Дата поступления рукописи в редакцию: 17.07.2026 г. DOI: 10.24412/2224-9133-2026-7-308-314
Дата принятия рукописи в печать: 31.07.2026 г.

ДАВЫДОВ Евгений Васильевич,
доцент кафедры исследования документов учебно-научного комплекса экспертно-криминалистической деятельности Волгоградской Академии МВД России, кандидат юридических наук, доцент,
e-mail: dawydov@yandex.ru.

ФИНОГЕНОВ Владимир Федорович,
доцент кафедры криминалистики Саратовской государственной юридической академии, кандидат юридических наук, доцент,
e-mail: finogenovv@yandex.ru

ИСПОЛЬЗОВАНИЕ СИСТЕМ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УГОЛОВНО-ПРОЦЕССУАЛЬНОМ ДОКАЗЫВАНИИ: СОВРЕМЕННЫЕ РЕАЛИИ И ПРАВОВЫЕ ПЕРСПЕКТИВЫ

Аннотация. *В статье рассматриваются современные правовые и криминалистические проблемы использования систем биометрической идентификации личности, основанных на технологиях искусственного интеллекта, в уголовно-процессуальном доказывании. Особое внимание уделено вопросам допустимости, достоверности и проверяемости результатов автоматизированного биометрического анализа, а также рискам их некритического восприятия в следственной и судебной практике. Автор исходит из того, что алгоритмическое совпадение не может рассматриваться как самостоятельное доказательство виновности лица, поскольку нуждается в процессуальном закреплении, экспертной либо специальной проверке и оценке в совокупности с иными доказательствами. Анализируются положения уголовно-процессуального законодательства, законодательства о персональных данных и нормативного регулирования биометрической идентификации. Отмечается, что развитие систем распознавания лиц, голоса и иных биометрических признаков требует не только технического совершенствования, но и формирования специальных процессуальных правил их применения. В статье обосновывается необходимость ведомственного контроля, фиксации цифрового следа, раскрытия значимых параметров работы программных средств и подготовки сотрудников правоохранительных органов к грамотному использованию таких технологий. Делается вывод о вспомогательном характере искусственного интеллекта в доказывании и недопустимости подмены внутреннего убеждения суда результатами машинной обработки данных.*

Ключевые слова: *биометрическая идентификация, искусственный интеллект, уголовно-процессуальное доказывание, цифровые доказательства, персональные данные, распознавание лиц, допустимость доказательств, экспертная проверка, уголовный процесс, правоохранительная деятельность.*

DAVYDOV Evgeny Vasilyevich,
Associate Professor of the Department of Document Research at the Educational and Scientific Complex of Forensic Activities at the Volgograd Academy of the Ministry of Internal Affairs of Russia, Candidate of Legal Sciences, Associate Professor

FINOGENOV Vladimir Fedorovich,
Associate Professor of the Department of Criminalistics at the Saratov State Law Academy, Candidate of Legal Sciences, Associate Professor

USE OF BIOMETRIC IDENTIFICATION SYSTEMS BASED ON ARTIFICIAL INTELLIGENCE IN CRIMINAL PROCEDURE EVIDENCE: MODERN REALITIES AND LEGAL PROSPECTS

Annotation. *The article examines current legal and forensic issues related to the use of artificial intelligence-based biometric identification systems in criminal procedural proof. Special attention is paid to the admissibility, reliability and verifiability of automated biometric analysis results, as well as to the risks of their uncritical acceptance in investigative and judicial practice. The author proceeds from the position that an algorithmic match cannot be regarded as independent evidence of a person's guilt, since it requires proper procedural documentation, expert or specialist verification, and assessment in conjunction with other evidence. The article analyzes the provisions of criminal procedure legislation, personal data law and regulatory rules governing biometric identification. It is emphasized that the development of facial recognition, voice recognition and other biometric technologies requires not only technical improvement, but also the formation of special procedural rules for their use. The need for departmental control, recording of the digital trace, disclosure of significant parameters of software operation and training of law enforcement officers in the competent use of such technologies is substantiated. The article concludes that artificial intelligence should play an auxiliary role in criminal proof and that judicial discretion must not be replaced by the results of machine data processing.*

Key words: *biometric identification, artificial intelligence, criminal procedural proof, digital evidence, personal data, facial recognition, admissibility of evidence, expert verification, criminal procedure, law enforcement.*

Цифровизация уголовного судопроизводства уже давно перестала быть темой исключительно научных прогнозов. Следователь, дознаватель, эксперт, оперативный сотрудник и суд сегодня работают не только с традиционными следами, документами и показаниями, но и с видеозаписями, цифровыми профилями, метаданными, изображениями с камер наблюдения, результатами автоматизированного поиска, сведениями из информационных систем и т.д. На этом фоне особое значение приобретают системы биометрической идентификации личности, основанные на технологиях искусственного интеллекта и речь здесь идет, прежде всего, о распознавании лица, голоса, отпечатков пальцев, радужной оболочки глаза, особенностей походки, а в перспективе и о комплексной мультимодальной идентификации, когда несколько биометрических признаков анализируются одновременно.

Для уголовного процесса такие технологии выглядят одновременно привлекательными и опасными. Привлекательными — потому что позволяют быстрее установить личность подозреваемого, проверить алиби, обнаружить перемещения лица, сопоставить изображение с базами данных, сузить круг проверяемых лиц. Опасными — потому что результат машинного анализа легко воспринимается правоприменителем как «технически объективный», хотя в действительности он зависит от качества алгоритма, исходной базы, угла съемки, освещенности, настроек порога совпадения, ошибок оператора и даже от того, каким образом была сформирована обучающая выборка, хотя в уголовном судопроизводстве такая ошибка и не является простой технической погрешностью, но она способна привести к незаконному задержанию, необоснованному обвинению, формальному подтверждению следственной версии и, в худшем случае, к судебной ошибке.

Действующий Уголовно-процессуальный кодекс Российской Федерации не содержит специального вида доказательств, именуемого «результаты работы искусственного интеллекта» или «алгоритмическое заключение», однако статья 74 УПК РФ исходит из более широкой формулы: доказательствами признаются любые сведения, на основе которых суд, прокурор, следователь и дознаватель устанавливают обстоятельства, имеющие значение для уголовного дела [1]. Такая конструкция теоретически позволяет включать в доказывание сведения, полученные при помощи биометрических систем, но не снимает главного вопроса: каким процессуальным способом такие сведения должны быть получены, закреплены, проверены и оценены. И именно здесь, по нашему мнению, здесь начинается наиболее сложная часть проблемы.

Биометрическая идентификация в уголовном процессе не может рассматриваться как обычный технический сервис, подобный поисковой строке в базе данных, поскольку сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность, рос-

сийское законодательство относит к биометрическим персональным данным [2]. Уже одно это обстоятельство требует осторожности, так как в отличие от номера телефона или адреса электронной почты, биометрический признак не так просто заменить. Если похищенный или подобранный пароль можно сменить, то лицо, голос или папиллярный узор пальцев заменить не возможно. Поэтому использование таких данных в интересах раскрытия и расследования преступлений должно быть построено не на принципе технологического удобства, а на принципе строгой правовой необходимости.

Законодатель сделал важный шаг, приняв Федеральный закон от 29 декабря 2022 г. № 572-ФЗ, регулирующий идентификацию и аутентификацию физических лиц с использованием биометрических персональных данных [3]. Хотя и следует признать, что данный закон в большей степени ориентирован на гражданско-правовые, публично-сервисные и административные отношения, связанные с Единой биометрической системой. Уголовно-процессуальное доказывание же имеет иную природу, здесь результат биометрического сопоставления может стать поводом для следственного действия, основанием для проверки версии, элементом заключения эксперта либо частью иного документа. Но в тоже время он не должен автоматически превращаться в доказательство виновности, поскольку это и есть по своей сути та принципиальная граница, которую нельзя размывать даже ради оперативности.

На практике биометрические системы чаще всего используются на первоначальном этапе работы: при анализе видеозаписей с камер наблюдения, при поиске лиц, находящихся в розыске, при проверке причастности к преступлениям, совершенным в общественных местах. К примеру, запись с камеры фиксирует лицо, похожее на подозреваемого, алгоритм сопоставляет изображение с массивом фотографий и выдает вероятное совпадение. Для оперативного поиска это полезный инструмент, для доказывания же только начало работы, поскольку следователь обязан выяснить происхождение видеозаписи, условия съемки, целостность файла, отсутствие монтажа, параметры работы программы, порядок доступа к базе, действия специалиста, а затем сопоставить полученный результат с другими доказательствами. Если же этого не сделать, уголовный процесс рискует получить не доказательство, а красивую цифровую иллюзию. Ведь особенность искусственного интеллекта в биометрической идентификации состоит в том, что итоговый вывод часто формируется не путем простого совпадения признаков, как это может показаться на первый взгляд. Современные системы используют методы машинного обучения, компьютерного зрения, нейронные сети, вероятностные модели. Внешне результат выглядит кратко: «совпадение вероятно», «совпадение не установлено», «коэффициент сходства — такой-то», но за этой краткостью скрывается массив технических операций, не всегда понятных даже подготовленному юристу. М.С. Спиридонов справедливо указывает, что использование технологий искусственного интеллекта в уголовно-процессуальном доказывании не должно разрушать принцип свободы оценки доказательств и подменять деятельность суда машинным расчетом [7]. И с этим трудно спорить, так как алгоритм по сути не несет процессуальной ответственности, не предупреждается об уголовной ответственности за заведомо ложное заключение, не может быть допрошен как свидетель и не способен объяснить человеческим языком, почему именно он пришел к конкретному результату.

Отсюда вытекает первая правовая проблема: как квалифицировать результат биометрической идентификации. В одних случаях он может быть оформлен как приложение к протоколу следственного действия, например осмотра видеозаписи. В других — как результат оперативно-разыскной деятельности, который затем должен быть введен в уголовный процесс установленным законом способом. В третьих — как часть заключения эксперта, если исследование проводилось в рамках судебной экспертизы. Наконец, возможен вариант участия специалиста, который поясняет суду или следователю технические особенности работы программы. Но единообразия здесь пока нет, и это не мелкая методическая недоработка, а серьезный риск для допустимости доказательств. Поэтому допустимость в данной сфере должна пониматься шире, чем простое соблюдение формы протокола. Необходимо проверять законность получения исходных биометрических данных, правовой режим базы, полномочия лица, проводившего поиск, сохранность цифрового следа, наличие журнала операций, неизменность файла, технические характеристики программного средства. Если видеозапись была скопирована без фиксации хеш-суммы, если неизвестно, кто именно запускал поиск, если алгоритм выдавал несколько кандидатов, а в материалы дела попал только один, защита вполне обоснованно поставит вопрос о достоверности и полноте представленных сведений, поскольку УПК РФ признает недопустимыми доказательства, полученные с нарушением закона [1]. Для цифровой биометрии в целом это означает, что нарушение может быть не только процессуальным, но и технологическим, если оно повлияло на проверяемость результата.

Вторая проблема, как мы уже сказали, связана с достоверностью. Техническая точность

системы не равна доказательственной достоверности, даже авторитетные международные оценки систем распознавания лиц показывают, что их качество зависит от конкретного алгоритма, массива данных, сценария применения и демографических характеристик сравниваемых лиц [6]. Следовательно, нельзя ссылаться на «искусственный интеллект» как на некий универсальный знак надежности, ведь в уголовном деле имеет значение не репутация технологии вообще, а проверяемость конкретного результата по конкретному эпизоду. Было ли лицо в маске? Какой угол поворота головы? Какое разрешение камеры? Какой порог сходства выставлен? Сколько кандидатов выдала система? Кто исключил остальных? На эти вопросы должен отвечать не пресс-релиз разработчика, а конкретный специалист, и все должно быть процессуально офрмлено, чтобы закрепить результат.

Третья проблема — алгоритмическая непрозрачность. В учебной аудитории легко сказать: «нужно проверить алгоритм», в реальном же деле это сложнее. Коммерческий разработчик может ссылаться на охрану программного кода, ведомство — на служебный характер информации, эксперт — на невозможность раскрыть внутренние параметры нейросетевой модели. Но уголовный процесс не может строиться по принципу «поверьте системе, она сертифицирована», так как право на защиту предполагает возможность оспаривать доказательство, поскольку если сторона защиты лишена доступа к сведениям о методике, точности, ошибках и условиях применения программы, состязательность становится декоративной. Здесь требуется разумный баланс: раскрывать не обязательно весь исходный код, но должны быть доступны сведения, достаточные для проверки надежности результата, иначе цифровая технология превращается в недоступного для критики так называемого «скрытого эксперта».

Четвертая же проблема имеет криминалистический характер. Биометрические данные сегодня не только помогают расследованию, но и сами становятся объектом преступного воздействия. Развитие дипфейк-технологий, синтеза голоса, подделки изображений и имитации лица создает новую категорию рисков. М.А. Желудков в своих работах обращает внимание на возможность создания поддельных аудиозаписей и видеоизображений на основе незаконно полученных биометрических данных [10]. И с развитием сети интернет мы видим это практически повсеместно. Для доказывания это означает, что видеозапись с лицом человека уже нельзя воспринимать как безусловное подтверждение его присутствия. Если раньше спор чаще шел о качестве записи: видно или не видно, похож или не похож, то сейчас возникает другой вопрос: действительно ли на записи реальное лицо, а не сгенерированный или модифицированный образ. А это уже меняет саму культуру оценки цифровых доказательств.

Отдельного внимания заслуживает опыт зарубежного регулирования. Европейский союз в Регламенте 2024/1689 об искусственном интеллекте пошел по пути риск-ориентированного подхода, выделив удаленную биометрическую идентификацию, особенно в режиме реального времени и в публичных пространствах, в категорию наиболее чувствительных практик [5]. Для российского же уголовного процесса прямое заимствование европейской модели вряд ли возможно и не всегда оправданно, поскольку российская система имеет собственные задачи безопасности, иную организацию правоохранительных органов и иной режим процессуального контроля. Но сама идея предварительной оценки риска, ограничения целей, фиксации оснований применения и последующего контроля заслуживает внимания. Не всякая камера с распознаванием лиц должна автоматически становиться инструментом уголовного преследования. Здесь нужны критерии: тяжесть преступления, наличие иных способов установления личности, срочность, масштаб вмешательства в частную жизнь, круг лиц, попадающих под обработку. В отечественной доктрине даже сформировалось понимание того, что биометрическая идентификация по изображению лица способна повысить эффективность раскрытия и расследования преступлений, особенно в условиях крупных городов и развитой системы видеонаблюдения [8], о чем свидетельствует повсеместно применяемая система «умный город». Но эффективность сама по себе не является процессуальной ценностью, если она достигается ценой снижения гарантий личности. К тому же уголовный процесс исторически недоверчив к «слишком удобным» доказательствам. К примеру, признание, полученное без защитника, оперативная информация без процессуального закрепления, показания заинтересованного лица без проверки — все это может выглядеть убедительно, но закон требует большего. И с биометрическими алгоритмами должна действовать та же логика, их сила не в том, что они заменяют доказывание, а в том, что они помогают точнее организовать его.

Нам представляется ошибочным включать в УПК РФ отдельный вид доказательств под названием «результаты искусственного интеллекта», поскольку это создало бы ложное впечатление самостоятельной доказательственной природы алгоритмического вывода. Более разумным выглядит другой путь: закрепить специальные требования к использованию цифровых и биометрических сведений в доказывании. Такие требо-

вания могли бы включать указание на источник данных, способ их получения, технические параметры обработки, сведения о программном средстве, данные о лице, проводившем анализ, порядок сохранения исходных файлов и результатов обработки, а также возможность проверки стороной защиты. Тогда и результат работы системы будет оцениваться не по магической формуле «ИИ установил», а по обычным правилам относимости, допустимости, достоверности и достаточности. В то же время в экспертной деятельности перспективным является использование искусственного интеллекта как инструмента специальных знаний. И.П. Чекотов обоснованно рассматривает ИИ как возможную форму реализации специальных знаний при условии экспертной верификации и соблюдения процессуальных гарантий [9]. Практически это означает следующее: эксперт может применять программный комплекс для анализа изображения или голоса, но итоговый вывод должен принадлежать эксперту, а не программе и, при этом, эксперт обязан описать методику, исходные данные, ограничения исследования и причины, по которым он принимает либо отвергает результат автоматизированного анализа. Суд же, в свою очередь, не должен ограничиваться фразой «заключение эксперта сомнений не вызывает», поскольку в делах, где биометрическая идентификация имеет ключевое значение, требуется более предметная оценка.

Не менее важна и подготовка сотрудников органов внутренних дел, поскольку технологии биометрической идентификации нельзя внедрять только приказом о подключении к системе. Сотрудник должен понимать, что алгоритмическое совпадение — это версия, а не готовое обвинение, необходимо обучать не только нажимать кнопку поиска, но и правильно документировать действия, сохранять исходные данные, работать с цифровыми носителями, взаимодействовать со специалистом, оценивать риски, ошибки и т.д. И здесь, как мы считаем, будет полезен практико-ориентированный подход: разбор ситуаций, где система дала ложное совпадение; моделирование спора с защитником; подготовка протокола осмотра видеозаписи; анализ заключения эксперта по изображению лица и т.д. Поскольку без такой подготовки даже самая современная система будет порождать процессуальные дефекты. К тому же любая биометрическая система, используемая в правоохранительной сфере, должна оставлять проверяемый след: кто обращался к базе, по какому основанию, в отношении какого материала, какой результат получил, какие действия совершил после этого. Журналы доступа и аудита имеют не только значение информационной безопасности, они являются будущей гарантией допустимости. Ведь если сторона защиты заявит, что поиск проводился многократно до получения удобного результата, именно журнал операций позволит подтвердить или опровергнуть этот довод. В отсутствие же такого журнала доверие к доказательству снижается, даже если сама технология работала корректно.

Правовые перспективы видятся на в нескольких направлениях. Во-первых, требуется разработка межведомственных методических рекомендаций по использованию биометрической идентификации в раскрытии и расследовании преступлений, с отдельным блоком, посвященным уголовно-процессуальному закреплению результатов. Во-вторых, целесообразно уточнить в УПК РФ правила работы с цифровыми доказательственными материалами, включая видеозаписи, результаты автоматизированной обработки и сведения из информационных систем. В-третьих, необходимы стандарты экспертной проверки биометрических результатов: какие данные указываются в заключении, как описывается программное средство, как отражается вероятность ошибки, какие исходные материалы приобщаются к делу. В-четвертых, следует развивать судебную практику по оценке таких доказательств, иначе основные правила будут формироваться стихийно — через отмененные приговоры и жалобы.

Таким образов в заключение мы можем резюмировать, что системы биометрической идентификации личности на основе искусственного интеллекта уже вошли в сферу уголовного судопроизводства, хотя уголовно-процессуальный закон пока не успел дать им самостоятельное и точное описание. И это довольно типичная ситуация для цифровой эпохи, поскольку технология применяется раньше, чем появляется развитая правовая форма. Запрещать же такие системы бессмысленно, игнорировать их риски опасно, наиболее взвешенный путь состоит в том, чтобы признать их вспомогательным инструментом доказывания, но не источником истины в последней инстанции.

Главный вывод заключается в следующем: биометрическая идентификация может иметь доказательственное значение только при условии процессуальной прозрачности, технической проверяемости и возможности критической оценки сторонами. Результат работы искусственного интеллекта не должен подменять заключение эксперта, внутреннее убеждение суда и обязанность следователя доказывать обстоятельства дела совокупностью доказательств. Алгоритм может подсказать направление поиска, выявить совпадение, ускорить анализ массива данных, но обвинение человеку предъявляет не алгоритм, а государство, которое обязано обеспечить законность, контролируемость и объяснимость исполь-

зования таких технологий. Перспективы развития законодательства должны быть связаны не с механическим включением искусственного интеллекта в УПК РФ, а с формированием специальных правил обращения с биометрическими и иными цифровыми данными. Требуется ввести процессуальные требования к фиксации, хранению, проверке и представлению результатов автоматизированной идентификации; стандарты экспертной верификации; механизмы ведомственного и судебного контроля; подготовку сотрудников правоохранительных органов к грамотной работе с такими системами. Только при таком и никаком другом подходе биометрические технологии будут служить не цифровым украшением уголовного дела, а реальным средством установления обстоятельств преступления при сохранении прав личности.

Список литературы:

[1] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ : ред. действ. // Собрание законодательства Российской Федерации. 2001. № 52, ч. I. Ст. 4921. URL: https://www.consultant.ru/document/cons_ doc_LAW_34481/ (дата обращения: 07.07.2026).

[2] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» : ред. действ. // Собрание законодательства Российской Федерации. 2006. № 31, ч. I. Ст. 3451. URL: https://www.consultant.ru/document/ cons_doc_LAW_61801/ (дата обращения: 07.07.2026).

[3] 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» // Официальный интернет-портал правовой информации. URL: https://publication.pravo.gov.ru/Document/View/0001202212290024 (дата обращения: 07.07.2026).

[4] Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» : в ред. Указа Президента Российской Федерации от 15 февраля 2024 г. № 124 // Официальный интернет-портал правовой информации. URL: https://publication.pravo.gov.ru/ document/0001202402150063 (дата обращения: 07.07.2026).

[5] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. 2024. L 2024/1689. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата обращения: 07.07.2026).

[6] Face Recognition Vendor Test (FRVT) / Face Recognition Technology Evaluation (FRTE). National Institute of Standards and Technology. URL: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt (дата обращения: 07.07.2026).

[7] Спиридонов М. С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании // Journal of Digital Technologies and Law. 2023. Т. 1. № 2. С. 481–497. DOI: 10.21202/jdtl.2023.20. URL: https://www.lawjournal.digital/jour/ article/view/189/0 (дата обращения: 07.07.2026).

[8] Кутузов А. В. Криминалистическая идентификация с использованием систем распознавания лиц: состояние проблемы и потенциальные пути ее решения // Правовое государство: теория и практика. 2024. URL: https://pravgos.ru/index.php/journal/ article/view/954 (дата обращения: 07.07.2026).

[9] Чекотов И. П. Технологии искусственного интеллекта как источник специальных знаний // Вестник Института права Башкирского государственного университета. 2025. № 28. С. 349–360. DOI: 10.33184/vest-law-bsu-2025.28.32. URL: https://vestnik-ip.ru/index.php/journal/article/download/519/441 (дата обращения: 07.07.2026).

[10] Желудков М. А. Обеспечение защищенности биометрических персональных данных в условиях применения технологии «Дипфейк» // Вестник Санкт-Петербургского университета МВД России. 2025. № 2 (106). С. 159–169. DOI: 10.35750/2071-8284-2025-2-159-169. URL: https://vestnikspbmvd.ru/temp/f41fe9b3069ad77ba61d880b6e5d2db1.pdf (дата обращения: 07.07.2026).

References:

[1] Code of Criminal Procedure of the Russian Federation No. 174-FZ dated December 18, 2001: ed . // Collection of legislation of the Russian Federation. 2001. No. 52, part I. Art. 4921. URL: https://www.consultant.ru/document/cons_ doc _ LAW _ 34481/(access date: 07.07.2026).

[2] Federal Law of July 27, 2006 No. 152-FZ "On Personal Data": ed. 2006. No. 31, part I. Art. 3451. URL: https://www.consultant.ru/document/ cons _ doc _ LAW _ 61801/(access date: 07.07.2026).

[3] Federal Law of December 29, 2022 No. 572-FZ "On the identification and (or) authentication of individuals using biometric personal data, on amending certain legislative acts of the Russian Federation and invalidating certain provisions of legislative acts of the Russian Federation "// Official Internet portal of legal information.

URL: https://publication.pravo.gov.ru/ Document/View/0001202212290024 (access date: 07.07.2026).

[4] Decree of the President of the Russian Federation of October 10, 2019 No. 490 "On the development of artificial intelligence in the Russian Federation": as amended by Decree of the President of the Russian Federation of February 15, 2024 No. 124 // Official Internet portal of legal information. URL: https://publication.pravo.gov.ru/ document/0001202402150063 (access date: 07.07.2026).

[5] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. 2024. L 2024/1689. URL: https: //eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (access date: 07.07.2026).

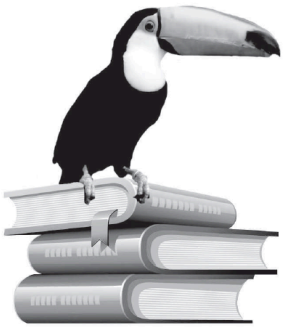
[6] Face Recognition Vendor Test (FRVT) / Face Recognition Technology Evaluation (FRTE). National Institute of Standards and Technology. URL: https: //www.nist.gov/programs-projects/face-recognition-vendor-test-frvt (дата обращения: 07.07.2026).

[7] Spiridonov M.S. Artificial intelligence technologies in criminal procedure evidence // Journal of Digital Technologies and Law. 2023. VOL. 1. № 2. PP. 481-497. DOI: 10.21202/jdtl.2023.20. URL: https ://www.lawjournal.digital/jour/article/view/189/0 (accessed: 07.07.2026).

[8] Kutuzov A. V. Forensic identification using face recognition systems: the state of the problem and potential ways to solve it // Rule of law: theory and practice. 2024. URL: https://pravgos.ru/index.php/journal/ article/view/954 (access date: 07.07.2026).

[9] Chekotov I.P. Artificial intelligence technologies as a source of special knowledge // Bulletin of the Institute of Law of Bashkir State University. 2025. № 28. S. 349-360. DOI: 10.33184/vest-law-bsu-2025.28.32. URL: https://vestnik-ip.ru/index.php/journal/article/download/519/441 (access date: 07.07.2026).

[10] Zheludkov M. A. Ensuring the security of biometric personal data in the context of the use of Deepfake technology // Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia. 2025. № 2 (106). S. 159-169. DOI: 10.35750/2071-8284-2025-2-159-169. URL: https://vestnikspbmvd.ru/temp/f41fe9b3069ad77ba61d880b6e5d2db1.pdf (access date: 07.07.2026).



www.law-books.ru

Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников, учебных и методических пособий, монографий, научных статей.

Профессионально.

В максимально короткие сроки.

Размещаем в РИНЦ, E-Library.