>1</sup>.

Внедрение новых технологий и комплексных систем идентификации личности с использованием всех известных биометрических параметров человека позволит расширить круг задач, решаемых оперативно-разыскными и следственными подразделениями органов внутренних дел, чем внесет достойный вклад в

---

<sup>1</sup> Бучакова М.А., Мушаков В.Е. Оптимизация деятельности российской полиции по защите прав человека в условиях цифровизации // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2022. № 4. С. 13.

глобальную проблему борьбы с преступностью<sup>1</sup>. Именно одной из таких задач должно стать наделение МВД России более широким перечнем полномочий в области административно-правовой защиты биометрических персональных данных.

По нашему мнению, основываясь на результатах исследования, целесообразно рассмотреть вопрос выделения полномочий в трех основных направлениях:

1) возбуждение дел об административных правонарушениях в области защиты биометрических персональных данных должностными лицами МВД России. Эффективность в раскрытии преступлений в области киберпространства МВД уже доказана результатами деятельности. Так, за 2024 год было зарегистрировано 765,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Практически все такие преступления (98,7%) выявляются органами внутренних дел<sup>2</sup>. Следовательно, у МВД России есть все ресурсы для восстановления прав граждан в области защиты биометрии граждан.

2) рассмотрение дел об административных правонарушениях, связанных с нарушением действующего законодательства в области защиты биометрических персональных данных. Полиция как ключевой элемент системы обеспечения общественной безопасности обладает современными информационными системами и передовыми технологиями, что позволяет ей эффективно выявлять и расследовать правонарушения. Безусловно, это требует от правоохранительных органов высокого уровня профессионализма, компетентности и использования передовых технологий.

3) создание (участие в создании) единой базы биометрических персональных данных, которая будет аккумулировать все данные в одном ресурсе. Это обеспечит прозрачность сбора, обработки и хранения биометрических персональных данных. Важно при создании такой системы

---

<sup>1</sup> Барковская Е.Г. Использование биометрических технологий в процессе криминалистической идентификации // Юрист-Правоведъ. 2011. № 4(47). С. 14.

<sup>2</sup> Состояние преступности в Российской Федерации за январь–декабрь 2024 года [Электронный ресурс]. – URL: <https://мвд.рф/reports/item/60248328/> (дата обращения: 09.04.2025).

определить полномочия правоохранительных органов при взаимодействии с системой, предусмотреть фиксацию цифрового следа, чтобы исключить нецелевой доступ к биометрии.

В МВД России функционируют Департамент информационных технологий, связи и защиты информации (ДИТСиЗИ)<sup>1</sup> и Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УОБПИТ)<sup>2</sup>. Однако в Положениях о деятельности данных структурных подразделений МВД России отсутствует упоминание о направлении деятельности по защите биометрии. Важной задачей должно стать совершенствование деятельности указанных подразделений в вопросах защиты прав граждан в области биометрических персональных данных.

Актуальность использования биометрии, в том числе и в правоохранительной деятельности, требует выработки действенных мер по защите биометрии и актуализации деятельности полиции в данной области. Полагаем, что одной из эффективных мер могло бы стать создание «биометрического омбудсмана». Публичная деятельность полиции находится под особо пристальным вниманием общества. Перед правоохранительными органами стоит задача сделать публичным и открытым процесс сбора, обработки и хранения биометрических персональных данных. Необходимо освещение мер, применяемых для защиты биометрии, в качестве профилактики правонарушений в данной области. Важно предусмотреть и контрольно-надзорную деятельность омбудсмана в отношении самой системы, на него должна быть возложена обязанность по независимой проверке структурных подразделений МВД России на соблюдение действующего законодательства в области правового регулирования биометрических персональных данных. Безусловно, профилактика

---

<sup>1</sup> Приказ МВД России от 15 июня 2021 г. № 44 (ред. от 31.03.2025) «Об утверждении Положения о Департаменте информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации» // СПС «КонсультантПлюс».

<sup>2</sup> Приказ МВД России от 29 декабря 2022 г. № 1110 «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации» // СПС «КонсультантПлюс».

данного направления находится в ведении Роскомнадзора, но этого недостаточно, необходима системная работа в данной области. В полномочия биометрического омбудсмена необходимо включить его участие во взаимодействии с иными организациями в целях формирования действенной политики по административно-правовой защите биометрических персональных данных. Нам кажется важным реализовать принцип государственного управления, когда «бездействие конкретного органа власти (или недостаточное реагирование на нарушение закона) должно «компенсироваться» реакцией другого органа»<sup>1</sup>.

Хотелось бы отметить, что создание «биометрического омбудсмена» должно быть эффективным инструментом в реализации и защите прав не только физических лиц, сдающих биометрию, но сотрудников правоохранительных органов, подлежащих прохождению обязательной государственной дактилоскопической регистрации.

Дополнительно в рамках исследования считаем необходимым рассмотреть Инструкцию по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации, утвержденную Приказом МВД России от 6 июля 2012 г. № 678<sup>2</sup> (далее – Инструкция). Данная Инструкция разработана в целях обеспечения реализации требований законодательства Российской Федерации в области защиты персональных данных при их автоматизированной обработке. Однако биометрические персональные данные не нашли в ней своего отражения. Возможно это следствие того, что биометрия включена в общую совокупность персональных данных. Такая позиция на сегодняшний день является неактуальной и требует своего совершенствования. На общем фоне законодательной тенденции к обособлению биометрии в отдельную категорию

---

<sup>1</sup> Позднякова Е.В. Субъекты управления в сфере обеспечения безопасности государства и защиты жизненных ценностей граждан // Научный вестник Омской академии МВД России. 2024. Т. 30, № 3(94). С. 251.

<sup>2</sup> Приказ МВД России от 6 июля 2012 г. № 678 «Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации» // Российская газета. 2012. № 230.

данных в Инструкцию необходимо внести изменения, касающиеся правой защиты биометрических данных (Приложение 5).

Подводя итог исследованию в рамках данного параграфа, отметим следующее.

1. Биометрические данные, интегрированные в правоохранительные системы, демонстрируют высокую эффективность в контексте идентификации, расследования преступлений и обеспечения общественной безопасности. Тем не менее, их использование влечет за собой целый спектр этических, правовых и социальных дилемм, связанных с вопросами конфиденциальности, потенциальной дискриминации и рисков злоупотребления.

2. В рамках исследования, направленного на оптимизацию функционирования органов внутренних дел Российской Федерации в контексте административно-правовой защиты биометрических персональных данных, были выявлены существенные пробелы в правовом регулировании данной сферы в оперативно-разыскной деятельности. В частности, отсутствует детальная регламентация процедур сбора и обработки биометрических персональных данных, включая отсутствие четко определенного перечня биометрических характеристик, подлежащих идентификации.

Следует отметить, что в контексте правоохранительной деятельности не требуется предварительное согласие субъекта биометрических данных, как это предусмотрено для добровольной регистрации. Однако, по нашему мнению, необходимо разработать альтернативные механизмы информирования субъектов, такие как письменное уведомление с перечнем биометрических данных, которые будут использоваться в оперативно-разыскных мероприятиях, с обязательным ознакомлением субъекта и получением подписи.

Дополнительно необходимо разработать и внедрить систему контроля за использованием биометрических персональных данных в оперативно-разыскной деятельности.

3. В структуре Министерства внутренних дел Российской Федерации функционируют два ключевых подразделения, занимающихся вопросами

информатизации и кибербезопасности: Департамент информационных технологий, связи и защиты информации (ДИТСиЗИ) и Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УОБПИТ). Несмотря на значимость этих структур, в Положениях об их деятельности отсутствует упоминание о защите биометрических данных, что является существенным пробелом в правовом регулировании.

Совершенствование деятельности ДИТСиЗИ и УОБПИТ в контексте защиты биометрических данных является задачей, требующей системного подхода и координации усилий на межведомственном уровне. Это предполагает разработку и внедрение комплекса мер, направленных на обеспечение конфиденциальности, целостности и доступности биометрической информации, а также на предотвращение ее несанкционированного использования.

Интеграция вопросов защиты биометрии в деятельность ДИТСиЗИ и УОБПИТ является необходимым условием для обеспечения высокого уровня информационной безопасности в правоохранительной сфере и защиты прав и свобод граждан.

4. Формирование современного кадрового потенциала МВД России требует комплексного подхода, включающего привлечение специалистов технических профессий и создание оптимальных условий для их эффективной работы в сфере информационных технологий. В условиях цифровизации правоохранительных органов этот аспект приобретает особую значимость, поскольку технические компетенции играют ключевую роль в обеспечении информационной безопасности и оперативности принятия решений.

Особое внимание следует уделить вопросам соблюдения этических норм при обработке биометрических персональных данных граждан и сотрудников органов внутренних дел. В контексте растущей угрозы кибератак и утечки конфиденциальной информации соблюдение этических стандартов становится не только моральным императивом, но и стратегическим фактором, обеспечивающим доверие общества к правоохранительным органам.

## ЗАКЛЮЧЕНИЕ

Государственная политика в отношении биометрических персональных данных в Российской Федерации ориентирована на централизацию управления и контроля за сбором, обработкой и хранением биометрических характеристик физических лиц. Это обусловлено сущностью биометрических персональных данных как правовой категории, требующей строгой реализации конституционного права на неприкосновенность частной жизни и гарантий защиты биометрических персональных данных от неправомерного доступа, использования, распространения и уничтожения.

Биометрия – динамично развивающаяся область общественных отношений, и задача законодательных органов постоянно совершенствовать правовые нормы, регулирующие вопросы административно-правовой защиты биометрических персональных данных. Существующие на сегодняшний день правовые пробелы требуют дополнительного внимания к проблеме применения действующего законодательства.

К числу наиболее значимых выводов как в теоретическом, так и в практическом аспектах относятся следующие.

1. История становления биометрических персональных данных как юридической категории обусловлена этапами развития института идентификации личности. Возникновение автоматизированных систем идентификации, в том числе с использованием искусственного интеллекта, обусловило расширение области применения биометрических персональных данных, произошла эволюция, когда биометрия стала идентификатором не только в криминалистике, но в гражданских правоотношениях.

2. Расширение возможностей автоматизированной идентификации создало предпосылки для применения большего количества биометрических характеристик. Кроме статических биометрических персональных данных активно стали использоваться поведенческие маркеры. Вследствие этого, возникла необходимость совершенствования понятия «биометрические персональные данные».

Комплексное исследование международных правовых актов действующего законодательства Российской Федерации, мнения ведущих ученых в области защиты биометрических персональных данных позволили сформировать следующее определение.

Под биометрическими персональными данными следует понимать сведения, относящиеся к физиологическим и поведенческим характеристикам физического лица, полученные в целях идентификации и (или) аутентификации в результате специальной технической обработки, в том числе с использованием автоматизированных систем.

Обосновано использование термина «биометрия» в отношении биометрических персональных данных как правовой категории. Основываясь на мнении ученых, общественных деятелей, установлено, что возможно употребление биометрии как синонима биометрических персональных данных.

3. Установлено, что биометрические персональные данные как правовая категория должны удовлетворять общим и специальным признакам. При этом цель сбора, обработки и хранения физиологических или поведенческих характеристик является определяющей в перечне общих признаков. Цель обработки биометрических персональных данных заключается в проведении идентификации и (или) аутентификации.

К числу специальных признаков, обуславливающих необходимость защиты биометрических персональных данных относятся уникальность, невозможность восстановления утраченных данных, высокий риск необратимых последствий при утечке, этический аспект (соблюдение принципа неприкосновенности частной жизни).

В качестве дополнительных мер мы предлагаем ввести обязательное обучение должностных лиц органов публичной власти, операторов систем биометрических персональных данных основам этических норм по работе с субъектами биометрии.

4. Конституционное регулирование в области защиты биометрических персональных данных осуществляется по принципу построения баланса между

интересами государства и граждан. Это обуславливает необходимость специального правового режима с усиленными мерами защиты. В настоящее время система административно-правового регулирования защиты биометрических персональных данных в России находится на стадии своего активного формирования.

5. Предлагаем понимать под мерами административно-правовой защиты биометрических персональных данных совокупность административно-правовых мер, в том числе организационного и принудительного характера, применяемых органами публичной власти и иными участниками правовых отношений в области защиты биометрических персональных данных, направленных на нейтрализацию и устранение угроз в данной области, а также предусматривающие юрисдикционную деятельность в сфере защиты биометрии.

Особенность административно-правовой защиты биометрических персональных данных заключается в необходимости реализации одновременно правовых, технических, организационных и информационных мер.

В связи с чем административная ответственность в области защиты биометрических персональных данных устанавливается за правонарушения, совершаемые за противоправное, виновное действие (бездействие) при реализации указанных мер.

6. Установлено, что объектом административного правонарушения в области защиты биометрических персональных данных является установленный государством порядок в сфере информации и связи, обеспечивающий реализацию конституционных прав граждан на неприкосновенность частной жизни и защиту персональных данных, а также конкретные общественные отношения, гарантирующие соблюдение специального правового режима обработки, конфиденциальности и безопасности уникальных биометрических характеристик человека.

7. Проведенный анализ показал, что за административные правонарушения в области защиты биометрии предусмотрена административная ответственность за общие нормы (для всех персональных данных) и специальные (только для

биометрических данных). При этом в рамках исследования установлено, что неправомерные действия в отношении биометрии должны расцениваться как более тяжкие нежели правонарушения в отношении традиционных персональных данных. Это обусловлено природой биометрических персональных данных – невозможностью (в большей степени) к восстановлению утраченной конфиденциальности, и как следствие невозможность последующей идентификации по утраченным данным.

В связи с этим предлагаем выделить правонарушения данного вида в отдельные составы в соответствии с действующим законодательством и предусмотреть достаточно жесткие меры административной ответственности в качестве инструмента упреждающего характера.

8. Установлено, что согласие на обработку биометрических персональных данных на сегодняшний день является гарантом добровольности.

Однако часто его получают недобросовестно и по халатности самого субъекта биометрических характеристик.

Также складывается еще один тип ситуации, когда согласие не требуется – проведение процессуальных действий (например, в рамках допроса, следственного эксперимента). В данном случае следователь может взять образцы голоса или отпечатки пальцев, при этом разъяснив в рамках какого дела и для чего это делается (фактически, это форма уведомления о цели сбора). Данная процедура отражается в протоколе, который подписывает субъект биометрических персональных данных.

При этом существует пробел, когда сведения запрашиваются правоохранительными органами в Единой биометрической системе. Безусловно, орган направляет запрос на предоставление доступа к идентификатору, однако субъект биометрических персональных данных остается в неведении. Предлагаем предусмотреть создание автоматического уведомления, которое будет направлено в кабинет Госуслуг физического лица при совершении действия в отношении его биометрической информации.

9. В действующей редакции КоАП РФ правонарушения в области защиты биометрических персональных данных отражены не только в главе 13 «Административные правонарушения в области связи и информации», но и в главе 5 «Административные правонарушения, посягающие на права граждан» (часть 2.1 статьи 5.63) и главе 14 «Административные правонарушения в области предпринимательской деятельности и деятельности саморегулируемых организаций» (статья 14.8). Считаем, что необходимо систематизировать данные нормы и объединить их в единой специализированной главе. Объединение норм, регулирующих правонарушения в этой области, в рамках единой главы позволит обеспечить комплексный и систематизированный подход к защите прав и свобод граждан в контексте использования биометрических технологий.

10. Установлено, что в правовой науке существует дискуссия о сущности дипфейков и их юридической оценке. Позиция законодательства весьма неопределенна в данном вопросе. Однако прецеденты, связанные с утратой конфиденциальности биометрическими персональными данными в результате создания дипфейка имеют место быть. Установлено, что дипфейк – это инструмент, а спуфинг – процесс (несанкционированный доступ).

Целесообразно внести изменения в Федеральный закон от 29 декабря 2022 г. № 572-ФЗ и закрепить понятия дипфейка и спуфинга:

дипфейк биометрических персональных данных – это воссоздание биометрических характеристик человека посредством использования искусственного интеллекта в целях совершения несанкционированного доступа при идентификации личности;

спуфинг с использованием биометрических персональных данных – это использование дипфейка на основе биометрических характеристик в целях совершения неправомерной идентификации личности, ведущее к несанкционированному доступу.

11. Система органов публичной власти, осуществляющих защиту биометрических персональных данных – это совокупность органов публичной власти всех уровней (федеральных, субъектов Российской Федерации, местных) и

организаций, осуществляющих взаимодействие по сбору, обработке и хранению биометрических персональных данных в установленных действующим законодательствах целях и реализующих меры по обеспечению правовой и технической безопасности полученных данных с соблюдением этических норм в отношении полученных данных.

Систему органов публичной власти, осуществляющих защиту биометрических персональных данных в Российской Федерации, можно представить в виде групп, подразделяемых по классифицирующим признакам.

I. Территориальность уровней управления: федеральный, региональный, местный.

II. Цель сбора, обработки и хранения биометрических персональных данных: органы и организации, осуществляющие сбор, обработку и хранение биометрических персональных данных для осуществления гражданских правоотношений (Центральный банк России, многофункциональные центры); органы и организации, осуществляющие сбор, обработку и хранение биометрических персональных данных для обеспечения безопасности государства и общества (ФСБ России, МВД России и другие).

III. Направление деятельности органов публичной власти в обеспечении защиты биометрических персональных данных: законодательные органы, исполнительные и контролирующие органы.

12. В ходе исследования рассмотрены меры административно-правовой защиты биометрических персональных данных, которые предполагают разделение их в две группы: общие и специальные.

Для общих мер административно-правовой защиты характерным является государственно-властный характер. Данные меры регламентируются законодательно и осуществляются в условиях государственной политики по цифровизации общества. К таким мерам целесообразно отнести методологические, правовые, организационные и технические меры.

К группе специальных мер относятся информационные меры, этические меры и судебная защита. Данная группа мер направлена на субъект

биометрических персональных данных и реализации им самостоятельно своих прав при поддержке государства.

13. Установлено, что у полиции отсутствуют полномочия по привлечению к административной ответственности за совершение противоправных действий в исследуемой области. На сегодняшний день при обращении физического лица с заявлением о нарушении его прав в отношении его биометрических персональных данных, полномочия полиции ограничиваются необходимостью передачи сведений в подведомственность Роскомнадзора.

Это представляет собой определенный пробел. МВД России обладает значительным опытом в раскрытии правонарушений и преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Как результат, наделение полиции полномочиями по расследованию административных правонарушений способствовало бы повышению доверия граждан к правоохранительным органам.

14. Публичная деятельность полиции находится под особо пристальным вниманием общества. Перед правоохранительными органами стоит задача сделать публичным и открытым процесс сбора, обработки и хранения биометрических персональных данных. Также необходимо освещение мер, применяемых для защиты биометрии в качестве профилактики правонарушений в данной области.

Особенность правоохранительных органов заключается в том, что они одновременно являются операторами биометрических персональных данных, а подведомственные сотрудники являются субъектами биометрии. В связи с чем актуальным является создание «биометрического омбудсмана». На него должна быть возложена обязанность по независимой проверке структурных подразделений МВД России на соблюдение действующего законодательства в области правового регулирования биометрических персональных данных. В полномочия биометрического омбудсмана значимо предусмотреть его участие во взаимодействии с иными организациями, в целях формирования действенной политики по административно-правовой защите биометрических персональных данных.

15. Комплексный анализ статистических данных практической деятельности и судебной практики показал, что определенную сложность представляет собой выделение материалов о правонарушениях в области защиты биометрических персональных данных. Открытые статистические данные о неправомерных действиях, результаты их пресечения и информация о применяемых мерах административной ответственности способны благоприятно сказаться на репутации биометрических персональных данных в качестве идентификатора, а также способствовать проведению профилактических мероприятий, направленных на административно-правовую защиту биометрических характеристик граждан.

## СПИСОК ЛИТЕРАТУРЫ

### Нормативные правовые акты и официальные документы

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Собрание законодательства Российской Федерации. – 2009. – № 4. – Ст. 445.

2. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства Российской Федерации. – 2002. – № 1 (часть I). – Ст. 1.

3. Федеральный закон от 3 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» // Собрание законодательства Российской Федерации. – 2008. – № 49. – Ст. 5740.

4. Федеральный закон от 15 августа 1996 г. № 114-ФЗ «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию» // Собрание законодательства Российской Федерации. – 1996. – № 34. – Ст. 4029.

5. Федеральный закон от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации» // Собрание законодательства Российской Федерации. – 1998. – № 31. – Ст. 3806.

6. Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 06.02.2023) «О персональных данных» // Собрание законодательства Российской Федерации. – 2006. – № 31 (часть 1). – Ст. 3451.

7. Федеральный закон от 28 февраля 2023 г. № 43-ФЗ «О прекращении действия в отношении Российской Федерации международных договоров Совета Европы» // Собрание законодательства Российской Федерации. – 2023. – № 10. – Ст. 1566.

8. Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные

законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства Российской Федерации. – 2023. – № 1 (часть I). – Ст. 19.

9. Федеральный закон от 3 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации // Собрание законодательства Российской Федерации. – 2008. – № 49. – Ст. 5740.

10. Федеральный закон от 30 ноября 2024 г. № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» [Электронный ресурс]. – URL: <http://publication.pravo.gov.ru> (дата обращения: 11.03.2025).

11. Федеральный закон от 6 февраля 2023 г. № 8-ФЗ «О внесении изменений в Федеральный закон «О государственной геномной регистрации в Российской Федерации» и отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. – 2023. – № 6. – Ст. 915.

12. Федеральный закон от 7 мая 2013 г. № 99-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» и Федерального закона «О персональных данных» // Собрание законодательства Российской Федерации. – 2013. – № 19. – Ст. 2326.

13. Федеральный закон от 8 декабря 2020 г. № 394-ФЗ «О Государственном Совете Российской Федерации» // Собрание законодательства Российской Федерации. – 2020. – № 50 (часть III). – Ст. 8039.

14. Постановление Правительства Российской Федерации от 22 мая 2023 г. № 810 «Об утверждении Правил аккредитации организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, оснований ее приостановления и прекращения и признании утратившим силу постановления Правительства Российской Федерации от 20 октября 2021 г. № 1799» / Официальный сайт Министерства цифрового развития, связи и

массовых коммуникаций Российской Федерации [Электронный ресурс]. – URL: <https://digital.gov.ru/documents/> (дата обращения: 06.04.2025).

15. Постановление Правительства Российской Федерации от 29 декабря 2022 г. № 2511 «О Координационном совете по развитию цифровых технологий идентификации и аутентификации на основе биометрических персональных данных» // Собрание законодательства Российской Федерации. – 2023. – № 1. Ст. 312 (часть II).

16. Указ Президента Российской Федерации от 21 декабря 2016 г. № 699 «Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации» / Собрание законодательства Российской Федерации. – 2016. – № 52 (часть V). – Ст. 7614.

17. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы // Собрание законодательства Российской Федерации. – 2017. – № 20. – Ст. 2901.

18. Постановление Правительства Российской Федерации от 15 июня 2022 г. № 1067 «О случаях и сроках использования биометрических персональных данных, размещенных физическими лицами в единой биометрической системе с использованием мобильного приложения единой биометрической системы» // Собрание законодательства Российской Федерации – 2022. – № 25. – Ст. 4337.

19. Постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» // Собрание законодательства Российской Федерации. – 2009. – № 12. – Ст. 1431.

20. Постановление Правительства Российской Федерации от 22 мая 2023 г. № 810 «Об утверждении Правил аккредитации организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, оснований ее приостановления и прекращения и признании утратившим силу постановления Правительства Российской Федерации от 20 октября 2021 г.

№ 1799» // Собрание законодательства Российской Федерации. – 2023. – № 22. – Ст. 3945.

21. Постановление Правительства Российской Федерации от 25 июня 2022 г. № 1140 «О порядке применения персонифицированной карты для посещения спортивного соревнования, а также идентификации и аутентификации зрителей, участников официального спортивного соревнования, иных лиц, задействованных в проведении такого соревнования» (с изм. и доп.) // Собрание законодательства Российской Федерации. – 2022. – № 27. – Ст. 4835.

22. Постановление Правительства Российской Федерации от 28 декабря 2018 г. № 1703 «О предоставлении оператором единой биометрической системы и оператором регионального сегмента единой биометрической системы в Министерство внутренних дел Российской Федерации и Федеральную службу безопасности Российской Федерации сведений, содержащихся в единой биометрической системе и региональном сегменте единой биометрической системы» // Собрание законодательства Российской Федерации. – 2018. – № 53 (часть II). Ст. 8727.

23. Постановление Правительства РФ от 30 июня 2018 г. № 772 «Об определении состава сведений, размещаемых в единой биометрической системе, в том числе в ее региональных сегментах, а также о внесении изменений в некоторые акты Правительства Российской Федерации» // Собрание законодательства Российской Федерации. – 2018. – № 28. – Ст. 4234.

24. Постановление Правительства РФ от 31 мая 2023 г. № 883 «Об утверждении Положения о единой биометрической системе, в том числе о ее региональных сегментах, и о признании утратившим силу постановления Правительства Российской Федерации от 16 июня 2022 г. № 1089» [Электронный ресурс]. – URL: <http://publication.pravo.gov.ru/document/0001202306010068>.

25. Распоряжение Правительства Российской Федерации от 16 марта 2024 г. № 637-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления» // Собрание законодательства Российской Федерации. – 2004. – № 43. – Ст. 4169.

26. Распоряжение Правительства Российской Федерации от 16 января 2024 г. № 30-р «О Плана мероприятий по реализации в 2024–2025 гг. Концепции государственной миграционной политики РФ на 2019-2025 гг.» // СПС «КонсультантПлюс».

27. Приказ МВД России от 15 июня 2021 г. № 44 (ред. от 31.03.2025) «Об утверждении Положения о Департаменте информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации» // СПС «КонсультантПлюс».

28. Приказ МВД России от 29 декабря 2022 г. № 1110 «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации» // СПС «КонсультантПлюс».

29. Приказ МВД России от 6 июля 2012 г. № 678 «Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации» / Российская газета. 2012. № 230.

30. Приказ МВД России от 19 июня 2018 г. № 384 «Об утверждении Порядка проведения идентификации личности человека по отпечаткам пальцев (ладоней) рук в режиме реального времени и Перечня категорий лиц, в отношении которых обязательная государственная дактилоскопическая регистрация не проводится в случае идентификации их личности в результате проверки по отпечаткам пальцев (ладоней) рук в режиме реального времени» // СПС «КонсультантПлюс».

31. Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 31 марта 2023 г. № 333 «Об утверждении Методики расчета показателя «Доля массовых и государственных сервисов, обеспеченных возможностью их получения с использованием цифрового профиля гражданина» федерального проекта «Цифровое государственное управление» национальной программы «Цифровая экономика Российской Федерации» и внесении изменений в некоторые приказы Министерства цифрового развития, связи и массовых

коммуникаций Российской Федерации об утверждении методик расчета показателей федеральных проектов национальной программы «Цифровая экономика Российской Федерации» // СПС «КонсультантПлюс».

32. Приказ Минцифры России от 17 апреля 2023 г. № 378 «Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица соответствующим векторам единой биометрической системы и определении степени взаимного соответствия биометрических персональных данных и векторов единой биометрической системы, достаточной для проведения идентификации и (или) аутентификации» // СПС «КонсультантПлюс».

33. Приказ Минцифры России от 5 мая 2023 г. № 446 «Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением организаций финансового рынка, и единой биометрической системы, а также актуальных при взаимодействии информационных систем государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов с указанными информационными системами, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных» // СПС «КонсультантПлюс».

34. Приказ Минцифры России от 6 марта 2025 г. № 150 «Об утверждении доклада о правоприменительной практике организации и осуществления федерального государственного контроля (надзора) в сфере идентификации и (или) аутентификации в 2024 году» // СПС «КонсультантПлюс».

**Монографии, учебники, учебные пособия, научные публикации  
и статьи в иных периодических изданиях**

35. Аврутин, Ю. Е. О парадигме государственного управления в контексте модернизации российского административного права / Ю. Е. Аврутин / Актуальные проблемы административного и административно-процессуального права: сборник статей по материалам ежегодной всероссийской научно-практической конференции (Сорокинские чтения), посвященной 70-летию доктора юридических наук, профессора, заслуженного деятеля науки Российской Федерации, заслуженного юриста Российской Федерации Аврутина Юрия Ефремовича: в 3 частях, Санкт-Петербург, 24 марта 2017 года. – Санкт-Петербург: Санкт-Петербургский университет МВД России, 2017. Часть 1. – С. 32–47.

36. Административное право: учебник / под ред. Л.Л. Попова, М.С. Студеникиной. – 3-е изд., перераб. и доп. – Москва: Норма: ИНФРА-М, 2025. – 736 с.

37. Административное право в схемах: учебник и практикум для вузов / под ред. А.И. Стахова, П.И. Кононова. – 4-е изд., перераб. и доп. – Москва: Юрайт, 2025. – 501 с.

38. Административное право России: учебник для студентов вузов, обучающихся по специальности 030501 «Юриспруденция» / под ред. П.И. Кононова, В.Я. Кикотя, И.Ш. Килясханова. – 3-е изд., перераб. и доп. – Москва: ЮНИТИ-ДАНА: Закон и право, 2015. – 559 с.

39. Акаткин, Ю. М. Цифровая трансформация правительства датацентричность и модели-ориентированность / Ю. М. Акаткин, Е. Д. Ясиновская // Информационные ресурсы России. – 2019. – № 1(167). – С. 2–7.

40. Актуальные проблемы бухгалтерского учета, аудита и анализа в современных условиях: монография / Н. Н. Бондина, И. А. Бондин, К. А. Бабенчук [и др.]; под ред. Н.Н. Бондиной. – Пенза: Пензенский государственный аграрный университет, 2023. – 263 с.

41. Алгулиев, Р. М. Методы обнаружения живучести в биометрических системах / Р. М. Алгулиев, Я. Н. Имамвердиев, В. Я. Мусаев // Вопросы защиты информации. – 2009. – № 3(86). – С. 16–21.

42. Александров, А. Н. Организационно-правовые аспекты применения полицией специальных технических средств противодействия беспилотным воздушным судам / А. Н. Александров, О. А. Дизер / Актуальные проблемы полицейского права: материалы международной научно-практической конференции, Омск, 1–2 июня 2023 года. – Омск: Омская академия МВД России, 2023. – С. 3–7.

43. Амельчакова, В. Н. Соотношение вины и субъективной стороны административного правонарушения / В. Н. Амельчакова, Г. Н. Суслова // Вестник Московского университета МВД России. – 2023. – № 3. – С. 23–26.

44. Артамонова, Я. В. Биометрические технологии: отношение населения и преодоление рисков / Я. В. Артамонова, С. С. Барсуков, А. А. Суханова // Государственное и муниципальное управление. Ученые записки. 2024. № 1. С. 231–236.

45. Архипов, В. В. Теоретико-правовые вопросы охраны прав человека при использовании биометрических данных системами искусственного интеллекта: европейский опыт / В. В. Архипов, В. Б. Наумов // Вестник Удмуртского университета. Серия Экономика и право. – 2022. – Т. 32, № 1. – С. 109–118.

46. Асянова, С. Р. Спуфинг как угроза кибербезопасности: понятие, виды, меры противодействия / С. Р. Асянова, Я. И. Жигалова // Журнал монетарной экономики и менеджмента. – 2024. – № 11. – С. 242–247.

47. Баженов, С. А. Создание Концепции национальной системы биометрической идентификации личности / С. А. Баженов, В. Е. Дивольд, А. А. Морозов, Д. В. Попов, Д. М. Сафронов, А. В. Серов // Труды Академии управления МВД России. – 2020. – № 2 (54). – С. 41–53.

48. Барковская, Е. Г. Использование биометрических технологий в процессе криминалистической идентификации / Е. Г. Барковская // Юрист-Правоведь. – 2011. – № 4(47). – С. 10–13.

49. Барковская, Е. Г. Исторические предпосылки и практические потребности интеграции биометрического и криминалистического знания / Е. Г. Барковская // Философия права. – 2010. – № 6(43). – С. 28–31.

50. Барсуков, С. С. Криминалистическая идентификация по радужной оболочке и сетчатке глаза: современные возможности и проблемы применения / С. С. Барсуков // Юрист-Правоведъ. – 2021. – № 1(96). – С. 170-175.

51. Башкирова, О. В. Цифровой профиль гражданина: мировая практика создания и применения / О. В. Башкирова, О. И. Долганова, Б. Б. Славин // Информационное общество. – 2023. – № 2. – С. 134–144.

52. Безверхов, А. Г. Биометрия и право: вопросы теории и права / Безверхов А. Г., Юдин А. В. // Юридический вестник Самарского университета. – 2021. – Т. 7, № 1. – С. 7–8.

53. Белая, О. В. Биометрические данные как средство идентификации и аутентификации человека: российский и международный опыт / О. В. Белая, Ю. А. Кицай // Право и практика. – 2020. – № 1. – С. 85–89.

54. Бондарь, К. М. Современные цифровые технологии для коррегирования социального взаимодействия населения с сотрудниками и обучающимися правоохранительных органов / К. М. Бондарь, В. С. Дунин, А. В. Кантышева // Мир науки, культуры, образования. – 2024. – № 6(109). – С. 70–73.

55. Брюхомицкий, Ю. А. Биометрические технологии идентификации личности: учебное пособие / Ю. А. Брюхомицкий. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2017. – 288 с.

56. Бурлака, С. Н. Защита биометрических персональных данных: проблемы правового регулирования / С. Н. Бурлака, О. Г. Бельдина // Право и государство: теория и практика. – 2023. – № 10(226). – С. 277–279.

57. Буряков, Е. В. Использование достижений науки в розыскной и идентификационной деятельности / Е. В. Буряков // Вестник Уфимского юридического института МВД России. – 2023. – № 3 (101). – С. 53–59.

58. Бучакова, М. А. Оптимизация деятельности российской полиции по защите прав человека в условиях цифровизации / М. А. Бучакова, В. Е. Мушаков //

Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2022. – № 4. – С. 9–13.

59. Вайпан, В. А. Источники цифрового права / В. А. Вайпан // Вестник арбитражной практики. – 2024. – № 1(110). – С. 3–29.

60. Васильев, Г. С. Человеческий биоматериал как объект права / Г. С. Васильев // Правоведение. – 2018. – № 2(337). – С. 308–361.

61. Виноградова, Е. В. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации / Е. В. Виноградова, Т. А. Полякова, А. В. Минбалеев // Правоприменение. – 2021. – Т. 5, № 4. – С. 5–19.

62. Возгрин, И. А. История возникновения и развития криминалистики / И. А. Возгрин // Вестник Санкт-Петербургского университета МВД России. – 2000. – № 2(6). – С. 87–94.

63. Волков, П. А. Современный подход к определению понятия административной ответственности / П. А. Волков // Известия Российского государственного педагогического университета имени А.И. Герцена. – 2008. – № 82-1. – С. 93–96.

64. Волкова, С. С. Метод обнаружения технологии манипуляции с идентичностью лиц с применением сверточных нейронных сетей / С. С. Волкова // Искусственный интеллект и принятие решений. – 2022. – № 2. – С. 62–73.

65. Гаврилова, Ю. А. Конституционализация информационной безопасности в российском праве: проблема совершенствования теоретической модели / Ю. А. Гаврилова // Вестник Российского университета дружбы народов. Серия: Юридические науки. – 2023. – Т. 27, № 1. – С. 97–116.

66. Галиуллина, Д. Р. Биометрические персональные данные / А. Л. Гогаева // Документ. Архив. История. Современность. – 2015. – Т. 15. – С. 264–268.

67. Гогаева, А. Л. Сферы практического внедрения биометрических технологий идентификации личности для решения правоохранительных задач органов полиции / А. Л. Гогаева / Инновационные технологии производства и переработки сельскохозяйственной продукции: материалы всероссийской научно-практической конференции, Владикавказ, 30–31 марта 2021 года. В 2-х ч. –

Владикавказ: Горский государственный аграрный университет, 2021. Ч. 2. – С. 179–181.

68. Государственное регулирование Интернета и права человека / М. С. Саликов, С. Э. Несмеянова, Н. Е. Колобаева [и др.]. – Екатеринбург: УМЦ УПИ, 2022. – 220 с.

69. Грачев, Н. И. Публичная власть как политико-правовая категория: понятие, основные признаки и формы / Н. И. Грачев // Вестник Волгоградской академии МВД России. – 2020. – № 4(55). – С. 8–19.

70. Гуртовая, К. А. Актуальные проблемы безопасности хранения персональных данных клиентов / К. А. Гуртовая, А. Г. Окунева // Вестник Самарского государственного экономического университета. – 2025. – № 1(243). – С. 106–113.

71. Гусев, В. А. Цифровая гигиена vs. киберпреступность / В. А. Гусев // Психопедагогика в правоохранительных органах. – 2022. – Т. 27, № 1(88). – С. 102–108.

72. Гусева, Т. А. Цифровизация в публично-правовой и частно-правовой сферах: монография / Т. А. Гусева. – Орел: Орловский государственный университет имени И.С. Тургенева, 2024. – 90 с.

73. Данелян, Р. Н. Особенности правового регулирования биометрических персональных данных в Российской Федерации / Р. Н. Данелян, В. А. Яковлев-Чернышев // Вестник Казанского юридического института МВД России. – 2024. – Т. 15, № 3(57). – С. 26–33.

74. Денисович, В. В. Особенности применения современных цифровых технологий в сфере охраны персональных данных / В.В. Денисович, А.В. Кудряшов, Л.Ю. Перемолотова // Правопорядок: история, теория, практика. – 2024. – № 4 (43). – С. 100–106.

75. Дивольд, В. Е. Предпосылки создания национальной системы биометрической идентификации личности / В. Е. Дивольд // Научный вестник Омской академии МВД России. – 2021. – Т. 27, № 2(81). – С. 139–143.

76. Дизер, О. А. Административно-правовая охрана общественного порядка и общественной безопасности в условиях формирования цифрового пространства / О. А. Дизер // Вестник Уфимского юридического института МВД России. – 2020. – № 3(89). – С. 63–70.

77. Дизер, О. А. Совершенствование административно-правовой защиты прав граждан в условиях формирования и развития информационного общества / О. А. Дизер / Актуальные проблемы административного и административно-процессуального права (Сорокинские чтения): материалы Международной научно-практической конференции, Санкт-Петербург, 26 марта 2021 г. – Санкт-Петербург: Санкт-Петербургский университет МВД России, 2021. – С. 64–67.

78. Динамические методы биометрической аутентификации / А. А. Островский, Д. Н. Жариков, В. С. Лукьянов, Д. С. Попов // Известия Волгоградского государственного технического университета. – 2010. – № 6(66). – С. 72–76.

79. Добробаба, М. Б. Выработка правовых средств адаптации к санкционным мерам в сфере ИТ-сектора / М. Б. Добробаба, А. В. Минбалеев // Журнал Сибирского федерального университета. Серия: Гуманитарные науки. – 2024. – Т. 17, № 6. – С. 1047–1066.

80. Добробаба, М. Б. Дипфейки как угроза правам человека / М. Б. Добробаба // Lex Russica (Русский закон). – 2022. – Т. 75, № 11(192). – С. 112–119.

81. Добробаба, М. Б. Проблема обеспечения безопасности персональных данных, обрабатываемых с использованием систем искусственного интеллекта / Российская правовая система: в поисках национальной идентичности: сборник докладов XIV Московской юридической недели, Москва, 26–29 ноября 2024 г. В 6-ти ч. – Москва: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2025. – С. 119–124.

82. Долганова, О. И. Сотрудничество стран Азии в области цифровой идентификации личности / О. И. Долганова // Азия и Африка сегодня. – 2023. – № 7. – С. 42–48.

83. Долганова, О. И. Цифровой профиль гражданина: необходимый и достаточный набор персональных данных / О. И. Долганова, Е. В. Васильева, Д. А. Рябов // Вопросы инновационной экономики. – 2022. – Т. 12, № 3. – С. 1523–1540.

84. Долженко, Н. И. Криминалистические генетические базы данных: отечественный и зарубежный опыт использования / Н. И. Долженко, Е. А. Купряшина, Н. С. Подмоков // Современный ученый. – 2023. – № 1. – С. 258–263.

85. Дроздов, А. В. Криминалистическая идентификация по радужной оболочке глаза / А. В. Дроздов // Вестник Сибирского юридического института ФСКН России. – 2013. – № 1(12). – С. 82–87.

86. Дугенец, А. С. Актуальные проблемы противодействия административным правонарушениям, совершаемым с использованием информационных технологий / А. С. Дугенец, Н. Г. Канунникова // Пробелы в российском законодательстве. – 2024. – Т. 17, № 4. – С. 23-29.

87. Дугенец, А. С. Государственное регулирование обеспечения информационной безопасности несовершеннолетних как составляющая национальной безопасности России / А. С. Дугенец, Л. В. Павлова // Административное право и процесс. – 2023. – № 5. – С. 22-25.

88. Евсикова, Е. В. Некоторые аспекты усовершенствования миграционного контрольно-надзорного производства в аспекте введения «цифрового профиля мигранта» / Е. В. Евсикова, С. Б. Буц // Вопросы судебной деятельности и правоприменения в современных условиях: сборник статей II международной научно-практической конференции, посвященной празднованию 10-летней годовщины воссоединения Крыма с Российской Федерацией, Симферополь, 15 марта 2024 г. – Симферополь: Ариал, 2024. – С. 426–433.

89. Егорова, М. А. Проблема цифровой идентификации личности в Российской Федерации и Европейском Союзе / М. А. Егорова // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2022. – № 1(89). – С. 17–29.

90. Жандров, В. Ю. Решение задач оперативно-розыскной деятельности посредством получения сведений в информационно-телекоммуникационной среде / В. Ю. Жандров // Вестник Московского университета МВД России. – 2024. – № 4. – С. 56–65.

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

92. Зайцев, О. А. Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений / О. А. Зайцев, П. С. Пастухов // Вестник Пермского университета. Юридические науки. – 2022. – № 56. – С. 281–308.

93. Запольский, С. В. Новые актуальные основания модернизации в сфере информационного права / С. В. Запольский, В. Б. Исаков // Правовая информатика. – 2023. – № 1. – С. 4–14.

94. Запорожец, С. А. К вопросу о противодействии киберпреступности в условиях новой геополитической реальности / С. А. Запорожец, Н. А. Крайнова // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2023. – Т. 9(75), № 3. – С. 448–456.

95. Затолокин, А. А. Административно-правовые аспекты государственного регулирования обработки биометрических персональных данных / А. А. Затолокин, В. В. Стрельцов // Общество и право. – 2023. – № 1(83). – С. 79–83.

96. Звягин, И. С. Основы криминалистической биометрической идентификации / И. С. Звягин, А. Ю. Евреинова // Вестник Воронежского института МВД России. – 2025. – № 1. – С. 209–214.

97. Зинин, А. М. Биометрические системы и идентификация человека / А. М. Зинин // Lex Russica (Русский закон). – 2012. – Т. 71, № 5. – С. 1064–1070.

98. Искусственный интеллект в юридической деятельности: учебник для вузов / под ред. С.Е. Чаннова. – Москва: Юрайт, 2025. – 131 с.

99. Исследование системы идентификации и подтверждения легитимности доступа на основе динамических методов биометрической аутентификации / М. М. Путято, А. С. Макарян, Ш. М. Чич, В. К. Маркова // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 3(51). – С. 83–93.

100. Ищенко, Е. П. Криминалистика: учебник / Е. П. Ищенко, А. А. Топорков. – 2-е изд. – Москва: Контракт, Инфра-М, 2006. – 748 с.

101. Казанцева, Н. Г. Цифровизация государственного управления и права человека / Н. Г. Казанцева / Мировые научные дискуссии в эпоху цифровизации: от теории к практике: материалы XVI Международной научно-практической конференции, Рязань, 29 декабря 2023 г. – Рязань: Концепция, 2023. – С. 375–378.

102. Каримов, В. Х. Актуальные вопросы правового регулирования биометрической регистрации в России / В. Х. Каримов, С. В. Яценко // Правда и закон. – 2023. – № 4(26). – С. 26–34.

103. Карпушина, А. В. Вопросы правового регулирования биометрических персональных данных в условиях современной миграционной политики / А. В. Карпушина / Проблемы юриспруденции и педагогики высшей школы в работах молодых ученых: сборник материалов Всероссийской научно-практической конференции, Белгород, 28 ноября 2024 г. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2025. – С. 93–97.

104. Карпушина, А. В. Вопросы правового регулирования при обязательной государственной регистрации биометрических персональных данных / А. В. Карпушина / XIII Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: материалы Международной научно-практической конференции, Калининград, 20 декабря 2024 г. – Калининград: Санкт-Петербургский университет МВД России, Калининградский филиал, 2025. – С. 31–32.

105. Карпушина, А. В. К понятию биометрических персональных данных / А. В. Карпушина // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2023. – № 4. – С. 118–123.

106. Карпушина, А. В. Правовые аспекты использования биометрических персональных данных в борьбе с терроризмом / А. В. Карпушина // Проблемы правоохранительной деятельности. – 2025. – № 3(61). – С. 53–59.

107. Карпушина, А. В. Приоритетные направления правового регулирования биометрических персональных данных / А. В. Карпушина // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2024. – № 4. – С. 100–105.

108. Катмаков, П. С. Биометрия: учебник для вузов / П. С. Катмаков, В. П. Гавриленко, А. В. Бушов; под общ. ред. П.С. Катмакова. – 3-е изд., перераб. и доп. – Москва: Юрайт, 2025. – 186 с.

109. Керимова, С. Н. Понятие и основные черты административного правонарушения как основания административной ответственности / С. Н. Керимова, М. М. Раджабова // Вестник Дагестанского государственного университета. Серия 3: Общественные науки. – 2016. – Т. 31, № 4. – С. 78–84.

110. Кириленко, В. С. Проблемы и перспективы применения днк в системе уголовного правосудия / В. С. Кириленко, Е. А. Хомутова // Вестник Алтайской академии экономики и права. – 2021. – № 11-1. – С. 123–128.

111. Киселев, А. С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности / А. С. Киселев // Вестник Московского государственного областного университета. Серия: Юриспруденция. – 2021. – № 3. – С. 54–64.

112. Кобзарь-Фролова, М. Н. Система органов публичной власти Российской Федерации: понятие, характерные признаки, взаимодействие / М. Н. Кобзарь-Фролова // Сибирское юридическое обозрение. – 2021. – № 2. – С. 192–203.

113. Ковалева, Н. Н. Проблемы обеспечения конфиденциальности персональных данных при использовании систем искусственного интеллекта / Н. Н. Ковалева, Н. А. Жирнова // Журнал российского права. – 2024. – Т. 28, № 7. – С. 109–121.

114. Ковшевацкий, В. И. Проблемы установления отдельных признаков субъективной стороны административного правонарушения / В. И. Ковшевацкий, С. П. Стащенко // Актуальные проблемы административного права и процесса. – 2019. – № 1. – С. 31–35.

115. Кожевников, О. А. К вопросу о понятии и признаках административной ответственности / О. А. Кожевников // Вестник Уральского юридического института МВД России. – 2018. – № 1. – С. 16–18.

116. Койсин, А. А. История становления и развития уголовной (криминалистической) регистрации / А. А. Койсин // Сибирский юридический вестник. – 2018. – № 2(81). – С. 104–115.

117. Комаров, В. В. Исследование технологий распознавания лиц для идентификации участников несанкционированных публичных мероприятий / В. В. Комаров, С. Н. Попова, В. А. Ворожейкин, Д. С. Давидов // Вестник экономической безопасности. – 2022. – № 6. – С. 136–141.

118. Коннова, Л. А. Идентификации личности – история развития и вклад в безопасность жизнедеятельности / Л. А. Коннова, Г. К. Артамонова // Надзорная деятельность и судебная экспертиза в системе безопасности. – 2017. – № 1. – С. 42–49.

119. Кононов, П. И. Проблемы соотношения административной ответственности юридических лиц и их руководителей, иных работников (по материалам арбитражно-судебной практики) / П. И. Кононов // Законодательство Российской Федерации об административных правонарушениях: после реформы, перед реформой: Материалы Международной научно-практической конференции, посвященной памяти Д.Н. Бахраха, Екатеринбург, 17 ноября 2022 года. – Екатеринбург: Уральский государственный юридический университет, 2023. – С. 5-14.

120. Криминалистика: Техника и тактика расследования преступлений / под ред. А.Я. Вышинского. – Москва: Юрид. изд-во, 1938. – 540 с.

121. Кузнецов, П. У. «Цифровая трансформация государственного управления как этап развития информатизации в России» / П. У. Кузнецов // Четвертые Бачиловские чтения: материалы Международной научно-практической конференции / отв. ред. Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. – Москва: Саратов: Амирит, 2022. – 568 с.

122. Кузнецова, С. С. Биометрическая идентификация в Интернете: тенденции правового регулирования в России и за рубежом / С. С. Кузнецова, А. Н. Мочалов, М. С. Саликов // Вестник Томского государственного университета. – 2022. – № 476. – С. 257–267.

123. Кутейников, Д. Л. Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности / Д. Л. Кутейников, О. А. Ижаев, В. А. Лебедев, С. С. Зенин // Lex russica. – 2022. – Т. 75. – № 2. – С. 121–131.

124. Лакин, Г. Ф. Биометрия / Г. Ф. Лакин. – 3-е изд. – Москва: Высшая школа, 1980. – 291 с.

125. Лебеденко, Ю. И. Биометрические системы безопасности / Ю. И. Лебеденко. – Тула: ТулГУ, 2012. – 159 с.

126. Лескина, Э. И. Доктринальные аспекты правовых режимов данных в условиях развития технологий больших данных / Э. И. Лескина // Журнал российского права. – 2024. – Т. 28, № 7. – С. 122–136.

127. Лескина, Э. И. Реформирование правового режима обезличенных данных с целью развития инноваций / Э. И. Лескина / Актуальные проблемы науки и практики: Гатчинские чтения – 2023: сборник научных трудов по материалам X Международной научно-практической конференции, Гатчина, 26 мая 2023 г. – Гатчина: Государственный институт экономики, финансов, права и технологий, 2023. – С. 40–43.

128. Лескина, Э. И. Характеристика отдельных правовых режимов больших данных (Big Data) / Э. И. Лескина // Теоретическая и прикладная юриспруденция. – 2025. – № 1(23). – С. 102–116.

129. Магомедова, Е. А. К вопросу о понятии системы права в отечественной юридической науке / Е. А. Магомедова, М. В. Курзаков, М. А. Зайцева // Тенденции развития науки и образования. – 2024. – № 107-5. – С. 139–141.

130. Мазурин С. Ф. Административное право: учебное пособие / С. Ф. Мазурин, К. Г. Прокофьев. – Санкт-Петербург: Фонд «Университет», 2019. – 312 с.

131. Макарейко, Н. В. Органы внутренних дел как субъект обеспечения национальной безопасности / Н. В. Макарейко // Полиция и общество: проблемы и перспективы взаимодействия. – 2024. – № 6. – С. 86–92.

132. Мальгинов, Е. А. Сбор и обработка биометрических данных топ-менеджеров и предпринимателей: возможно ли защитить корпоративный интерес? / Е. А. Мальгинов // Право и экономика. – 2023. – № 5(423). – С. 11–17.

133. Машковцев, А. А. Электронное наблюдение как современный способ оперативно-розыскного документирования преступлений / А. А. Машковцев, Е. А. Моляров // Вестник Сибирского юридического института МВД России. – 2024. – № 4(57). – С. 91–99.

134. Мигачев, Ю. И. Административное право Российской Федерации: учебник для вузов / Ю. И. Мигачев, Л. Л. Попов, С. В. Тихомиров; под ред. Л.Л. Попова. – 7-е изд., перераб. и доп. – Москва: Юрайт, 2025. – 474 с.

135. Минбалеев, А. В. Понятие и правовая природа цифрового профиля человека / А. В. Минбалеев // Вестник Южно-Уральского государственного университета. Серия: Право. – 2022. – Т. 22, № 1. – С. 110–116.

136. Минбалеев, А. В. Проблемы цифрового права: учебное пособие / А. В. Минбалеев. – Саратов: Амирит, 2022. – 234 с.

137. Минбалеев, А. В. Проблемы и перспективы обеспечения защиты персональных данных граждан в цифровом профиле / А. В. Минбалеев // Вестник УрФО. Безопасность в информационной сфере. – 2021. – № 4(42). – С. 59–63.

138. Минникес, И. А. Правовая защита: понятие и механизм / И. А. Минникес // Известия Иркутской государственной экономической академии. – 2013. – № 6. – С. 15–22.

139. Митянов, З. О. Принудительная и добровольная биометрия: содержание и разграничение в российском праве // Теоретическая и прикладная юриспруденция. – 2024. – № 3 (21). – С. 63–74.

140. Михайлов, М. А. Организационные, правовые и этические аспекты получения, хранения и использования биометрической информации в целях всеобщей регистрации населения / М. А. Михайлов, Т. А. Кокодей // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2022. – Т. 8 (74), № 4. – С. 345–353.

141. Михеева, И. Е. Отдельные правовые аспекты биометрической идентификации в банковской сфере / И. Е. Михеева // Lex Genetica. – 2025. – Т. 4, № 1. – С. 24–38.

142. Могилин, К. А. Интеллектуальные системы видеонаблюдения в комплексах безопасности / К. А. Могилин, В. А. Селищев // Известия Тульского государственного университета. Технические науки. – 2020. – № 3. – С. 89–94.

143. Мочалов, А. Н. Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности / А. Н. Мочалов // Lex russica (Русский закон). – 2021. – Т. 74, № 9. – С. 88–101.

144. Нейросетевая защита персональных биометрических данных: монография / В. И. Волчихин, А. И. Иванов, И. Г. Назаров [и др.]; под ред. Ю.К. Язова. – Москва: Радиотехника, 2012. – 157 с.

145. Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности / Д. Л. Кутейников, О. А. Ижаев, Л. В. Алексеевич, С. С. Зенин // Lex Russica (Русский закон). – 2022. – Т. 75, № 2(183). – С. 121–131.

146. Овчинникова, Е. А. К вопросу об обеспечении безопасности биометрических персональных данных в информационных системах персональных данных / Е. А. Овчинникова, Г. В. Попков // Телекоммуникации. – 2025. – № 1. – С. 36–40.

147. Организационное и правовое обеспечение информационной безопасности: учебник / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов. – 2-е изд., перераб. и доп. – Москва: Юрайт, 2025. – 357 с.

148. Орлова, Е. Р. Отдельные вопросы внедрения цифрового профиля гражданина / Е. Р. Орлова, Э. В. Голоманчук // Труды Института системного анализа Российской академии наук. – 2024. – Т. 74, № 2. – С. 96–105.

149. Осипенко, А. Л. Проблемы доступа правоохранительных органов к скрываемой компьютерной информации при раскрытии преступлений / А. Л. Осипенко, В.Ф. Луговик // Общество и право. – 2021. – № 2(76). – С. 60–68.

150. Остроушко, А. В. Проблемы правового обеспечения процесса внедрения цифрового профиля гражданина / А. В. Остроушко // Юридические исследования. – 2022. – № 5. – С. 34–47.

151. Панфилова, О. А. Биометрические методы и системы идентификации личности при обеспечении информационной безопасности в уголовно-исполнительной системе: учебное пособие / О. А. Панфилова, Д. Ю. Крюкова. – Вологда: Вологодский институт права и экономики Федеральной службы исполнения наказаний, 2022. – 58 с.

152. Петрова, Д. А. Обработка биометрических персональных данных в свете изменения законодательства / Д. А. Петрова, В. А. Папкова // Правовая политика и правовая жизнь. – 2024. – № 3. – С. 329–336.

153. Пилия, Д. Э. Основные подходы к определению понятия «публичная власть» в публично-правовых (государственно-правовых) науках / Д. Э. Пилия // Lex Russica (Русский закон). – 2023. – Т. 76, № 5(198). – С. 9–23.

154. Пинчук, П. В. Дактилоскопия: исторические аспекты и роль в решении идентификационных задач на современном этапе ее развития / П. В. Пинчук // Проблемы экспертизы в медицине. – 2001. – Т. 1, № 2. – С. 46–49.

155. Платонова, Н. И. Современные правовые подходы к пониманию биометрических данных / Н. И. Платонова // Информационное право. – 2018. – № 1. – С. 22–26.

156. Платонова, Н. И. Биометрические персональные данные: возможности и проблемы / Н. И. Платонова, А. Ю. Соловьева-Опошнянская // Юрист. – 2019. – № 6. – С. 63–67.

157. Позднякова, Е. В. Субъекты управления в сфере обеспечения безопасности государства и защиты жизненных ценностей граждан / Е. В. Позднякова // Научный вестник Омской академии МВД России. – 2024. – Т. 30, № 3(94). – С. 247–251.

158. Полимеразная цепная реакция в микробиологии / Д. П. Гладин, А. М. Королук, И.В. Дробот [и др.] // Российские биомедицинские исследования. – 2021. – Т. 6, № 3. – С. 36–46.

159. Получение визуальной информации с использованием современных технических средств в целях выявления, пресечения и раскрытия преступлений / А. Ю. Молянов, В. Г. Любан, К. А. Сермягин, С. М. Филиппов. – Москва: Московский университет МВД России имени В.Я. Кикотя, 2019. – 88 с.

160. Полуянова, Е. В. Нормативное регулирование использования биометрических персональных данных в Российской Федерации / Е. В. Полуянова, С. Д. Ковалев // Вестник Томского института повышения квалификации работников ФСИН России. – 2020. – № 3(5). – С. 45–51.

161. Полуянова, Е. В. Отдельные вопросы функционирования и правового регулирования Единой биометрической системы Российской Федерации / Е. В. Полуянова // Аграрное и земельное право. – 2025. – № 3. – С. 105–108.

162. Полякова, Т. А. Актуальные проблемы систематизации законодательства России под влиянием цифровых технологий в период цифровой трансформации / Т. А. Полякова, Н. А. Троян // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2023. – № 2(102). – С. 25–33.

163. Полякова, Т. А. Особенности взаимодействия и правового обеспечения информационной безопасности в единой биометрической системе в Российской Федерации / Т. А. Полякова, И. С. Бойченко // Правовая политика и правовая жизнь. – 2023. – № 3. – С. 26–34.

164. Попов, О. В. Особенности правового регулирования использования биометрических персональных данных в системе государственного управления на современном этапе цифровой трансформации общества / О. В. Попов, А. Н. Прокопенко // Административное право и процесс. – 2023. – № 2. – С. 22–24.

165. Попова, Т. В. Федеральная база данных геномной информации в системе обеспечения баланса частных и публичных интересов в уголовном судопроизводстве / Т. В. Попова, А. Б. Сергеев // Юридическая наука и правоохранительная практика. – 2017. – № 1(39). – С. 132–139.

166. Постников, Н. А. Биометрия сквозь века: от первых отпечатков к современным методам идентификации / Н. А. Постников // Поволжский вестник науки. – 2025. – № 1(35). – С. 31–41.

167. Правовая защита информации: учебное пособие / А. И. Антипов, Д. Е. Дробов, Н. М. Крамаренко [и др.]. – Санкт-Петербург: СПбУ МВД России, 2024. – 544 с.

168. Правовое обеспечение безопасного использования генетической и геномной информации: учебник для вузов / под ред. Л.Н. Берг, А.В. Лисаченко. – Москва: Юрайт, 2025. – 123 с.

169. Правовое обеспечение суверенитета и кодификация информационного законодательства / Ю. М. Батулин, Т. А. Полякова, А. В. Минбалеев [и др.]. – Москва: Институт государства и права РАН, 2024. – 228 с.

170. Правоохранительные органы: учебник для среднего профессионального образования / под общ. ред. М.П. Полякова. – 3-е изд., перераб. и доп. – Москва: Юрайт, 2025. – 329 с.

171. Правоохранительные органы России: учебник / Б. Я. Гаврилов, Е. А. Бархатова, А. Ю. Винокуров [и др.]. – 7-е изд., пер. и доп. – Москва: Юрайт, 2023. – 344 с.

172. Применение метода коротких tandemных повторов для аутентификации клеточных линий / М. Д. Хорольский, И. С. Семенова, Е. В. Мельникова, Ю. В. Олефир // Биопрепараты. Профилактика, диагностика, лечение. – 2019. – Т. 19, № 4. – С. 251–260.

173. Проектирование модели цифровой обработки биометрических характеристик человека / А. М. Трошков, М. А. Трошков, Д. В. Шлаев [и др.] // Вестник АПК Ставрополя. – 2017. – № 1(25). – С. 57–62.

174. Прокопенко, А. Н. Борьба с утечками персональных данных – поможет ли ужесточение ответственности? / А. Н. Прокопенко // Вестник Казанского юридического института МВД России. – 2024. – Т. 15, № 2(56). – С. 48–56.

175. Протасевич, А. А. О возможностях криминалистической габитоскопии при реализации мер противодействия современной киберпреступности / А. А. Протасевич, Е. И. Фойгель // Всероссийский криминологический журнал. – 2020. – Т. 14, № 3. – С. 471–480.

176. Протасов, П. А. Биометрия в банковской системе РФ / П. А. Протасов // Вестник Томского государственного университета. Экономика. – 2020. – № 49. – С. 141–148.

177. Равоян, Р. А. Правовое регулирование защиты персональных и биометрических данных в условиях цифровизации / Р. А. Равоян // Юридическая наука. – 2023. – № 5. – С. 83–86.

178. Рассолов, И. М. Защита генетических данных при генетическом тестировании и генотерапевтическом лечении: информационно-правовые аспекты / И. М. Рассолов, С. Г. Чубукова // Актуальные проблемы российского права. – 2020. – Т. 15, № 5(114). – С. 65–72.

179. Романько, Н. А. О судебно-экспертной идентификации личности по признакам внешности и особенностям строения тела / Н. А. Романько, А. М. Зинин, Ш. Н. Хазиев // Судебная медицина. – 2017. – Т. 3, № 1. – С. 21–25.

180. Россинский, Б. В. Административное право и административная ответственность: курс лекций / Б. В. Россинский. – 2-е изд., перераб. – Москва: Норма: ИНФРА-М, 2025. – 352 с.

181. Россинский, Б. В. Административное право: учебник / Б. В. Россинский, Ю. Н. Стариков, – 6-е изд., пересмотр. – Москва: Норма: ИНФРА-М, 2020. – 640 с.

182. Россинский, Б. В. Формирование публичной власти как реализация системного принципа ингрессии / Б. В. Россинский // Административное право и процесс. – 2022. – № 7. – С. 4–8.

183. Саликов, М. С. Государственное регулирование Интернета и права человека: монография / М. С. Саликов, С. Э. Несмеянова, Н. Е. Колобаева, С. С. Кузнецова, А. Н. Мочалов. – Екатеринбург: УМЦ УПИ, 2022. – 220 с.

184. Саркисян, Г. Г. Использование информационно-коммуникационных технологий в оперативно-аналитической деятельности органов внутренних дел Российской Федерации / Г. Г. Саркисян // Труды Академии управления МВД России. – 2024. – № 4(72). – С. 172–181.

185. Сборник циркуляров Министерства внутренних дел по вопросам воинской и военно-конской повинности. 1874–1906. – 3-е изд., доп. и испр. – Санкт-Петербург: Упр. по делам о воинской повинности М-ва внутренних дел, 1906. – 747 с.

186. Свидетельство о государственной регистрации программы для ЭВМ № 2025661428 Российская Федерация. Биометрическая аутентификация по клавиатурному почерку: заявл. 17.04.2025 : опубл. 06.05.2025 / В. А. Валиуллин.

187. Свиридова Е.А. Защита персональных данных в условиях цифровой трансформации общественных отношений // Проблемы экономики и юридической практики. – 2022. – Т. 18. – № 6. – С. 53–58.

188. Семенов, Ю. Н. Функциональные и технические требования к платформе мультимодальных биометрических решений (регистрация, хранение, идентификация/верификация, обработка и аналитика) / Ю. Н. Семенов, В. И. Кабаров, А. Р. М. Кассу / Альманах научных работ молодых ученых Университета ИТМО: XLVII научная и учебно-методическая конференция, Санкт-Петербург, 31 января – 3 февраля 2018 г. В 2-х т. – Санкт-Петербург: Национальный исследовательский университет ИТМО, 2018. Т. 2. – С. 188–191.

189. Семенчук, В. В. Судебный контроль за оперативно-розыскной деятельностью – альтернатива прокурорскому надзору / В. В. Семенчук // Вестник Нижегородского университета имени Н.И. Лобачевского. – 2020. – № 4. – С. 130–141.

190. Серго, С. В. К вопросу о реорганизации баз данных дактилоскопических учетов / С. В. Серго, Ж. Ю. Снежкова // Юрист-Правоведъ. – 2022. – № 1(100). – С. 123–127.

191. Сердюк, А. С. Обеспечение безопасности на объектах спортивной инфраструктуры / А. С. Сердюк, Е. М. Абросимова / Современные материалы, техника и технология: сборник научных статей 7-й международной научно-практической конференции, Курск, 29–30 декабря 2017 года / отв. ред. А.А. Горохов. – Курск: Университетская книга, 2017. – С. 345–348.

192. Сизимова, О. Б. Правовое регулирование использования технологий искусственного интеллекта в банковской деятельности / О. Б. Сизимова // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2024. – № 9(121). – С. 132–140.

193. Сморчкова, Л. Н. Цифровое правительство как перспектива государственного управления в России: информационно-правовые аспекты / Л. Н. Сморчкова // Правовая информатика. – 2022. – № 2. – С. 25–33.

194. Создание Концепции национальной системы биометрической идентификации личности / С. В. Баженов, В. Е. Дивольд, А. А. Морозов [и др.] // Труды Академии управления МВД России. – 2020. – № 2(54). – С. 41–53.

195. Соколова, О. А. Дактилоскопия и дактилоскопическая экспертиза: учебник для вузов / О. А. Соколова, В. В. Пономарев; под общ. ред. О.А. Соколовой. – Москва: Юрайт, 2025. – 266 с.

196. Старанцова, Е. В. Современные методы биометрической идентификации / Е. В. Старанцова // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9, № 1(39). – С. 44–48.

197. Старостин, С. А. О подмене понятий в государственном управлении / С. А. Старостин // Вестник Томского государственного университета. Право. – 2019. – № 32. – С. 76–96.

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

199. Сулавко, А. Е. Высоконадежная двухфакторная биометрическая аутентификация по рукописным и голосовым паролям на основе гибких нейронных сетей / А. Е. Сулавко // Компьютерная оптика. – 2020. – Т. 44, № 1. – С. 82–91.

200. Сухостат, В. В. Основы информационной безопасности / В. В. Сухостат, И. Н. Васильева. – Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2019. – 103 с.
201. Талапина, Э. В. Защита персональных данных в цифровую эпоху: российское право в Европейском контексте / Э. В. Талапина // Труды Института государства и права Российской академии наук. – 2018. – Т. 13, № 5. – С. 117–150.
202. Тархов, С. В. Цифровые двойники человека и личности в организационных системах / С. В. Тархов, Л. М. Тархова, Ю. Р. Назарова // Современные наукоемкие технологии. – 2025. – № 3. – С. 47–52.
203. Тебекин, А. В. Влияние технологических укладов на развитие криминалистики в XVIII-XX веках / А. В. Тебекин, И. В. Глазунова // Вестник Российской таможенной академии. – 2016. – № 2. – С. 79–83.
204. Терещенко, И. А. Биометрические персональные данные: проблемы и перспективы определения понятия / И. А. Терещенко // Закон и право. – 2024. – № 2. – С. 186–192.
205. Терещенко, Л. К. Фейки и треш-стримы как угроза информационной безопасности / Л. К. Терещенко // Журнал российского права. – 2023. – Т. 27, № 11. – С. 103–114.
206. Технические средства визуального контроля, используемые в органах внутренних дел / А. А. Черных, Ф. В. Безгачев, Е. А. Лаппо, А. Лхамсурэн. – Красноярск: Сибирский юридический институт МВД России, 2022. – 124 с.
207. Тимошенко, И. В. Понятие административной ответственности / И. В. Тимошенко // Северо-Кавказский юридический вестник. – 2009. – № 2. – С. 74–79.
208. Тимченков, В. А. Исторический опыт и вектор развития дактилоскопической экспертизы в РФ / В. А. Тимченков, О. В. Нестерова // Наукосфера. – 2021. – № 5-2. – С. 246–249.
209. Тихомиров, Ю. А. Систематика в праве в условиях глобальной нестабильности / Ю. А. Тихомиров // Журнал российского права. – 2022. – Т. 26, № 5. – С. 5–18.

210. Трофимов, А. А. Биометрическая идентификация субъектов частного права: понятие, признаки, способы / А. А. Трофимов // Правовая информатика. – 2024. – № 4. – С. 81–88.

211. Упоров И. В. Категория «публичная власть» в толковании ученых-правоведов / И. В. Упоров // Форум. – 2024. – № 2(32). – С. 299–304.

212. Фатхи, В. И. К вопросу о правовом регулировании порядка использования биометрических персональных данных: международный опыт / В. И. Фатхи // Философия права. – 2023. – № 4 (107). – С. 93–98.

213. Федосеева, А. П. Цифровая гигиена как средство защиты от цифровых угроз в информационном пространстве / А. П. Федосеева / XII Сильвестровские педагогические чтения. Духовность и нравственность в образовательном пространстве: глобальные вызовы современности и духовный выбор человека: материалы всероссийской научной конференции, Тара, 30 марта 2023 г. – Омск: Амфора, 2023. – С. 159–162.

214. Фиалковская, И. Д. Состав административного правонарушения: первичные и вторичные признаки / И. Д. Фиалковская // Законность и правопорядок. – 2018. – № 3(19). – С. 29–33.

215. Физиология человека и животных: учебник / Д. Л. Теплый, Ю. В. Нестеров, Е. В. Курьянова [и др.]; под общ. ред. проф. Д.Л. Теплого. – Астрахань: Астраханский государственный университет, 2017. – 336 с.

216. Фролова, Е. Ю. Идентификация человека по биометрическим данным: обзор современных технологий / Е. Ю. Фролова, Ю. А. Кошлыкова // Северо-Кавказский юридический вестник. – 2022. – № 3. – С. 167–174.

217. Хазиев, Ш. Н. Криминалистические и судебно-экспертные основы современных биометрических технологий / Ш. Н. Хазиев // Теория и практика судебной экспертизы. – 2023. – Т. 18, № 1. – С. 16–21.

218. Хачумов, М. В. Распознавание лиц по фотографиям на основе инвариантных моментов / М. В. Хачумов, Т. З. Нгуен // Современные проблемы науки и образования. – 2015. – № 2-2. – С. 187–193.

219. Химченко, А. И. Формирование цифровой среды доверия: динамика развития инфраструктуры идентификации при реализации цифровых услуг / А. И. Химченко // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2023. – № 2(102). – С. 101–109.

220. Ховавко, С. М. Теоретико-правовые и организационные основы технического отождествления личности на основе биометрической идентификации в оперативно-розыскной деятельности / С. М. Ховавко // Вестник Уральского юридического института МВД России. – 2022. – № 2. – С. 151–155.

221. Храмов, Е. Н. Биометрические технологии как фактор повышения безопасности и конкурентоспособности в финансовой инфраструктуре России / Е. Н. Храмов, О. В. Вершинина // Фундаментальные исследования. – 2025. – № 4. – С. 69–79.

222. Частикова, В. А. Аналитический обзор методов идентификации личности на основе биометрических характеристик / В. А. Частикова, А. А. Титова, Д. О. Войлова // Вестник Адыгейского государственного университета. Серия: Естественно-математические и технические науки. – 2022. – № 1(296). – С. 92–112.

223. Челышев, А. И. История становления отечественной криминалистики / А. И. Челышев // Вестник Владимирского юридического института. – 2006. – № 1(1). – С. 152–155.

224. Челышева, Н. Ю. Правовое регулирование использования биометрических технологий органами государственной власти / Н. Ю. Челышева // Администратор суда. – 2024. – № 4. – С. 25–28.

225. Шатов, Д. В. Лицевая биометрия и нейронные сети в криминалистике: современные возможности и проблемы применения / Д. В. Шатов, С. С. Барсуков, И. Н. Шипанов // Юрист-Правоведъ. – 2023. – № 1(104). – С. 155–163.

226. Шейдаева, С. Г. Ивашка из XVII века: отражение внешности человека в русской деловой письменности и в системе антропонимов / С. Г. Шейдаева // Вестник Удмуртского университета. Серия История и филология. – 2022. – Т. 32, № 4. – С. 697–715.

227. Шипулин, А. В. Проблемы нормативного сопровождения цифровой трансформации распознавания и применения биометрических признаков при обеспечении безопасности объектов / А. В. Шипулин, А. В. Пархаев // Информатизация и техническое обеспечение уголовно-исполнительной системы Российской Федерации: проблемы, решения и перспективы развития: сборник материалов III всероссийской научно-практической конференции, Тверь, 3–4 октября 2024 года. – Тверь: Научно-исследовательский институт информационных технологий Федеральной службы исполнения наказаний, 2024. – С. 422–429.

228. Шумилин, В. П. Биометрический метод распознавания лица в правоохранительных органах / В. П. Шумилин / Современное состояние и перспективы обеспечения безопасности дорожного движения: теория и практика: сборник материалов Всероссийской научно-практической конференции, Орел, 21 ноября 2019 г. – Орел: Орловский юридический институт МВД России имени В.В. Лукьянова, 2020. – С. 166–171.

229. Эволюция подходов к ДНК-идентификации личности / Д. А. Чемерис, А. М. Сагитов, Ф. Г. Аминев [и др.] // Биомика. – 2018. – Т. 10, № 1. – С. 85–140.

230. Эйхвальд, Н. Л. Использование дактилоскопических карт, полученных посредством комплекса «Живой сканер» и АДИС «Папилон», при производстве дактилоскопической экспертизы / Н. Л. Эйхвальд // Юридическая наука и правоохранительная практика. – 2020. – № 4(54). – С. 98–104.

231. Экономические и социальные права человека и гражданина: современные проблемы теории и практики: монография / Ф. М. Рудинский, Ю. В. Гаврилова, А. А. Крикунова, Т. А. Сошникова. – Москва: Права человека, 2009. – 495 с.

232. Эффективность государственных управленческих решений в условиях цифровизации: монография / С. М. Зубарев, А. В. Иванов, С. Г. Кирдина-Чэндлер [и др.]. – Москва: Проспект, 2023. – 184 с.

233. Bertalanffy L. von (1968). General System Theory: Foundations, Development, Applications. New York: George Braziller. P. 55.

234. Monroy v. Shutterfly, Inc. no. 1:2016cv10984 – Document 39 (N.D. Ill. 2017).

### **Диссертации, авторефераты диссертаций**

235. Бундин, М. В. Персональные данные в системе информации ограниченного доступа: дис. ... канд. юрид. наук: 12.00.13 / Бундин Михаил Вячеславович. – Москва, 2017. – 218 с.

236. Быстрыкова, С. А. Правовое регулирование цифрового оборота персональных данных в системе обеспечения транспортной безопасности: дис. ... канд. юрид. наук: 5.1.2 / Быстрыкова Светлана Анатольевна. – Москва, 2024. – 221 с.

237. Волкова, С. С. Методы повышения эффективности систем биометрической аутентификации пользователей информационных систем по изображению лица: дис. ... канд. техн. наук: 05.13.19 / Волкова Светлана Сергеевна. – Санкт-Петербург, 2017. – 129 с.

238. Гутник, С. И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных: дис. ... канд. юрид. наук: 12.00.08 / Гутник Сергей Иосифович. – Владивосток, 2017. – 241 с.

239. Дизер, О. А. Административно-правовая защита общественной нравственности: дис. ... д-ра юрид. наук: 12.00.14 / Дизер Олег Александрович. – Омск, 2019. – 408 с.

240. Дизер, О. А. Административно-правовая защита общественной нравственности: автореф. ... д-ра юрид. наук: 12.00.14 / Дизер Олег Александрович. – Омск, 2019. – 59 с.

241. Игуминов, В. В. Публично-правовое регулирование цифрового профилирования в Российской Федерации: автореф. дис. ... канд. юрид. наук: 5.1.2. / Игуминов Вячеслав Валерьевич. – Москва, 2024. – 263 с.

242. Кучеренко, А. В. Правовое регулирование персональных данных в Российской Федерации: дис. ... канд. юрид. наук: 12.00.14 / Кучеренко Анна Вячеславовна. – Челябинск, 2010. – 212 с.

243. Кушхова, Б. З. Юридическая ответственность публичной власти в современной России: общетеоретический аспект: дис. ... канд. юрид. наук: 12.00.01 / Кушхова Бэла Залимовна. – Краснодар, 2009. – 199 с.

244. Наумов, В. Б. Институт идентификации в информационном праве: дис. ... д-ра юрид. наук: 12.00.13 / Наумов Виктор Борисович. – Москва, 2020. – 455 с.

245. Проскурякова, М. И. Защита персональных данных в праве России и Германии: конституционно-правовой аспект: дис. ... канд. юрид. наук: 12.00.02 / Проскурякова Мария Ивановна. – Санкт-Петербург, 2017. – 193 с.

246. Рачинский, В. В. Публичная власть как общеправовая категория (Теоретико-прикладной аспект): дис. ... канд. юрид. наук: 12.00.01 / Рачинский Вячеслав Владимирович. – Уфа, 2003. – 195 с.

247. Соловкин, С. В. Публично-правовое регулирование процессов автоматизированного сбора данных о человеке в условиях цифровой трансформации: дис. ... канд. юрид. наук: 5.1.2 / Соловкин Сергей Васильевич. – Москва, 2024. – 278 с.

248. Сорокин Ю.Ю. Публичная власть и интересы общества: проблемы взаимодействия: дис. ... канд. юрид. наук: 12.00.01: Сорокин Юрий Юрьевич. – Москва, 2011. – 213 с.

### **Интернет-ресурсы**

249. Административные правонарушения в области связи и информации / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://stat.api-пресс.рф/stats/adm/t/31/s/73> (дата обращения: 13.04.2025).

250. АДИС (AFIS) Папилон – система мультибиометрической идентификации / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://www.papillon.ru/products/programs/adis/> (дата обращения: 12.05.2025).

251. Аккредитация в сфере аутентификации на основе биометрических персональных данных / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://digital.gov.ru/activity/gos-uslugi/akkreditacziya-v-sfere-autentifikaczii-na-osnove-biometricheskih-personalnyh-dannyh> (дата обращения: 04.12.2024).

252. Биометрия на марше: лицом к лицу с будущим Официальный интернет-сайт [Электронный ресурс]. – URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/biometrija-na-marshe-licom-k-licu-s-budushchim> (дата обращения: 12.05.2025).

253. Биоэквайринг – оплачивайте покупки по-новому / Официальный интернет-сайт [Электронный ресурс]. – URL: [https://ebs.ru/bio\\_pay/](https://ebs.ru/bio_pay/) (дата обращения: 10.06.2025).

254. В 2023 году в сеть утекло более 300 млн записей о россиянах // Официальный интернет-сайт [Электронный ресурс]. – URL: <https://tass.ru/obschestvo/19693845> (дата обращения: 21.03.2024).

255. В России образован координационный совет по развитию биометрических технологий / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://digital.gov.ru/news-media/v-rossii-obrazovan-koordinaczionnyj-sovet-po-razvitiyu-biometricheskih-tehnologij> (дата обращения: 25.03.2025).

256. ВС РФ: взятие буккального эпителия для генетических исследований уже само по себе требует наличия медлицензии по генетике / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://www.garant.ru/news/1313455/> (дата обращения: 22.05.2024).

257. Госдума предложила проверить социальную сеть MyHeritage / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://iz.ru/980229/2020-02-26/gosduma-predlozhila-proverit-sotcialnuiu-set-myheritage> (дата обращения: 08.04.2025).

258. ГОСТ Р 58624.3-2019 Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний [Электронный ресурс]. – URL: <https://base.garant.ru/402129295/> (дата обращения: 21.03.2025).

259. Депутаты приняли еще три законопроекта, направленных на совершенствование миграционной политики / Официальный интернет-сайт [Электронный ресурс]. – URL: <http://duma.gov.ru/news/60215/> (дата обращения: 10.12.2024).

260. Дипфейк шагает по планете. С чем связан рост числа сообщений, сгенерированных ИИ / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://rg.ru/2025/04/08/dipfejk-shagaet-po-planete.html> (дата обращения: 03.05.2025).

261. Единая биометрическая система – один из ключевых проектов цифровой инфраструктуры страны / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://ebs.ru/company/> (дата обращения: 26.12.2023).

262. Единая биометрическая система / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://digital.gov.ru/activity/czifrovaya-identifikacziya/edinaya-biometricheskaya-systema> (дата обращения: 21.03.2025).

263. Законопроект о единой системе биометрических данных россиян принят во втором чтении / Официальный интернет-сайт [Электронный ресурс]. – URL: <http://duma.gov.ru/news/56071/> (дата обращения: 02.02.2023).

264. Заселение в гостиницу / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://ebs.ru/services/> (дата обращения: 06.05.2025).

265. Информация по делу № 02а-0577/2019 / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://mos-gorsud.ru/rs/savyolovskij/services/cases/kas/details/988f386e-be51-47b0-b48f-e871043ef1fc> (дата обращения: 13.04.2025).

266. Информация по делу № 02а-0975/2024 // Официальный интернет-сайт [Электронный ресурс]. – URL: <https://mos-gorsud.ru/rs/savyolovskij/services/cases/kas/details/ad530ee1-f10b-11ee-b51f-5fe397bc9869> (дата обращения: 05.03.2025).

267. Ирина Яровая: Государственная Дума качественно и системно отработала вопросы противодействия нелегальной миграции / Официальный интернет-сайт [Электронный ресурс]. – URL: <http://duma.gov.ru/news/60401/> (дата обращения: 30.11.2024).

268. Исторические этапы образования / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://мвд.рф/mvd/structure1/Centri/> (дата обращения: 30.03.2023).

269. Итоги работы с обращениями граждан в Роскомнадзоре в 2024 году / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://rkn.gov.ru/treatments/p436/> (дата обращения: 25.05.2025).

270. Как государство защитит биометрические данные россиян / Официальный интернет-сайт [Электронный ресурс]. – URL: <http://duma.gov.ru/news/56087/> (дата обращения: 09.01.2024).

271. Какие типы биометрии выбраны для проекта и почему? / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://ebs.ru/faq/project/> (дата обращения: 21.03.2025).

272. Карцан И.Н. (2023). Биометрические данные: новые возможности и риски. Современные инновации, системы и технологии – Modern Innovations, Systems and Technologies, 3(3), 0201-0211 [Электронный ресурс]. – URL: <https://doi.org/10.47813/2782-2818-2023-3-3-0201> (дата обращения: 02.02.2025).

273. Ключевые компании / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://www.papillon.ru/about/company/kljuchevye-kompanii/> (дата обращения: 07.03.2025).

274. Количество пользователей сервисом биометрической идентификации / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://www.fedstat.ru/indicator/62445> (дата обращения: 11.10.2024).

275. Методические рекомендации Банка России от 9 октября 2024 г. № 19-МР по нейтрализации организациями финансового рынка угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением

единой биометрической системы, а также актуальных при взаимодействии информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей с указанными информационными системами [Электронный ресурс]. – URL: <https://cbr.ru/crosscut/lawacts/file/9881> (дата обращения: 11.02.2025).

276. Мониторинг развития информационного общества в Российской Федерации / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://www.rosstat.gov.ru/statistics/infocommunity> (дата обращения: 12.02.2025).

277. Мошенники стали в семь раз чаще использовать дипфейки в секторе финансовых технологий / Официальный интернет-портал [Электронный ресурс]. – URL: <https://ai.gov.ru/mediacenter/moshenniki-stali-v-sem-raz-chashche-ispolzovat-dipfeyki-v-sektore-finansovykh-tekhnologiy/> (дата обращения: 23.05.2025).

278. На портале «Госуслуги» зарегистрировались более 112 млн человек / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://объясняем.рф/articles/news/na-portale-gosuslugi-zaregistrovalis-bolee-112-mln-chelovek> / (дата обращения: 20.05.2025).

279. На Урале начался суд над убийцей, который 32 года назад забил молотком 7 человек / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://www.papillon.ru/about/blog/na-urale-nachalsja-sud-nad-ubijcej-kotoryj-32-goda-nazad-zabil-molotkom-7-chelovek/> (дата обращения: 23.05.2025).

280. Национальная программа «Цифровая экономика Российской Федерации» / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://digital.gov.ru/target/naczionalnaya-programma-czifrovaya-ekonomika-rossijskoj-federaczii> (дата обращения: 15.03.2025).

281. О биометрии и Единой биометрической системе / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://ebs.ru/documents/> (дата обращения: 24.11.2024).

282. Обзор Международного рынка биометрических технологий и их применение в финансовом секторе / Официальный интернет-сайт [Электронный ресурс]. – URL: [https://cbr.ru/content/document/file/36012/rev\\_bio.pdf](https://cbr.ru/content/document/file/36012/rev_bio.pdf) (дата обращения: 26.06.2023).

283. Обслуживание без паспорта/ Официальный интернет-сайт [Электронный ресурс]. – URL: [https://ebs.ru/services/?ELEMENT\\_ID=4189741](https://ebs.ru/services/?ELEMENT_ID=4189741) (дата обращения: 24.05.2025).

284. Одинаковы с лица: в России выросло число атак с применением дипфейков / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://iz.ru/1773345/oksana-belkina/odinakovy-s-lica-v-rossii-vyroslo-cislo-atak-s-primeneniem-dipfeikov> (дата обращения: 22.10.2024).

285. Определен перечень госуслуг, которые можно получить по биометрии в трех пилотных регионах / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://объясняем.пф/articles/news/opredelen-perechen-gosuslug-kotorye-mozhno-poluchit-po-biometrii-v-trekh-pilotnykh-regionakh/> (дата обращения: 12.06.2025).

286. Отчет о выполнении Плана и показателей деятельности Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций за 2023 год / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://digital.gov.ru/documents/reglament-informacionnogo-vzaimodejstviya-esia> (дата обращения: 13.04.2025).

287. Официальное сообщение Роскомнадзора (О функционировании системы «Антифрод») / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://cmu.gov.ru/ru/news/2023/11/27/o-funkcionirovanii-sistemy-antifrod/> (дата обращения: 13.12.2023).

288. Пароль не нужен: что нужно знать о биометрии / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://объясняем.пф/articles/useful/biometricheskie-dannye-chto-nuzhno-znat/> (дата обращения: 03.09.2024).

289. Министерства цифрового развития, связи и массовых коммуникаций РФ от 28.08.2020 № ЛБ-С-074-24059 «О методических рекомендациях» (вместе с Методическими рекомендациями для общеобразовательных организаций по вопросам обработки персональных данных) [Электронный ресурс]. – URL: <https://www.garant.ru/> (дата обращения: 03.11.2023).

290. Письмо Роскомнадзора от 31.01.2023 № 09-6488 «Об особенностях возбуждения Роскомнадзором дел об административных правонарушениях без проведения КНМ во взаимодействии с контролируемым лицом» [Электронный ресурс]. – URL: <https://legalacts.ru/doc/> (дата обращения: 16.04.2025).

291. Принят законопроект об ответственности за нарушения при использовании биометрических данных / Официальный интернет-сайт [Электронный ресурс]. – URL: <http://duma.gov.ru/news/57227/> (дата обращения: 29.02.2024).

292. Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки: Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30 августа 2013 г. / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://www.pd.rkn.gov.ru/press-service/subject1/news2729/> (дата обращения: 20.01.2023).

293. Расширенное заседание коллегии МВД / Официальный интернет-сайт [Электронный ресурс]. – URL: <http://www.kremlin.ru/events/president/transcripts/> (дата обращения: 11.04.2023).

294. Расширенное заседание коллегии МВД / Официальный интернет-сайт [Электронный ресурс]. – URL: <http://www.kremlin.ru/events/president/news/73770> (дата обращения: 07.04.2024).

295. Регламент информационного взаимодействия ЕСИА / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://digital.gov.ru/documents/reglament-informaczionnogo-vzaimodejstviya-esia> (дата обращения: 09.04.2025).

296. Результаты деятельности за период с 01.01.2023 по 29.12.2023 / Официальный интернет-сайт [Электронный ресурс]. – URL: [https://31.rkn.gov.ru/docs/31/Otchjot\\_zh\\_12\\_mes\\_2023\\_god.pdf](https://31.rkn.gov.ru/docs/31/Otchjot_zh_12_mes_2023_god.pdf) (дата обращения: 17.04.2024).

297. Решение № 2-5054/2020 2-5054/2020~М-4511/2020 М-4511/2020 от 24 ноября 2020 г. по делу № 2-5054/2020 / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://sudact.ru/regular/doc/Da9dDaSKUTom/> (дата обращения: 23.05.2023).

298. Роскомнадзор запустил платформу для борьбы с телефонным мошенничеством / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://digital.gov.ru/ru/events/42390/> (дата обращения: 13.02.2024).

299. Семь этических принципов Института биометрии / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://tcn.by/statii/sem-eticheskikh-printsipov-instituta-biometrii> (дата обращения: 16.03.2025).

300. Совещание с членами Правительства / Официальный интернет-сайт [Электронный ресурс]. – URL: <http://www.kremlin.ru/events/president/news/76409> (дата обращения: 27.03.2025).

301. Состояние преступности в Российской Федерации за январь - декабрь 2024 года / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://мвд.рф/reports/item/60248328/> (дата обращения: 09.04.2025).

302. Суд посчитал, что технологии распознавания лиц не нарушают законодательство о персональных данных / Официальный интернет-сайт [Электронный ресурс]. – URL: <https://www.advgazeta.ru/novosti/sud-poschital-cto-tehnologii-raspoznavaniya-lits-ne-narushayut-zakonodatelstvo-o-personalnykh-dannikh/> (дата обращения: 13.04.2025).

303. Судебная статистика РФ [Электронный ресурс]. – URL: <https://stat.апи-пресс.рф/stats/adm/t/31/s/1> (дата обращения: 16.04.2025).

304. Усиливается защита персональных биометрических данных граждан [Электронный ресурс]. – URL: <http://duma.gov.ru/news/58432/> (дата обращения: 27.12.2023).

305. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций разъясняет вопросы отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к

биометрическим персональным данным и особенности их обработки [Электронный ресурс]. – URL: <https://25.rkn.gov.ru/news/news54167.htm> (дата обращения: 13.05.2025).

306. ЦБ впервые раскрыл объем платежей россиян по лицу и QR-кодам [Электронный ресурс]. – URL: <https://www.rbc.ru/finances/24/12/2024/> (дата обращения: 11.05.2025).

307. Четверть века применения видео-конференц-связи в Верховном Суде Российской Федерации / Официальный интернет-сайт [Электронный ресурс]. – URL: [https://www.vsrf.ru/press\\_center/news/34349/](https://www.vsrf.ru/press_center/news/34349/) (дата обращения: 20.05.2025).

308. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Электронный ресурс]. – URL: <https://ogdpr.eu/en/gdpr-2016>.

### Вопросы и результаты анкетирования

Результаты анонимного анкетирования 375 граждан Российской Федерации, проведенного в рамках научного исследования по теме «Административно-правовая защита биометрических персональных данных».

| № вопроса | Вопросы                                                                                                                                                                                                                                         | Ответы респондентов                               |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| 1.        | <b>Как Вы относитесь к идентификации личности с помощью биометрических персональных данных? Выберите один вариант ответа.</b><br>а) положительно;<br>б) отрицательно;<br>в) нейтрально.                                                         | 161 чел. (43%)<br>90 чел. (24%)<br>124 чел. (33%) |
| 2.        | <b>Проходили ли Вы ранее процедуру регистрации биометрических персональных данных? Выберите один вариант ответа.</b><br>а) да, проходил(а);<br>б) нет, не проходил(а).                                                                          | 199 чел. (53%)<br>176 чел. (47%)                  |
| 3.        | <b>Данная регистрация проводилась добровольно или Вы подлежали обязательной государственной регистрации? Выберите один вариант ответа.</b><br>а) добровольно;<br>б) обязательная государственная регистрация;<br>в) регистрация не проводилась. | 184 (49%)<br>15 (4%)<br>176 (47%)                 |
| 4.        | <b>При регистрации биометрических персональных данных Вы давали письменное согласие? Выберите один вариант ответа.</b><br>а) да;<br>б) нет;<br>в) не придавал этому значения;<br>г) регистрация не проводилась.                                 | 64 (17%)<br>30 (8%)<br>105 (28%)<br>176 (47%)     |
| 5.        | <b>В каком из видов учреждений Вы регистрировали биометрические персональные данные? Выберите один вариант ответа.</b><br>а) государственный орган исполнительной власти;<br>б) орган местного самоуправления;<br>в) банк;                      | 26 чел. (7%)<br>0 чел. (0%)<br>116 чел. (31%)     |

|    |                                                                                                                                                                                                                                                                                                                |                                                                                                                                  |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
|    | г) иные кредитные организации;<br>д) лица, оказывающие профессиональные услуги на финансовом рынке;<br>е) индивидуальный предприниматель;<br>ж) нотариус;<br>з) МФЦ;<br>и) мобильное приложение;<br>к) другие организации (укажите какая _____);<br>л) не регистрировал (а).                                   | 0 чел. (0%)<br>0 чел. (0%)<br>0 чел. (0%)<br>0 чел. (0%)<br>23 чел. (6%)<br>34 чел. (9%)<br>0 чел. (0%)<br>176 (47%)             |
| 6. | <b>Случалось ли, что Ваши биометрические персональные данные подвергались утечке и были использованы в мошеннических целях? Выберите один вариант ответа.</b><br>а) да,<br>(подчеркните какие – запись голоса, фотоизображение, дактилоскопическая информация, геномная информация, иное ( _____));<br>б) нет. | 45 чел. (12%)<br><b>из них:</b><br>16 чел. (35%)<br>29 чел. (65%)<br>0 чел. (0%)<br>0 чел. (0%)<br>0 чел. (0%)<br>330 чел. (88%) |
| 7. | <b>В какой государственный орган Вы бы обратились или уже обращались при утечке биометрических персональных данных? Выберите один вариант ответа.</b><br>а) МВД России;<br>б) Роскомнадзор;<br>в) Центральный Банк РФ;<br>г) Суды;<br>д) МФЦ;<br>е) Прокуратура.                                               | 293 чел. (78%)<br>4 чел. (1%)<br>11 чел. (3%)<br>22 чел. (6%)<br>15 чел. (4%)<br>30 чел. (8%)                                    |
| 8. | <b>Достаточно ли по Вашему мнению на сегодняшний день ресурсов у МВД России для обеспечения безопасности биометрических персональных данных граждан? Выберите один вариант ответа.</b><br>а) да, достаточно;<br>б) нет, не достаточно;<br>в) требует совершенствования.                                        | 191 чел. (51%)<br>45 чел. (12%)<br>139 чел. (37%)                                                                                |
| 9. | <b>К какому виду ответственности Вы считаете правильным привлекать лиц, виновных в утрате биометрических персональных данных? Выберите один вариант ответа.</b>                                                                                                                                                |                                                                                                                                  |

|     |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                 |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
|     | а) дисциплинарная;<br>б) гражданская;<br>в) административная;<br>г) уголовная.                                                                                                                                                                                                                                                                                                                                                                    | 45 чел. (12%)<br>41 чел. (11%)<br>214 чел. (57%)<br>75 чел. (20%)                               |
| 10. | <b>Какой из видов административного наказания Вы считаете допустимым при совершении правонарушений действий в отношении биометрических персональных данных гражданина РФ? Выберите один вариант ответа.</b><br>а) предупреждение;<br>б) административный штраф;<br>в) административный арест;<br>г) административное приостановление деятельности;<br>д) обязательные работы.                                                                     | 26 чел. (7%)<br>322 чел. (86%)<br>15 чел. (4%)<br>7 чел. (2%)<br>0 чел. (0%)                    |
| 11. | <b>Какой размер административного штрафа Вы считаете справедливым за правонарушения в области биометрических персональных данных в отношении оператора единой биометрической системы? Выберите один вариант ответа.</b><br>а) от 500 до 1500 рублей;<br>б) от 1 500 до 3 000 рублей;<br>в) от 5 000 до 10 000 рублей;<br>г) от 50 000 до 100 000 рублей;<br>д) от 100 000 до 500 000 рублей;<br>е) от 1 000 000 рублей и выше.                    | 0 чел. (0%)<br>0 чел. (0%)<br>11 чел. (3%)<br>79 чел. (21%)<br>150 чел. (40%)<br>135 чел. (36%) |
| 12. | <b>Какой размер административного штрафа Вы считаете справедливым за правонарушения в области биометрических персональных данных в отношении должностного лица оператора единой биометрической системы? Выберите один вариант ответа.</b><br>а) от 500 до 1 500 рублей;<br>б) от 1 500 до 3 000 рублей;<br>в) от 5 000 до 10 000 рублей;<br>г) от 50 000 до 100 000 рублей;<br>д) от 100 000 до 500 000 рублей;<br>е) от 1 000 000 рублей и выше. | чел. (0%)<br>чел. (0%)<br>191 чел. (51%)<br>154 чел. (41%)<br>30 чел. (8%)<br>чел. (0%)         |
| 13. | <b>Как Вы считаете, достаточны ли на сегодняшний день размеры административных штрафов за нарушения в</b>                                                                                                                                                                                                                                                                                                                                         |                                                                                                 |

|     |                                                                                                                                                                                                                                                                                                                                                                                        |                                                              |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
|     | <b>области защиты биометрических персональных данных?</b><br>а) да, достаточны;<br>б) нет, не достаточны.                                                                                                                                                                                                                                                                              | 281 чел. (75%)<br>94 чел. (25%)                              |
| 14. | <b>Как Вы считаете положена ли материальная компенсация физическому лицу при утрате его биометрическими персональными данными конфиденциальности вследствие совершения неправомерных действий? Выберите один вариант ответа.</b><br>а) да, положена;<br>б) нет, достаточно привлечения к административной ответственности.                                                             | 364 чел. (97%)<br>11 чел. (3%)                               |
| 15. | <b>Какой размер материальной компенсации физическому лицу при утрате его биометрическими персональными данными конфиденциальности вследствие совершения неправомерных действий Вы считаете справедливым? Выберите один вариант ответа.</b><br>а) от 5 000 до 1 0000 рублей;<br>б) от 10 000 до 100 000 рублей;<br>в) от 500 000 до 1 000 000 рублей;<br>г) от 1 000 000 рублей и выше. | чел. (0%)<br>27 чел. (7%)<br>307 чел. (82%)<br>41 чел. (11%) |
| 16. | <b>Знаете ли Вы о запретах на принудительный сбор биометрии и на дискриминацию людей, отказывающихся ее предоставлять? Выберите один вариант ответа.</b><br>а) да, знаю;<br>б) нет, не знаю.                                                                                                                                                                                           | 120 чел. (32%)<br>255 чел. (68%)                             |
| 17. | <b>Известно ли Вам, что Вы имеете право отозвать ранее данное согласие на обработку биометрических персональных данных в любой момент? Выберите один вариант ответа.</b><br>а) да, известно;<br>б) нет, не известно.                                                                                                                                                                   | 41 чел. (11%)<br>334 чел. (89%)                              |

**Федеральный закон  
о внесении изменений в Федеральный закон  
от 27 июля 2006 г. № 152-ФЗ «О персональных данных»**

**Статья 1.** Внести в Федеральный от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ред. от 28.02.2025) (Собрание законодательства Российской Федерации от 2006 г., № 31, ст. 3451 (Часть I)) следующие изменения:  
часть 1 статьи 11 изложить в следующей редакции:

«Под биометрическими персональными данными следует понимать сведения, относящиеся к физиологическим и поведенческим характеристикам физического лица, полученные в целях идентификации и (или) аутентификации в результате специальной технической обработки, в том числе с использованием автоматизированных систем. Биометрические персональные данные могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.».

**Статья 2.** Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

Президент Российской Федерации

В. ПУТИН

« \_\_\_\_ » \_\_\_\_\_ 202\_\_ г.

**Федеральный закон**  
**о внесении изменений в Федеральный закон от 29 декабря 2022 г. № 572-ФЗ**  
**«Об осуществлении идентификации и (или) аутентификации физических лиц**  
**с использованием биометрических персональных данных, о внесении**  
**изменений в отдельные законодательные акты Российской Федерации и**  
**признании утратившими силу отдельных положений законодательных актов**  
**Российской Федерации»**

**Статья 1.** Внести в Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» (ред. от 28.12.2024) (Собрание законодательства Российской Федерации от 2023 г., № 1, ст. 19 (Часть I)) следующие изменения:

статью 2 дополнить пунктом 12 и 13:

«12) ложное воссоздание биометрических персональных данных с использованием искусственного интеллекта – воссоздание биометрических характеристик человека посредством использования искусственного интеллекта в целях совершения несанкционированного доступа при идентификации личности;

13) идентификация по ложному биометрическому идентификатору – использование копии биометрических персональных данных, полученных с использованием искусственного интеллекта на основе биометрических характеристик, в целях совершения неправомерной идентификации личности, ведущее к не санкционируемому доступу.».

**Статья 2.** Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

Президент Российской Федерации  
В. ПУТИН

«\_\_\_» \_\_\_\_\_ 202\_\_ г.

**Федеральный закон**  
**О внесении изменений в Кодекс Российской Федерации**  
**об административных правонарушениях**

Внести в Кодекс Российской Федерации об административных правонарушениях (Собрание законодательства Российской Федерации, 2002, № 1, ст. 1; 2007, № 26, ст. 3089; 2011, № 19, ст. 2715; 2013, № 30, ст. 4029; 2014, № 45, ст. 6142; 2020, № 9, ст. 1123; 2022, № 29, ст. 5226) следующие изменения:

статью 13.11.3. дополнить пунктом 5:

«Создание копии биометрических персональных данных, полученных с использованием искусственного интеллекта на основе биометрических характеристик, в целях совершения неправомерной идентификации личности, ведущее к не санкционируемому доступу

влечет наложение административного штрафа на физических лиц в размере от пятисот тысяч до одного миллиона рублей; на юридических лиц – от одного миллиона до двух миллионов рублей.».

**Статья 2.** Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

Президент Российской Федерации

В. ПУТИН

« \_\_\_\_ » \_\_\_\_\_ 202\_\_ г.

## Проект

**Приказ МВД России от «\_\_»\_\_\_\_\_ 2025 г.  
«О внесении изменений в Инструкцию по организации защиты  
персональных данных, содержащихся в информационных системах органов  
внутренних дел Российской Федерации, утвержденную приказом  
МВД России от 6 июля 2012 г. № 678»**

Внести изменения в Инструкцию по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации, утвержденную приказом МВД России от 6 июля 2012 г. № 678 (ред. от 07.12.2016) (Зарегистрировано в Минюсте России 18 сентября 2012 г. № 25488), согласно прилагаемому Перечню.

Министр  
генерал полиции Российской Федерации

В. Колокольников

Приложение  
к приказу МВД России  
от «\_\_»\_\_\_\_\_ 2023 г. №\_\_

**Перечень  
изменений, вносимых в Инструкцию по организации защиты  
персональных данных, содержащихся в информационных системах  
органов внутренних дел Российской Федерации, утвержденную приказом  
МВД России от 6 июля 2012 г. № 678**

1. Пункт 2 изложить в следующей редакции:

«2. Настоящая Инструкция определяет порядок выполнения мероприятий по защите персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации, устанавливает меры по обеспечению безопасности ПДн, в том числе биометрических, при их обработке в информационных системах персональных данных, а также определяет обязанности должностных лиц.

В Инструкции не рассматриваются вопросы обеспечения безопасности ПДн, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также меры, связанные с применением шифровальных (криптографических) средств защиты информации.

Методы и способы защиты информации, содержащейся в государственных информационных системах, определяются в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17.

2. Пункт 3 изложить в следующей редакции:

«3. Министерство внутренних дел Российской Федерации в соответствии с Федеральным законом № 152-ФЗ является оператором, организующим и (или) осуществляющим обработку ПДн, в том числе биометрических, а также определяющим цели обработки, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.».

3. Пункт 27 дополнить следующими подпунктами:

«27. Руководители подразделений-операторов ИСПДн обеспечивают выполнение правовых, организационных и технических мер, предусмотренных законодательными и иными нормативными правовыми актами Российской Федерации, в части, их касающейся, в том числе:

планирование и организацию выполнения мероприятий по обеспечению безопасности ПДн, в том числе биометрических;

конфиденциальность, целостность и доступность ПДн, в том числе биометрических;

организацию взаимодействия подразделений МВД России, обеспечивающих создание (модернизацию) и эксплуатацию ИСПДн, в том числе биометрических;

защиту ПДн, в том числе биометрических;

определение должностных обязанностей лиц, ответственных за организацию обработки ПДн, в том числе биометрических, и за эксплуатацию ИСПДн;

организацию и осуществление контроля за выполнением установленных требований по обеспечению безопасности ПДн, в том числе биометрических.»