УДК 34

Тарасенко В.А.
студентка 3 курса
Институт прокуратуры
Саратовская государственная юридическая академия
(г. Саратов, Россия)

Федюкова К.А.
студентка 3 курса
Институт прокуратуры
Саратовская государственная юридическая академия
(г. Саратов, Россия)

Научный руководитель:
Соловьёва Т.В.
доктор юридических наук, профессор
кафедра гражданского процесса
Саратовская государственная юридическая академия
(г. Саратов, Россия)

БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ: ПРОБЛЕМЫ АУТЕНТИФИКАЦИИ ПРЕДСТАВИТЕЛЯ

Аннотация: *в данной статье рассмотрен вопрос о проблеме идентификации представителя, биометрическая идентификация рассматривается как технология автоматизированного распознавания личности. Выделены основные проблемы, а также пути решения через поправки законодательства. Из этого следует необходимость создавать нормы, которые бы обязывали разработчиков и поставщиков биометрических данных раскрывать информацию об используемых алгоритмах, что позволит обеспечить соответствие принципам правовой определенности и конкурентоспособности.*

Ключевые слова: *биометрия, идентификация представителя, аутентификация, гражданское судопроизводство, правовое регулирование, защита персональных данных, прозрачность алгоритмов.*

Современное судопроизводство невозможно представить без строгого соблюдения процессуальных гарантий, направленных на обеспечение законности и справедливости разбирательства. Одной из фундаментальных обязанностей суда, закреплённой в Гражданском процессуальном и Арбитражном процессуальном кодексах, является проверка личности участвующих в деле лиц и их представителей. Эта процедура служит не просто формальностью, а важнейшим инструментом, позволяющим установить, кто именно явился в заседание и обладает ли данное лицо необходимым объёмом полномочий для участия в процессе. Согласно ГПК и АПК суд обязан проверить личность участвующих в деле и их представителей.

Суды, проверяя доверенности и копии паспортов, удостоверяются в том, что лица, предоставившие документы суд должен проверить, кто именно явился на заседание и есть ли у этих людей право участвовать в деле. Изучая доверенности и паспорта, судья убеждается, что перед ним действительно нужные участники процесса, а не посторонние. Если с документами всё в порядке, суд признаёт полномочия явившихся и допускает их к участию в разбирательстве [1]. При этом процессуальная проверка служит гарантией законности судебного разбирательства, а также обеспечивает реализацию принципа состязательности и равноправия сторон, предотвращает случаи участия в процессе неправомочных лиц.

Законодатель намеренно и вполне осознанно проводит различие между двумя самостоятельными процедурами: установлением личности того, кто явился в суд, и определением того объёма полномочий, которым этот явившийся наделён. Такое разделение имеет принципиальное значение, ведь далеко не всегда подтверждение личности автоматически означает наличие у представителя всего необходимого круга прав. Даже в ситуации, когда личность представителя не вызывает никаких сомнений и подтверждена надлежащим образом, его правомочия могут оказаться существенно ограниченными. Данные ограничения способны вытекать из текста выданной ему доверенности, из прямых указаний закона либо из решения органа юридического лица. Именно

поэтому законодатель счёл необходимым рассматривать эти два вопроса отдельно друг от друга, не допуская их смешения и не позволяя считать, что удостоверение личности явившегося автоматически влечёт признание за ним полного объёма полномочий. В связи с этим, судебная практика исходит из недостаточности проверки полномочий, что может повлечь отмену судебного акта, так как это затрагивает права и законные интересы представляемого лица.

Биометрия — это система идентификации человека на основе его уникальных характеристик.

Биометрическая идентификация как технология автоматизированного распознавания личности стала неотъемлемой частью нашей жизни и активно используется в технике, банковском секторе и конечно же в государственных услугах. Но, конечно, такая технология имеет свои недостатки, одним из которых является проблема в конфиденциальности и безопасности данной системы. Человек и его биометрические данные служат с одной стороны простым ключом доступа, а с другой уязвимостью системы. Для начала стоит определить, что: биометрия – это уникальные физиологические и поведенческие характеристики человека [2].

К ним относятся:

отпечатки пальцев,

изображение лица,

голос,

радужка глаза.

В контексте государственной системы речь идет прежде всего о сканировании лица и образце голоса. Эти данные используются для подтверждения личности, например, при входе в мобильный банк или оказании некоторых госуслуг. Но в отличие от обычных паролей, биометрические данные нельзя сменить. Это делает их особенно уязвимыми при утечках. Помимо этого, биометрические данные в отличие от пароля или PIN-кода, не могут быть отозваны или перевыпущены: если такой идентификатор скомпрометирован, лицо практически лишено возможности заменить его на новый. Это порождает

дополнительные риски, связанные с невозможностью восстановления нарушенного права и с длительным характером последствий утечки. Существенно также то, что биометрическая идентификация может осуществляться дистанционно, без личного присутствия носителя данных, что создает почву для мошеннических действий, включая подмену изображения лица, использование синтезированного голоса и иных методов обхода систем распознавания.

Фундаментальной проблемой аутентификации является выбор биометрического признака как непосредственного идентификатора.

Важно сказать, что биометрия человека устроена куда сложнее, соответственно изменить такой ключ доступа как обычный пароль - нельзя.

Здесь важно учитывать особенности анатомического строения и устройства человека, а также индивидуальность, например папиллярные узоры на пальцах рук.

Следует учитывать и то, что биометрический признак не является тайной в строгом смысле слова: изображение лица или голос человек демонстрирует публично, поэтому они могут быть собраны без его явного согласия. Это отличает биометрию от пароля, который изначально предполагает конфиденциальность. Кроме того, биометрические системы не обладают абсолютной точностью: возможны как ложные отказы, так и ложные совпадения, а вероятность ошибки возрастает при изменении внешности, заболеваниях, старении или технических сбоях. Наконец, хранение биометрических шаблонов требует повышенных мер защиты, поскольку их утечка необратима и создаёт угрозу на весь период жизни человека.

Опираясь на федеральный закон от 29 декабря 2022 г. № 572-ФЗ можно увидеть, что он прямо допускает использование биометрии для аутентификации лица «в целях совершения определенных действий или подтверждения волеизъявления либо подтверждения полномочия лица на совершение определенных действий» [3].

Однако, занимательным является то, что при этом законодатель разграничивает идентификацию и аутентификацию. Идентификация отвечает на вопрос, кто перед нами, тогда как аутентификация подтверждает, что лицо действительно является тем, за кого себя выдаёт.

Такая аутентификация удостоверяет лишь тождество физического лица, но не содержание и объем его полномочий. Именно здесь заключается главная проблема: между подтверждённой личностью и неподтвержденным объемом полномочий возникает противоречие: представитель может быть аутентифицирован как конкретное лицо и при этом действовать за пределами предоставленных ему полномочий. Если говорить иначе, то биометрия подтверждает субъекта, но не подтверждает его правовой статус в конкретном правоотношении. Представитель может являться тем лицом, за которое он себя выдает, однако доверенность может быть ничтожной, срок ее действия истекшим, а перечень полномочий не включать совершение конкретного процессуального действия.

Аналогичным образом законный представитель может быть аутентифицирован, но при этом не иметь как такового права на совершение распорядительных действий без специального указания. Следовательно, биометрическая аутентификация сама по себе не способна заменить проверку полномочий, которую суд обязан проводить в силу процессуального закона.

В таком случае, в качестве решения обусловленной проблемы можно выделить следующий перечень рекомендаций:

Не сводить подтверждение полномочий исключительно к биометрическим данным,

Прямо фиксировать объем полномочий и допустимые способы подтверждения,

Контролировать согласие на обработку биометрических данных,

Круг субъектов, управомоченных применять единую биометрическую систему для аутентификации лица, давшего согласие, указан в части 1 статьи 10 Закона № 572-ФЗ. В него входят государственные органы, органы МСУ, Банк

России и иные организации. Однако на практике возникает вопрос: как соотносится биометрическая аутентификация с проверкой полномочий представителя, которую суд обязан проводить в силу процессуального закона.

Одним из способов решения актуальных проблем данной сферы является введение в законодательство требования прозрачности алгоритмов, используемых в биометрических системах. Из этого следует необходимость создавать нормы, которые обяжут разработчиков и поставщиков биометрических данных раскрывать информацию об используемых алгоритмах, что позволит обеспечить соответствие принципам правовой определенности и конкурентоспособности [3]. Прозрачность алгоритмов важна и потому, что она позволяет выявлять дискриминационные эффекты, проверять корректность обработки данных и оспаривать решения, принятые автоматизированной системой. Помимо этого, открытость сведений об алгоритмах способствует формированию доверия граждан к биометрическим технологиям, а также снижает риск их отказа от использования соответствующих сервисов. Проведенное исследование позволяет сделать вывод о том, что суд, руководствуясь процессуальным законодательством обязан удостовериться в полномочиях всех участников дела, включая их представителей. В настоящее время биометрическая идентификация активно внедряется в банковскую сферу и систему государственных услуг. Для повышения ее эффективности был предложен комплекс мер, направленных на совершенствование данного инструмента. Для начала важно сказать, что полномочия участников не должны ограничиваться только биометрическими данными, необходимо четко определить полный объем и допустимые методы подтверждения, включая электронные. Далее, на законодательном уровне следует закрепить требования к прозрачности алгоритмов, используемых в биометрических системах. Это будет способствовать развитию конкуренции на рынке технологий и повышению уровня доверия к биометрической аутентификации. Также, следует отметить, что биометрическая аутентификация выполняет свою специфическую функцию (установление личности), однако она не заменяет судебную проверку

полномочий. Биометрия является лишь инструментом и ее использование должно сопровождаться определенными юридическими процедурами, подтверждающими реальный объём прав и обязанностей участников судебного процесса. Важно сказать, что законодателю в данном контексте недостаточно ограничиться лишь декларированным заявлением о прозрачности алгоритмов, такой шаг сам по себе не создает действенных правовых гарантий и не способен предотвратить злоупотребление на практике. Необходимо установить четкую, юридически обязывающую ответственность операторов биометрических систем за возможные ошибки идентификации, включая как материальные, так и процессуальные последствия таких ошибок.

При этом важно, чтобы ответственность сводилась не просто к формальным санкциям, а обеспечивала реальную возможность оспаривания и пересмотра решений, принятых на основе автоматизированного анализа. Суду также должно быть предоставлено не только право, но и фактическая возможность запрашивать альтернативные доказательства полномочий в тех случаях, когда корректность работы автоматизированной системы вызывает обоснованные сомнения. Подводя итог, важно отметить, что только комплексный подход, сочетающий в себе правовую ответственность, процессуальные гарантии и техническую оснащенность обеспечит укрепление законности при внедрении цифровых технологий в судопроизводство, а также позволит минимизировать как коррупционные, так и технические риски, связанные с использованием биометрических и иных автоматизированных систем.

СПИСОК ЛИТЕРАТУРЫ:

1. Биометрия: лицо и голос вместо паспорта [Электронный ресурс] // ГАРАНТ.РУ: [сайт]. 16.07.2025. URL: https://www.garant.ru/article/1829500/ (дата обращения: 01.10.2026)
2. Вильданова М.М. Проблемы идентификации и аутентификации сторон гражданско-правовых споров при дистанционном рассмотрении дел в суде // Право и практика. 2020. № 4. URL: https://cyberleninka.ru/article/n/problemy-identifikatsii-i-autentifikatsii-storon-grazhdansko-pravovyh-sporov-pri-distantsionnom-rassmotrenii-del-v-sude (дата обращения: 01.10.2026)
3. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (ред. от 04.08.2026) (с изм. и доп., вступ. в силу с 01.09.2026)
4. Федеральный закон от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»»
5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями и дополнениями)
6. Чебанный К.А. Проблемы идентификации личности по биометрическим данным в условиях киберугроз: правовой аспект // Молодой ученый. 2025. № 22 (573). С. 513–515. URL: https://moluch.ru/archive/573/126006

Tarasenko V.A.
student of 3rd year
Institute of the Prosecutor's Office
Saratov State Law Academy
(Saratov, Russia)

Fedyukova K.A.
student of 3rd year
Institute of the Prosecutor's Office
Saratov State Law Academy
(Saratov, Russia)

Scientific advisor:
Soloveva T.V.
PhD in Law, Professor
Department of Civil Procedure
Saratov State Law Academy
(Saratov, Russia)

BIOMETRIC IDENTIFICATION: CHALLENGES IN AUTHENTICATING A REPRESENTATIVE

Abstract: *this article examines challenges in identifying a representative and considers biometric identification as a technology for automated identity recognition. It identifies key problems and proposes solutions via legislative amendments. This highlights the need for rules requiring developers and providers of biometric data to disclose information about the algorithms they use, thereby supporting legal certainty and competitiveness.*

Keywords: *biometrics, representative identification, authentication, civil proceedings, legal regulation, personal data protection, algorithmic transparency.*