

Дата поступления рукописи в редакцию: 20.02.2026 г.

DOI: 10.24412/2076-1503-2026-2-793-798

Дата принятия рукописи в печать: 10.03.2026 г.

ШЕСТАК Виктор Анатольевич,
доктор юридических наук, доцент,
профессор 25 кафедры (военной администрации,
административного и финансового права)
Военного университета имени князя Александра Невского
Министерства обороны Российской Федерации,
e-mail: viktor_shestak@mail.ru

ЛЕОНТЬЕВА Адель Альбертовна,
курсант 4-го курса,
факультет подготовки следователей,
Московская академия Следственного комитета
Российской Федерации имени А.Я. Сухарева,
e-mail: mail@law-books.ru

КРИМИНАЛИСТИКА И БИОМЕТРИЯ: ПРЕИМУЩЕСТВА, ОГРАНИЧЕНИЯ, ПРОБЛЕМЫ КОНФИДЕНЦИАЛЬНОСТИ

Аннотация. В статье анализируется использование и значение биометрических данных в методике расследования преступлений. Освещаются правовые аспекты защиты персональных данных и рассматриваются основные стороны развития биометрических технологий. Авторы подчёркивают тенденцию внедрения и развития биометрических методов в криминалистике, которые представляют собой практические способы применения технологий и методов идентификации личности. Рассматриваются определённые источники биометрических данных, такие как папиллярный узор пальцев, радужная оболочка и сетчатка глаза, голосовой профиль и изображение лица. Обозначена значимость применения таких технологий при расследовании преступлений и розыске преступников. Особое внимание обращено как на имеющиеся в данной сфере преимущества, в том числе точность идентификации, так и на ограничения данного метода, а также проблемы конфиденциальности, связанные со сбором и хранением биометрических данных.

Ключевые слова: криминалистика, технологии, биометрия, персональные данные.

SHESTAK V.A.,
Professor of the 25th Department
(Military Administration, administrative and financial law)
of the Prince Alexander Nevsky Military University
of the Ministry of Defense of the Russian Federation,
Doctor of Juridical Science, Moscow

LEONTEVA A.A.,
4th year cadet,
Faculty of Investigator Training, A. Ya. Sukharev Moscow Academy
of the Investigative Committee of the Russian Federation

FORENSICS AND BIOMETRICS: ADVANTAGES, LIMITATIONS, AND PRIVACY CONCERNS

Annotation. This article analyzes the use and importance of bio-metric data in the methodology of crime investigation. The legal aspects of personal data protection are covered and the main aspects of biometric technologies development are considered. The authors emphasize the tendency of introduction and development of biometric methods in criminalistics, which represent practical ways of application of technologies and methods of personal identification. Certain sources of biometric data such as finger papillary pattern, iris and retina, voice profile and facial image are consid-

ered. The significance of the use of such technologies in the investigation of crimes and search for criminals is emphasized. Particular attention is paid to the advantages in this area, such as high accuracy of identification, as well as the limitations of this method, as well as privacy issues associated with the collection and storage of biometric data.

Key words: *forensics, biometric technologies, biometrics, personal data.*

Современная криминалистика эволюционирует в условиях активной цифровизации правоохранительной сферы, что обуславливает интенсивную интеграцию технологий автоматизированной верификации личности. Биометрия как прикладное междисциплинарное направление формирует инструментальный базис для разрешения идентификационных задач, представляя собой совокупность методов количественного анализа уникальных физиологических и поведенческих характеристик индивида. Методы идентификации личности, основанные на биометрической информации, определяются так называемыми биометрическими технологиями. Указанные технологии оперируют данными о физических и поведенческих особенностях человека, которые подвергаются сопоставлению с эталонными параметрами, зарегистрированными ранее, в целях идентификации (аутентификации).

Биометрические данные включают информацию о биометрических характеристиках личности, а именно о физических и персональных параметрах, которые сравниваются с ранее зафиксированными показателями субъекта для его идентификации (аутентификации). К числу источников биометрических данных относятся кожный покров (папиллярные узоры) пальцев, радужная оболочка и сетчатка глаза, голосовой профиль, изображение лица, особенности почерка, кинетика движений и иные параметры [2].

Исторически внедрение биометрической информации в криминалистику сопряжена с прогрессом научного знания и интеграцией различных научных областей в единую дисциплину. Биометрия, позиционируя себя как прикладная наука, уходит корнями в иные научные направления и изначально развивалась в контексте более широких отраслевых дисциплин. Данный процесс включал не только формирование теоретического аппарата, но и синтез аккумулированных знаний, что потребовало расширения научного горизонта и определения новых векторов для последующего развития. В этой связи знаковым этапом стала интеграция смежных наук для конструирования унифицированной биометрической системы [1].

Открытие минисателлитной ДНК в области молекулярной генетики в 1985–1987 гг. ученым А. Джефрисом кардинально трансформировало парадигму возможностей идентификации личности. Это позволило существенно модернизировать

методы установления личности, одновременно значительно расширив доказательственный потенциал. Структура гипервариабельных участков ДНК, локализованных в нескольких локусах хромосом, является уникальной для каждого индивидуума. С этого момента правомерно констатировать формирование фундамента для разработки молекулярно-генетической идентификации личности и для более прецизионного анализа генетических данных. Практическая значимость данного научного открытия проявилась в возможности анализа как ядерной, так и митохондриальной ДНК. Это обеспечило возможность идентификации даже по минимальным биологическим объектам — фрагментам костной ткани, волосам, частям черепа. Важно акцентировать, что параллельно с этим существуют и менее масштабные подходы к идентификации. В частности, использование параметров радужной оболочки и сетчатки глаза, которые применимы для установления личности, но в более ограниченном объеме.

Криминалистическая идентификация постепенно трансформировалась из преимущественно морфологического сличения признаков в высокотехнологичный комплекс анализа биологических, антропометрических, а впоследствии и цифровых параметров. Так, в становление фоноскопического направления криминалистической идентификации весомый вклад внесли изыскания Э.И. Абалмазова и А.И. Кугушева, которые аргументировали возможность использования акустических параметров речевого сигнала в качестве индивидуализирующих признаков личности [4]. В их исследовании фокус был направлен на поиск и формализацию таких совокупностей характеристик звуковой волны, которые позволяли бы создавать математически верифицируемые модели распознавания диктора, чем была заложена теоретическая база для разработки алгоритмов идентификации человека по фонограммам речи.

В 2016 году была учреждена Национальная биометрическая платформа (далее — НБП), впоследствии переименованная в Единую биометрическую систему (далее — ЕБС). В 2019 году эта система начала функционировать в контуре Единой системы идентификации и аутентификации (далее — ЕСИА) посредством верификации биометрических данных в ЕБС, оператором которой выступает ПАО «Ростелеком». Биометрические данные фиксируются различными способами, включая аудио- и видеозапись, фотографирова-

ние, описание, графическое отображение, а также с использованием их комбинаций [2]. При этом необходимо учитывать, что использование биометрической информации тесно сопряжено с императивом строгого регулирования процессов сбора, обработки и защиты персональных данных.

Так, развитие ведомственных информационных систем МВД России началось существенно раньше. С 2005 года в стране реализуется программа создания единой информационно-телекоммуникационной системы органов внутренних дел, поддержанная Правительством Российской Федерации [6]. В рамках этой программы было разработано несколько ключевых подпрограмм, которые стали основой для функционирования Главного информационно-аналитического центра Министерства внутренних дел Российской Федерации (далее – ГИАЦ МВД РФ). Эти подпрограммы были ориентированы на решение ряда приоритетных задач, среди которых — реконструкция и модернизация информационных центров МВД России, формирование и расширение базы данных дактилоскопической информации в регионах, развитие региональных программно-технических комплексов, а также разработка автоматизированной информационной системы (далее – АИС) для аккумуляции биометрических данных.

Необходимо учитывать, что при решении идентификационных задач совместное функционирование АИС и автоматизированных информационно-поисковых систем (далее – АИПС) с определенной алгоритмизацией обеспечивает технологическую платформу современной криминалистической идентификации. В данной архитектуре связей АИС обеспечивает учетно-организационную и информационную основу, выраженную в накоплении, структурировании и поддержании актуальности массивов данных, тогда как АИПС реализует поисково-сопоставительный механизм, направленный на выявление потенциальных совпадений и генерацию перечня релевантных результатов. Подобная взаимосвязь и последовательность этапов функционирования детерминирует скорость, полноту и достоверность идентификационного решения.

В рамках приоритетных задач информационно-аналитической работы ГИАЦ МВД РФ в условиях современной цифровизации выделяются, в частности, развитие ведомственной ИТ-инфраструктуры и комплекса учётно-регистрационных массивов, а также повышение качества аналитических продуктов (обзоры, сводки, информационные справки и проч.).

В современной практике фоноскопических исследований активно применяются комплексные АИС, обеспечивающие анализ и сопоставление речевых сигналов. К числу таких разработок отно-

сятся система идентификации диктора «SIS», созданная в Центре речевых технологий, программный комплекс «Диалект», ориентированный на обработку и акустический анализ речи, а также зарубежная автоматизированная система «CSL», разработанная в США. Использование данных технологий позволяет осуществлять идентификацию личности по зафиксированному речевому материалу, что приобретает особую значимость при расследовании преступлений, связанных с похищениями, вымогательством, финансовыми мошенничествами и заведомо ложными сообщениями о террористических актах [3]. Применение таких систем расширяет доказательственные возможности правоохранительных органов, повышая объективность и точность экспертных заключений.

В современных условиях активно разрабатываются перспективные направления биометрической идентификации, базирующиеся на расширении спектра используемых признаков. К числу таких подходов относится применение антропометрических характеристик, включая параметры кистей рук и морфологические особенности ушных раковин. Наряду с этим исследуются инновационные методы, предполагающие анализ отражающих свойств кожного покрова, построение тепловых карт тела и лица, а также идентификацию по индивидуальным одорологическим признакам. Такое расширение перечня биометрических параметров позволяет акцентировать внимание на повышении точности распознавания личности и минимизации вероятности ошибок при автоматизированном сопоставлении данных. В частности, направление, связанное с динамическими аспектами человека, охватывает методы и технологии, позволяющие идентифицировать личность по таким признакам, как жестикуляция, походка, мимика, речь, стиль набора текста на клавиатуре и другие поведенческие характеристики субъекта [4].

В России одним из наиболее распространённых методов биометрической идентификации личности остается дактилоскопия. Также активно применяются технологии распознавания по изображениям лиц и голосам, которые отличаются высокой стабильностью и уникальностью физиологических характеристик человека. Биометрические данные, основанные на физиологических характеристиках человека, обладают свойством индивидуальной неповторимости и константности на протяжении длительного времени. К таким признакам относятся папиллярные узоры пальцев, морфологические особенности лица, структура радужной оболочки глаза, параметры голосового сигнала и иные анатомо-физиологические характеристики. Их резистентность к естественным

изменениям и высокая степень межиндивидуальной вариативности позволяют использовать данные признаки в качестве надежных идентификаторов личности.

Указанные свойства обуславливают возможность длительного хранения биометрической информации, её систематизации и интеграции в централизованные базы данных. Формирование специализированных информационных массивов обеспечивает автоматизированное сопоставление параметров, повышает скорость установления личности и способствует объективизации идентификационных процедур в правоохранительной практике и иных сферах применения.

Вместе с тем именно имманентная неизменяемость большинства биометрических признаков формирует специфический правовой и технологический риск. В отличие от пароля или иного цифрового идентификатора, биометрический параметр невозможно «заменить» в случае его компрометации. Утечка таких данных способна повлечь долгосрочные негативные последствия для субъекта, поскольку повторное использование похищенной информации может происходить латентно, без его ведома. Данное обстоятельство усиливает требования к режиму хранения, алгоритмам шифрования и нормативному регулированию оборота биометрических персональных данных, что требует комплексного подхода к их защите.

Отметим, что высокая идентификационная ценность биометрических данных сочетается с повышенной степенью их чувствительности и уязвимости. Это предопределяет необходимость установления особого правового режима их сбора, обработки и хранения. В условиях цифровизации государственного управления и расширения сфер применения биометрии формирование четких нормативных механизмов защиты персональных данных становится неотъемлемым условием легитимности использования таких технологий. Именно поэтому вопросы правового регулирования биометрической информации занимают центральное место в современной научной и правоприменительной практике, требуя комплексного анализа международных и национальных норм, определяющих пределы допустимости интервенции в сферу частной жизни. Так, статья 8 Международной декларации о генетических данных человека, принятой 16 октября 2003 года на 20-м пленарном заседании Генеральной конференции ЮНЕСКО, устанавливает, что для сбора, обработки и хранения генетической информации необходимо получить информированное согласие человека. Декларация также допускает, что национальные законодательные акты могут вводить

ограничения на получение такого согласия, при условии, что они не противоречат международным правовым нормам [5].

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» устанавливает, что операторы обязаны принимать меры для защиты персональных данных, включая биометрическую информацию, от несанкционированного доступа, уничтожения и распространения [9]. Кроме того, разъяснением Минфина России в письме № 03-01-11/52306 от 15 июля 2019 года определено, что обработка персональных данных, включая биометрические параметры, может быть произведена без согласия субъекта, если это необходимо для выполнения международных договоров, отправления правосудия или в случаях, когда действия соответствуют законодательству в области обороны, безопасности и противодействия терроризму [8]. Вместе с тем, несмотря на наличие нормативных актов, направленных на обеспечение конфиденциальности и защиту прав субъекта персональных данных, на практике возможны случаи использования этих данных без согласия владельца. Примером может служить размещение фотографий сотрудников в пропускных системах или на служебных удостоверениях без предварительного уведомления, что вызывает вопросы о целесообразности и пропорциональности таких действий в контексте защиты персональных данных.

Отметим, что защита биометрических данных остаётся относительно новой и недостаточно исследованной областью, что создаёт риски злоупотреблений и манипуляций с конфиденциальной информацией. Недостаточная теоретическая и практическая проработка отдельных аспектов её защиты создаёт предпосылки для поиска и применения способов обхода существующих механизмов безопасности. Это обстоятельство повышает криминогенные риски в сфере использования автоматизированных идентификационных систем. Так, современная практика свидетельствует о том, что злоумышленники используют технические ограничения АИПС для снижения вероятности распознавания личности. В частности, модификация визуального образа может достигаться за счёт грима, имитации шрамов, применения маскирующих элементов одежды и головных уборов, а также использования очков с затемнёнными, зеркальными либо нестандартной формы линзами. Названные приёмы направлены на искажение ключевых антропометрических признаков, лежащих в основе алгоритмов распознавания [7].

В подобных ситуациях визуальный облик лица трансформируется таким образом, что алгоритмы распознавания либо не фиксируют совпа-

дений, либо формируют результаты с низкой степенью достоверности. Это существенно снижает доказательственную ценность полученных данных в рамках уголовного судопроизводства. Практика свидетельствует, что наличие видеозаписи само по себе не гарантирует установления личности, если параметры изображения не позволяют провести надёжное биометрическое сопоставление. При этом в отдельных случаях установлено, что даже при фиксации подозреваемых средствами видеонаблюдения их идентификация затруднена из-за лимитированности используемых технологий. Тем самым прослеживается объективная зависимость эффективности АИПС от качества исходного материала, алгоритмической точности и полноты базы сравнения.

В этой связи, несмотря на расширение практики применения АИПС и рост числа раскрытых преступлений с их использованием, потенциал этих систем реализуется неравномерно. Так, в Российской Федерации их вклад в общую статистику раскрываемости остаётся умеренным, тогда как в отдельных регионах, включая Москву и Московскую область, наблюдаются значительно более высокие показатели результативности, в виду наличия более развитой технической инфраструктуры и более масштабных баз данных. При этом данная сфера общественных отношений имеет ряд ограничений. Так, эффективность применения биометрических методов зависит от качества и количества предоставленных данных. Не всегда возможно получить достаточный объем образцов для обучения системы, особенно в случаях, когда речь идёт о редких или специфических характеристиках. Ограничения также проявляются и во влиянии культурных и этнических особенностей на результаты идентификации. Биометрические системы могут быть менее эффективными при работе с людьми из разных культур и этнических групп, так как их антропометрические черты могут отличаться от общепринятых стандартов.

Следует подчеркнуть, что эффективность применения биометрических методов распознавания существенно лимитируется использованием двумерных изображений. Плоский формат фиксации лица не позволяет в полной мере учитывать глубинные анатомические параметры, что может снижать точность сопоставления и увеличивать вероятность ошибок. В этой связи перспективным направлением развития габитологии выступает внедрение трёхмерного анализа лица, основанного на уникальности костной структуры черепа и пространственных пропорций лицевых элементов. Создание трёхмерной модели на основе светового или лазерного сканирования

позволяет учитывать глубину, объём и геометрию лица, а также минимизировать влияние внешних факторов — очков, головных уборов и иных маскирующих элементов. В результате обработки антропометрических данных формируется цифровой идентификатор, пригодный для инкорпорации в специализированные базы данных и дальнейшего автоматизированного сопоставления [1].

Технологии трёхмерной реконструкции открывают новые горизонты для криминалистической габитологии, однако их практическая имплементация сопряжена с рядом объективных трудностей. Формирование трёхмерного изображения лица требует сложного математического моделирования, высокоточного оборудования и специализированного программного обеспечения. Такой процесс является ресурсоёмким и требует участия квалифицированных специалистов в области информационных технологий и судебной экспертизы. Так, совершенствование методов трёхмерного анализа и постепенное снижение технологических издержек, по нашему мнению, способны существенно повысить достоверность идентификационных процедур и вывести габитологию на качественно новый уровень развития.

Отметим, что биометрия и криминалистика сталкиваются с проблемой конфиденциальности. Они связаны с возможностью хищения и несанкционированного использования биометрической информации. Злоумышленники могут получить доступ к личным данным, используя различные методы, в частности, такие как фишинг, социальная инженерия и взлом приложений и сервисов. Одним из основных рисков является кража биометрических данных: отпечатки пальцев, электронный образ радужной оболочки глаза или голоса. Эти данные могут быть использованы для создания поддельных идентификационных профилей или мошенничества с использованием чужих документов. Не способствует обеспечению биометрической безопасности и деятельность ряда крупных компаний, которые активно собирают и хранят большие объёмы биометрической информации, что периодически приводит как к утечке данных, так и нарушению конфиденциальности пользователей.

Таким образом, несмотря на то, что в России применение биометрических технологий, в том числе для распознавания лиц, распространено достаточно локально, в наиболее крупных городах (в частности, система «безопасный город» запущена в крупных городах, в частности в Москве, Краснодаре, Казани, Санкт-Петербурге), продолжающееся внедрение биометрических методов идентификации в различные аспекты жизнедеятельности человека отражает устойчи-

вую мировую тенденцию, имеющую ряд преимуществ по сравнению с другими способами идентификации личности.

Согласованное взаимодействие правоохранительных и правоприменительных структур направлено на поддержание публичного правопорядка и нейтрализацию угроз национальной безопасности. В сложившихся условиях интеграция передовых технологических решений обретает стратегический характер. Вместе с тем внедрение подобных инноваций предполагает не только их техническое совершенствование, но и формирование нормативной базы, а также неукоснительное соблюдение баланса между результативностью следственных действий и неприкосновенностью прав и свобод личности. Достижение такого баланса, по нашему мнению, является фундаментальным условием для легитимности и общественного признания идентификационных процедур.

Комплексный подход к проектированию и внедрению биометрических технологий, базирующийся на достижениях науки и цифровых инновациях, формирует облик современной парадигмы криминалистической идентификации. При обеспечении адекватного правового регулирования и реализации принципов информационной безопасности рассмотренные технологии способны качественно повысить оперативность расследования, оптимизировать доказательственную базу и внести существенный вклад в повышение общего уровня раскрываемости преступлений.

Список литературы:

- [1] Баканова Я.В. Некоторые аспекты применения биометрических технологий в криминалистике // Альманах молодого исследователя. 2020. № 9. С. 91-94.
- [2] Егоров, Н. Н. Криминалистика: учебник и практикум для вузов / Н. Н. Егоров, Е. П. Ищенко. Москва: Издательство Юрайт, 2024. 617 с.
- [3] Жуков Н.М. Обоснованность использования биометрических данных в криминалистической науке: история вопроса и проблемы правовой защиты персональных данных // Международный научно-исследовательский журнал. 2021. № 12. Ч. 4. С. 164-167.
- [4] Криминалистика: учебник для вузов / И. В. Александров. Москва : Издательство Юрайт, 2024. 409 с.
- [5] Международная декларация о генетических данных человека// Организация объединенных наций - URL: https://www.un.org/ru/documents/decl_conv/declarations/genome_dec.shtml (дата обращения: 14.02.2026).
- [6] Новиков В.В. Перспективы развития информационной инфраструктуры органов внутренних дел // Проблемы экономики и юридической практики. 2009. № 5. С. 72-77.
- [7] Писарев Д.Ю. Проблемы применения биометрических систем в раскрытии преступлений.: дис. канд. наук: 12.00.09 / Писарев Дмитрий Юрьевич. Краснодар, 2012. 20 с.
- [8] Письмо Минфина России № 03-01-11/52306 от 15.07.2019. – Электронный ресурс. – URL: <https://online11.consultant.ru/cgi/online.cgi?req=doc&base=QUEST&n=186934&cacheid=2A80106DC9C4E1C66A4D5AC3135A3E5B&mode=splus&rnd=t8DYbQ#rBIEKBV8ydrdRKBa2> (дата обращения: 12.02.2026).
- [9] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ // Российская газета. 2006. № 165. С изм. и допол. в ред. от 24.06.2025.

References:

- [1] Bakanova Y.V. Some aspects of the application of biometric technologies in forensics//Almanac of a young researcher. 2020. № 9. S. 91-94.
- [2] Egorov, N. N. Criminalistics: textbook and workshop for universities/N.N. Egorov, E.P. Ishchenko. Moscow: Yurayt Publishing House, 2024. 617 pp.
- [3] Zhukov N.M. Validity of the use of biometric data in forensic science: the history of the issue and the problems of legal protection of personal data// International Research Journal. 2021. № 12. PART 4. S. 164-167.
- [4] Forensics: a textbook for universities/I.V. Alexandrov. Moscow: Yurayt Publishing House, 2024. 409 pp.
- [5] International Declaration on Human Genetic Data//United Nations - URL: https://www.un.org/ru/documents/decl_conv/declarations/genome_dec.shtml (Accessed: 14.02.2026).
- [6] Novikov V.V. Prospects for the development of the information infrastructure of the internal affairs bodies//Problems of economics and legal practice. 2009. № 5. S. 72-77.
- [7] Pisarev D.Yu. Problems of using biometric systems in solving crimes.: dis. cand. sciences: 12.00.09/Pisarev Dmitry Yuryevich. Krasnodar, 2012. 20 s.
- [8] Letter of the Ministry of Finance of Russia No. 03-01-11/52306 dated 15.07.2019. - Electronic resource. – URL: <https://online11.consultant.ru/cgi/online.cgi?req=doc&base=QUEST&n=186934&cacheid=2A80106DC9C4E1C66A4D5AC3135A3E5B&mode=splus&rnd=t8DYbQ#rBIEKBV8ydrdRKBa2> (дата обращения: 12.02.2026).
- [9] Federal Law “On Personal Data” dated 27.07.2006 No. 152-FZ//Rossiyskaya Gazeta. 2006. № 165. Amended and supplemented as amended by 24.06.2025.